

eSecurity

The First Line of Digital Defense Begins with Knowledge

Vol 51 - (2/2021)

Spyware



Privacy Issues in Big Data

Quick Facts on Privacy Information Management Systems (PIMS)

Securing Data in Cloud Using BYOE and BYOK

Understanding Spyware: Types and Effects

"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 1905-1995



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

200601006881 (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

www.cybersecurity.my



WELCOME MESSAGE FROM THE CEO OF CYBERSECURITY MALAYSIA



Dear Readers,

Cybersecurity continues to be a vital topic today, given that we are still in the midst of a pandemic where information assets become more vulnerable, and an increasing number of people are working remotely. Companies need to adjust in this new world, with added pressures on the security of their services as they need to maintain efficient operations while working in a safe environment.

Cybersecurity industry's dynamics are changing as well. Digital services such as e-government, e-banking, online shopping, online classes, and even digital healthcare are rapidly expanding. In the future, the industry hopes to play a larger role in the overall 5G eco-system. More satellites and cloud platforms mean more threats and potential weak points. We must remain vigilant, as this new era of satellites closer to Earth could lead to more eyes on these sectors. Over the next decade, we foresee some of the most difficult challenges in years, to be more relevant than ever, yet more secure. This is a challenge that we need to embrace.

As the pandemic COVID-19 takes its terrible toll on human life and livelihoods, we witnessed the extraordinary measures by the governments, public-health authorities, businesses, and individuals. In order to protect people's health, governments and institutions impose movement restrictions as well as mechanisms for health tracking and reporting. These mechanisms include contact-tracing and self-reporting apps, some of which record and transmit personal health information, highlighting the importance of data protection and privacy during this crisis. However, there are concerns on personal privacy intrusion and its upcoming implications.

The COVID-19 pandemic has permanently altered our relationship with technology, accelerating the transition to digitalization. While this change is beneficial such as increased work from home opportunities and e-commerce innovations, its drawbacks are significant such as an increase in security and privacy breaches.

The progressively prominent — and inevitable — role of digital technologies during today's pandemic also correlate with concerning trends in privacy and digital ethics. Robust protection of our rights in the digital realm is possible in the near future as written in a few articles we prepared. Among the highlights that may interest you are as follow:

- Privacy Issues in Big Data
- Understanding Spyware: Types and Effects
- Securing Data in Cloud Using BYOE and BYOK
- Quick Facts on Privacy Information Management Systems (PIMS)

These are several examples of the valuable information you will find within the pages of this bulletin. I strongly believe security awareness and knowledge resources are of tremendous value to our readers.

As we move towards the new year and new normal hybrid way of life, the lightbulb for security awareness at all levels of the public should be well-lit. It is time to move on from the events of the previous year and open up new opportunities for the coming year. May 2022 be filled with blessing, good health, joy, and success.

Happy New Year 2022 and Stay Safe.

Thank you and warmest regards,

Dato' Ts. Dr. Haji Amirudin bin Abdul Wahab, FASc

Chief Executive Officer, CyberSecurity Malaysia

EDITORIAL BOARD

Chief Editor

Ts. Dr. Zahri Yunos

Editor

Col. Ts. Sazali Sukardi

Editorial Team

Yuzida Md Yazid

Designer & Illustrator

Zaihasrul Ariffin

Nurul Ain binti Zakariah

READERS' ENQUIRY

Knowledge Management, Level 1, 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

1.	How I Tried Password Brute-Force On My Home Router	1
2.	Modern Vehicle Hacking	4
3.	Strengthening Cybersecurity At Home	6
4.	Fraud In A Workplace – Why Does It Happen	8
5.	Malware On Android Is Not A Myth	11
6.	iPhone Bug Breaks Down Wi-Fi Features	15
7.	Cyber Insurance: Review Of Proposal Assessment Questionnaire	17
8.	Fintech: Risk And Security Perspectives	21
9.	Introduction To Money Laundering	24
10.	SiberKASA Initiative During The Pandemic	27
11.	Over-Sharenting: How Much Is Too Much?	29
12.	Purple Team: The Missing Piece To A Complete Puzzle	32
13.	Information Technology (IT) Books For Babies	36
14.	Securing Your Video Conferencing Meeting	40
15.	Privacy Issues In Big Data	42
16.	Website Preservation: Better Than Zero	46
17.	Understanding Spyware: Types And Effects	52
18.	Embracing and Adapting Early Baby Boomers Into The Digital Age – A Case Study	55
19.	The OIC-CERT Global Cybersecurity Award	58
20.	Securing Data In Cloud Using BYOE And BYOK	61
21.	Quick Facts On Privacy Information Management Systems	67
22.	The Impact Of GDPR Enactment	69
23.	Redundant Array Independent Disks (RAID): RAID Levels	72
24.	What Is Forensic Audit?	76
25.	Biometric In Forensic Identification	80
26.	Dawn Of A New Strain In Banking Trojan	87
27.	Comparison Between Security Risk Management Models	93
28.	Protection For Cyber-Bully Victims Under Malaysian Law	96
29.	Challenges Of New Working Normal	98
30.	Online Proctoring	101
31.	How Does People, Process & Technology Fit In To Mitigate Malware In A CSIRT Organization	103
32.	Etika Belajar Secara Dalam Talian	108
33.	Tip Keselamatan Siber: Bekerja Dari Rumah@WFH	110
34.	Bagaimana Hendak Bermula: Panduan Kerjaya Profesional Keselamatan Siber	111
35.	Unsur Keselamatan Siber Dalam Dasar Keselamatan Negara 2021-2025	114
36.	Langkah Berbelanja Dengan Selamat Secara Dalam Talian	117

How I Tried Password Brute-Force On My Home Router

By | Norhamadi Jaaffar

Introduction

In penetration testing, password brute-force is used to check whether clients have diligently set strong passwords on their systems or not. It is a simple process of guessing the correct password numerous times until you hit the jackpot. You can do this manually if you feel ever so lucky or with the help of a software. Your odds of hitting the jackpot would be higher if the correct username has been first identified through some other ways, such as social engineering.

For security purposes, servers and workstation login pages are configured to lockout after a certain number of failed login attempts. However, network equipment such as a router, switch or firewall is often not configured by the network admin to react the same way after several wrong attempts. Much worse, if those login pages are exposed to the Internet, it could be the gateway to your organisation's internal network. A pen tester could leverage on this vulnerability and perform a password brute-force attack.

As a pen tester, you need to sharpen your tactics, techniques and procedures in a lab environment specially set up in your office. However, there are times when you are stuck at home (because of the pandemic) and need to try something out. I have been looking forward to brute-force a switch or a router for some time now. Since I had plenty of time last weekend, I decided to try my hands on launching a password brute-force attack from the comforts of my home. All I needed was to find a target.

What better target is there than my home WIFI router! I assure you here that I did not know the username and password for it. So, what follows is my adventure in hacking my home router.

Brute-Force Attack

Step 1: Finding the WIFI router's IP address

It was not difficult to find the router's IP address.

All I needed to do was to issue the command `ipconfig` at the command prompt and look at the search results.

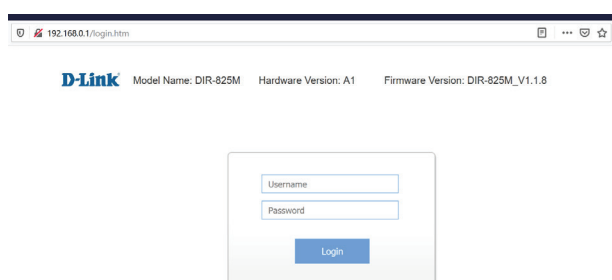
```
Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . : dlinkrouter.local
Link-local IPv6 Address . . . . . : fe80::fc49:22b8:f76d:feed%44
IPv4 Address. . . . . : 192.168.0.104
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.0.1
```

The IP address of my home router is 192.168.0.1, as it is the default gateway to the Internet for my home network. My computer's IP address is 192.168.0.104.

Step 2: Peeking into the Web Login Page

Now that I have the IP address, let us take a look at the web login page. I needed to fire up my favourite Firefox browser, so I keyed in the router's IP address and hit ENTER.



There you go. The login page was elegantly displayed for me.

Step 3: Finding the software tool that will do the dirty job for me.

I realised that there are probably hundreds of different ways to do this. However, I have been frequently visiting this particular site lately and wanted to check it out for any intel. Sure enough, it had what I was looking for, and it is called Hatch. I downloaded Hatch from the GitHub page <https://github.com/nsgodshall/Hatch> and cloned it on my computer.

Step 4: Making way for the hitman

There were a few dependencies that I had to take care of before cloning hitman Hatch. Hatch needs Python 2.0 to run, and I needed to get that fixed. I found the Python version that I wanted at this site <https://www.python.org/downloads/windows/>.

- [Python 2.7.13 - Dec. 17, 2016](#)
 - Download [Windows debug information files](#)
 - Download [Windows debug information files for 64-bit binaries](#)
 - Download [Windows help file](#)
 - Download [Windows x86-64 MSI installer](#)
 - Download [Windows x86 MSI installer](#)

I downloaded the Windows x86 MSI Installer and installed Python 2.7.13 under the root directory. To ensure Python was running fine, I typed in the command python and hit ENTER.

```
Command Prompt - python
C:\Python27>python
Python 2.7.13 (v2.7.13:a06454b1afa1, Dec 17 2016, 20:42:59) [MSC v.1500 32 bit (Intel)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
```

Next, I issued two commands to install the dependencies.

```
C:\Python27\Scripts>pip2 install selenium
C:\Python27\Scripts>pip2 install requests
```

I needed one more tool, which was to install a driver that would allow me to control Chrome through the Python program. To do so, I downloaded a file from the site <https://chromedriver.chromium.org/downloads> and then created a folder called webdrivers on my C drive and moved the downloaded file into this folder. To place it in another directory, I needed to modify the Python code.

Current Releases

- If you are using Chrome version 91, please download [ChromeDriver 91.0.4472.19](#)
- If you are using Chrome version 90, please download [ChromeDriver 90.0.4430.24](#)
- If you are using Chrome version 89, please download [ChromeDriver 89.0.4389.23](#)
- If you are using Chrome version 88, please download [ChromeDriver 88.0.4324.96](#)
- For older version of Chrome, please see below for the version of ChromeDriver that supports it.

```
01:28 PM <DIR> Webdrivers
```

Step 5: Cloning Hatch onto my computer

To help me clone Hatch easily onto my computer, I decided to install GIT for Windows from this site <https://git-scm.com/download/win>. Once done, I typed in the command to clone Hatch and hit ENTER.

```
Git CMD
C:\Users\hamadi> c:\> git clone https://github.com/nsgodshall/Hatch.git
```

As you can see, the hitman Hatch is now here.

```
03:38 PM <DIR> hatch
```

Step 6: Preparing the list of passwords for Hatch.

I could easily create my customised list of passwords using Windows Notepad. However, I wanted to check out what's available on the Github page. I visited a page and downloaded a few short password lists, and decided to edit them to suit my purpose. I stored all my password lists under the same directory as Hatch.

<https://github.com/danielmiessler/SecLists/tree/master/Passwords/Common-Credentials>

Step 7: Watching Hatch in action

To run Hatch, I typed in the command main.py and hit ENTER.

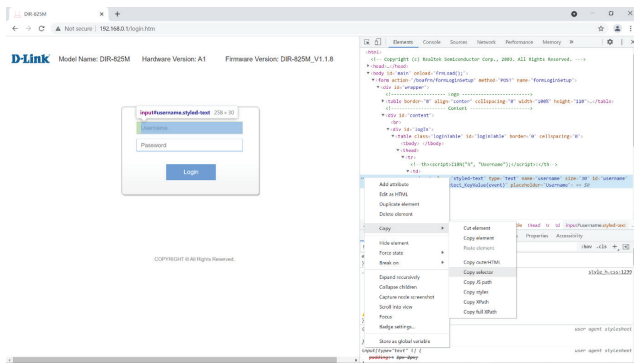
```
Command Prompt
C:\hatch>main.py
```

Once Hatch was up and running, it asked several questions. Those questions are listed below:

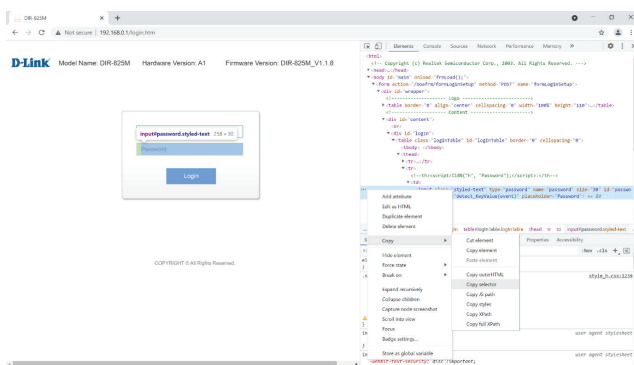
```
[~] Enter a website: http://192.168.0.1
[!] Checking if site exists
[~] Enter the username selector:
[~] Enter the password selector:
[~] Enter the Login button selector:
[~] Enter the username to brute-force:
[~] Enter a directory to a password list:
```

I had to provide Hatch with all the answers one by one. After I supplied the website address, Hatch checked to see if it existed. It opened the Chrome browser, and I opened the login page to inspect the selectors. I had to provide the selectors for the username, password and login button. I will show you how to do this later in the article. As mentioned earlier, I do not know the username and password for my home router. So, in this case, I used admin as the username. For the last question, my password list is located in C:\hatch\pwd1.txt.

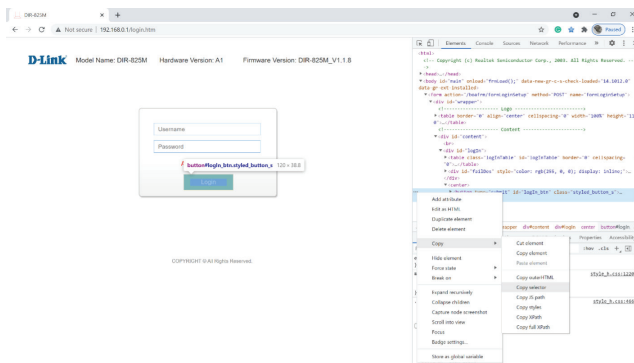
As for the selectors, I went to the login page, right-clicked on the username field and chose Inspect. The username selector is #username. I could either type it in or copy it over to Hatch. I copied it.



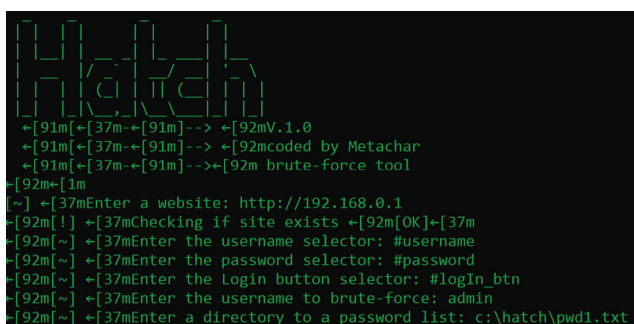
Next, I did the same for the password field. The password selector is #password, and I copied it over to Hatch.



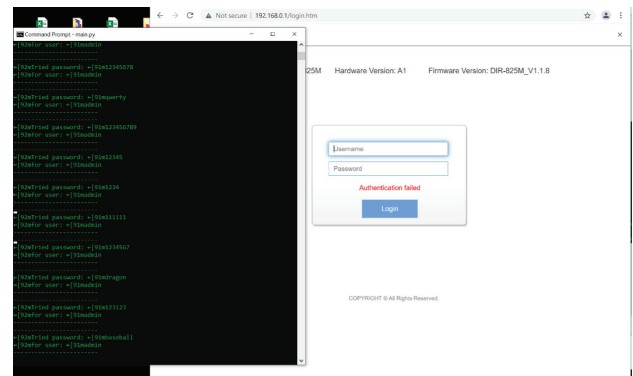
I repeated the procedure for the Login button. The selector for the button is #login_btn.



Step 8: Watching it happen before my eyes



Once Hatch started working, it sent the username and a password one at a time, spaced between a couple of seconds to the login page and hit that login button. With any luck, I would hit the jackpot in no time!



I spent my weekend learning an old craft in penetration testing, i.e., password brute-force. A weak password is a critical vulnerability. It is the easiest path for a hacker to hack into your system successfully. I urge users from all walks of life not to become another brute-force attack victim by diligently implementing strong passwords every time.

References

1. “The Story in Your Eyes – The Experiment.” By | Nazri Ahmad Zamani, Mohamad Firham Efendy Md. Senan – E-Security Bulletin 2013
2. “UFO in Putrajaya...Really?” By | Nazri Ahmad Zamani, MohdZaharudin Ahmad Darus – E-Security Bulletin 2013
3. “11 Brute-force Attack Tools for Penetration Test.” <https://geekflare.com/brute-force-attack-tools/> By | By Zaher Talab on May 20, 2021

Modern Vehicle Hacking

By | Nur Syakirah Binti Shahabuddin

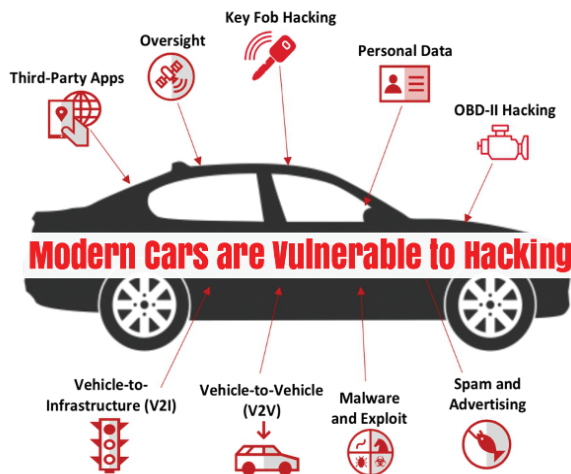


Figure 1: Modern Vehicles Security Risk

Introduction

As many are aware, modern vehicles nowadays are essential a moving information hub. Modern cars are equipped with advanced features such as global positioning system (GPS) devices, key fob entry, sensors and in-car communication such as the Bluetooth connection. These modern technologies, apart from making life easier, also make the car more vulnerable to software bugs, being a target for hackers and expose information to thieves and hackers [2].

Due to the lack of security standards, criminals have familiarized themselves on how to connect to a private network that is connected to household appliances and intelligent devices such as modern vehicles. Modern vehicles are progressively becoming the backdoor choice for data thieves due to the increasing amount of data collected and stored.

Attackers now have the option of focusing on either the vehicles by utilizing them to steal access to an e-mail account and private personal information or even access into cloud administrator.

How does it happen?

a. Information Tracking and Data Theft

Setting home address into GPS and using a telematics system will record driving data. However, once physical devices are connected to the Internet, they can be a target of cyberattack. Hackers can target an attack surface to access the vehicle's Controller Area Network (CAN) [5].

With access to a system of a connected car, hackers could send commands from a remote location to track individual vehicles, discover live site, access credit card information, passwords, and financial data. This would also lead to exploiting private and personal information including contact details, call history and short message service (SMS).

Cybercriminals can use these valuable data for various purposes such as marketing, insurance contracts, spying, and even tracking an individual's location.

b. Vehicle-to-Vehicle Communication

Vehicle-to-vehicle (V2V) communication technology allows vehicles to wirelessly communicate on the road to exchange information regarding direction, location and speed. This technology will enable vehicles to broadcast and receive omni-directional messages and it helps them to be aware of the other cars in proximity [4]. Modern cars fitted with safety applications as such can use the data regarding surrounding vehicles to identify potential crash dangers before they happen.

This technology utilizes visual, material and sound for alert. A combination of these alerts is able to caution drivers so that they can act beforehand to avoid car crashes. In this case, attackers can modify information within the wireless communication technology and reduce the car speed using destructive malware. The V2V system becomes a vector where a malicious actor could create malware to contaminate numerous connected cars.

c. Key Fob Hacking and Car Theft

Fob hacking is essentially a method to empower an attacker to enter the car without softening up. In this case, the attacker blocks the signal from the remote key, lock the vehicle and respond to the signal to compromise the car [1]. Based on McAfee Research, one variant of the attack uses a jammer to block the signal. The jammer meddles with electromagnetic waves in order to communicate with the vehicle, blocking the signal and preventing the car from locking, thus leaving access free to the attacker.

Ways to Improve Vehicle Cybersecurity to Prevent Hacking

Vehicle threats in this context refers to anything with the potential to cause vehicle hijack by attackers and they will try to attack the car in many ways. The car drivers should be alert in detecting suspicious activity at every vulnerable point before it turns into a breach. Some of the ways to improve vehicle cybersecurity in order to prevent vehicle hacking are as below;

1. Auth0's anomaly detection, an excellent example of threat detection for vehicle manufacturers which provides both password breach detection and brute force. It helps alert any malicious activity within the system that could go undetected [3].
2. Improve the encryption on critical fob radio frequencies, securing the credential login to the mobile application and necessary server access. Features like biometrics and multi-factor authentication (MFA) can help secure the access where the user needs more than their name and password to log in. Access requires an additional credential, such as a voice snippet, thumbprint or facial recognition. Thus, it could help block hackers looking for a quick way to hijack.
3. Before plugging in the USB drive into the vehicle, scan it first because an infected USB drive could contain malicious codes designed to compromise the vehicle.

Conclusion

Due to the dynamic and developing threat environment, even the most modern vehicle can be a target of a cyberattack. Extra measures need to be taken for security purposes through design and defense in depth. Modern vehicles with connected devices need constant oversight and protection from becoming a profitable target for cybercriminal.

References

1. <https://gbhackers.com/modern-cars-vulnerability/>
2. <https://www.forbes.com/sites/bernardmarr/2020/01/10/the-5-biggest-cybersecurity-trends-in-2020-everyone-should-know-about/?sh=6ff49b4e7ecc>
3. <https://auth0.com/blog/car-hacking-and-cybersecurity-in-automotive-industry/>
4. <https://www.nhtsa.gov/technology-innovation/vehicle-vehicle-communication>
5. <https://argus-sec.com/car-hacking/>

Strengthening Cybersecurity At Home

By | Ahmad Hazazi Bin Zakaria

Since early 2020, Covid-19 struck our world, forcing us to adjust to a new normal. Our daily routines, activities and working styles were adapted and changed in accordance with the latest standard operating procedure. This pandemic directly impacted our work routine as it forced us to work from home while having to maintain our quality of work. Working from home has become an essential measure to mitigate the risk of being infected by the COVID-19 virus. This new normal has led to another form of threat that employees need to face which is cyber threats. From a cyber security point of view, the risks are increasingly higher due to the exposure of employees working from home using informational technology such as email services, via personal laptop and mobile devices.

Phishing emails is one of the most common cybersecurity threats. As reported by Infosecurity Magazine, phishing emails cases have spiked by over 600% since end of February 2021. The cases rose rapidly from January, which recorded just 137 incidents to 1,158 in February and 9,116 in March 2021[1]. Phishing emails deceive users into handing over their login and confidential information to an unknown malicious actor. This action will lead to the unknown malicious actor deliberately downloading malware and spyware into the victim's computer systems. It is important to remember that cybercriminals will attack during their most vulnerable period.

Working from home presents many cybersecurity risks for the workers. According to SANS Institute, there are three top security risks: social engineering attacks, outdated system or software and weak passwords [2]. All these risks are manageable if workers possess a sound awareness of cybersecurity concerns because technology alone cannot fully protect them from a cyber-attack.

An attacker always knows the way to get what they want. Through social engineering, they pretend to be someone from technical or software sales team or offer technical assistance whereby they can create a sense of urgency and easily trick the workers into handing over

confidential information or credentials to access their personal laptops and computer. This kind of social engineering skills favour the attackers because workers lack cyber security knowledge. Hence, it is important to remember that the best defence against this type of attack are the workers themselves. They need to stay alert and always take precautions.

Due to SOPs imposed, meetings and discussions can no longer be held physically. Working from home requires an online platform to hold the meetings via video conferencing. It has become an essential part of a job. For video conferencing, it is crucial to ensure that cybersecurity is prioritised by the organizers, admins and all attendees. First and foremost, the software or the online platform that is being used need to be updated to the latest version. This is because the newest version includes the most recent security features and bug fixes. Secondly, before organisers invite any attendees, they need to ensure that the attendees join the video conference by providing passwords. Passwords should be given to all attendees in the invitation and be kept securely. Review each attendee who joins the video conference to ensure legitimacy. If necessary, ask attendees to turn on their camera so everyone in the meeting can recognise each other [3].

Electronic devices such as laptops and mobile phones are essential to help us work from home. Office issued laptops are usually installed with specific software and also contain workplace data, project details and confidential information. This information is at risk if the laptops are shared with other family members, kids especially, because they might accidentally delete important information if they are allowed to use them. In some cases, they can accidentally spill water onto the computer and damage the devices. This type of incidents can be avoided with a few simple precautions taken. Always separate office laptops from personal laptops, so that kids will not end up using critical devices. This will prevent them from deleting or modifying any data accidentally.[4] Besides that, setting an auto-log-out if the computer is idle for a specific period of time will also ensure

that no family members could use them without permission. These simple steps can bring great benefits in keeping the devices safe. Make sure family members understand the consequences of using office laptops. Instead, provide them with their own personal devices so workers can focus on the job.[5][6]

There are lots of tips and measures that can be taken to strengthen cybersecurity while working from home. The cybersecurity concerns, especially with a significant shift from the office to home, can be solved if workers apply best cyber security practices. Most of these cyber security best practices at the office can also be applied while working from home. In view of health and safety, working from home has become a new norm. Adhering to the standard operating procedures and taking proper measures can help reduce cyber security risks.

References

1. <https://www.infosecurity-magazine.com/news/covid19-drive-phishing-emails-667/>
2. <https://www.sans.org/security-awareness-training/sans-security-awareness-work-home-deployment-kit/>
3. <https://www.paloaltonetworks.com/blog/2020/04/network-video-conferencing-security/>
4. <https://www.siliconrepublic.com/advice/working-from-home-take-care-laptop-how-to>
5. <https://www.roberthalf.com/blog/salaries-and-skills/how-to-survive-working-from-home-when-your-kids-are-around>
6. <https://www.kaspersky.com/resource-center/threats/remote-working-how-to-stay-safe>

Fraud In A Workplace – Why Does It Happen

By | Azrina Binti Md Saad

Fraud is a big challenge for all organizations. It causes severe problems across all types of organizations, from corporations, limited liability companies, partnerships, and even to non-profits organizations. Curbing fraud activities has become a difficult challenge once it takes place. No matter which line of business, the reality is that employees and non-employees commit fraud. Fraud is defined as an act or course of deception, intentional concealment, omission, or perversion of truth:

1. to gain an unlawful or unfair advantage,
2. induce another to part with some valuable item or surrender a legal right, or
3. inflict injury in some manner.

Fraud should be taken seriously in all businesses but even then, why do some employees still choose to risk their integrity to commit a fraud? Although, the main reason of fraud is greed, there are many other motivations behind it and they should be looked into more in depth.

First and foremost, we must understand a human's wants and needs. A human being seeks sustainable social, financial, emotional, and physical needs to feel good. Social needs such as belonging, affection, family, and friends are essential and basic needs. Financial needs, on the other hand, include income, savings, investment, insurance, and credit. The most essential financial needs is a stable income that covers all basic necessities such as food, housing, and utilities. Physical needs is usually closely related to financial needs, where people who lack financial security almost always also lack physical security. Feeling appreciated, respected and loved are some of the examples of emotional needs.

Hence, fraud can occur when any of the needs cannot be met.

The Fraud Triangle is a classic framework designed to explain the reasoning behind a worker's decision to commit workplace fraud. The triangle represents three factors that are motivators for an employee to commit fraud: pressure, rationalisation, and opportunity. An employee in a stressful situation can view fraud as an easy way to solve his/her problems.

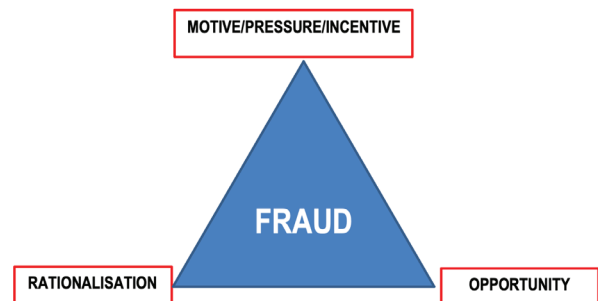


Figure 1 – Fraud Triangle

Motive/pressure/incentive

One of the motivations for an employee to commit fraud could be caused by pressure placed on him by other people such as spouse, relatives and even friends. To satisfy their human needs such as social, financial, emotional and physical needs, as stated earlier, also acts as a great motivator for committing this crime. For example, someone who lacks financial stability and facing mounting pressure to pay off debt, maintain a high standard of living, pay off a medical bill, settle rent, or dealing with some sort of addiction can be a motivator for them to risk their integrity and commit a fraud. A person who is struggling financially have the urge to solve his problems by hook or by crook. Some of the common frauds in an organization range from stealing small office stationeries to business funds, claiming benefits which an employee is not entitled to, abusing a business trip by making it a personal vacation or even as simple as misusing the annual leave.

Rationalisation

Rationalisation is the means by which an employee attempts to explain or justify their behaviour or attitude with logical reasons, even if they are not appropriate. An employee who has committed a fraud will attempt to justify his wrongdoings to overcome the ethical barrier of their conducts. Some of the reasoning's used to justify their crimes are as follow:

1. they have not been properly paid for their duties therefore they deserve to steal from the frauds

2. their employers can afford to absorb the financial losses
3. they could lose everything if they do not commit the fraud
4. they justify that “everybody does it”

Opportunity

The third element in the fraud triangle is opportunity. Even with motivation and rationalisation, a fraud cannot take place if a preparator does not see an opportunity to commit it. Weak internal controls, low likelihood of detection, lack of policy enforcement, inadequate security, or misusing their position of trust to get some personal gains, are some of the opportunities a perpetrator can make a move. For instance, when an employee was given a company car to utilise for business purposes, he sees it as an opportunity to misuse it for personal reasons.

The original fraud theory was developed by Suther Edwin Sutherland and Donald Cressey and ever since then, the conceptual framework of the fraud triangle has been expanded by other experts to relate to social influences, integrity, arrogance, competence, personal greed, and employee deprivation. In this new development, the *capability* element has been added to the three initial fraud components. This new edition of the fraud conceptual framework is called the fourth leg of the *Fraud Diamond*, and this was first presented by Wolfe and Hermanson in December 2004. Figure 2 below shows the diagram of the Fraud Diamond Theory.

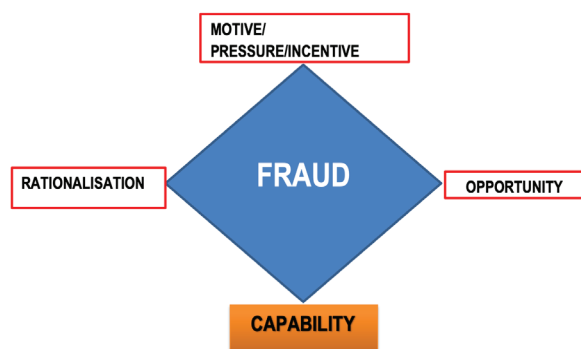


Figure 2 – Fraud Diamond

Some people possess a mindset that they could commit ethical violations or break the law without having any sense of guilt or stress. The mindset traits that support such capability include position, intellectual capacity, ego, coercion, deceit, and stress management.

Position /Function (Role)

The position or the fraudster’s function in an organization plays a crucial role in the capability for them to commit a fraud. Most of the fraud in the workplace occur because the employee has an exemplary ability to commit the fraud. They usually have knowledge on organisational policy, existing internal control, and security weakness and use them to commit a fraud. One of the critical factors in enabling someone to commit fraud is the function or position he/she holds in an organisation. Many scams occur when the right people are placed there with the ability to commit fraud. An employee who holds a certain position and function in the organisation may have the opportunity and capability to breach the organisation’s trust.

Intelligence/Creativity and Ego

A fraudster is typically someone who understands the internal control’s weaknesses and can exploit these weaknesses by using their position, function or authorised access. According to the Association of Certified Fraud Examiners (2003), 51% of the criminals of occupational fraud had at least a bachelor's degree, and 49% were over 40 years old. Also, managers or executives committed 46% of fraud, based on the Association's recent study (Rabi'u Abdullahi and Noorhayati Mansor 2015). Usually, the fraudster has a heightened ego, and they believe that nobody will notice the scam that they are doing. They also assume that they could easily get out of it if they ever get caught due to their high position.

Coercion, Deceit and Stress

Coercion and deceit are methods where the individuals can influence others to assist or conceal the fraud, and the fraudster is able to lie or divert convincingly. A fraudster usually has a very persuasive personality in order to convince others to go along with the crime. A common personality trait of these preparators is asserting themselves as “bully” to people that work below their hierarchical position. They would make unusual and significant demands by instilling fear into them. The preparators, on the other hand, do no respect and they avoid being subjected to the same rules and procedures as others (Wolfe and Hermanson 2004:41). According to Wolfe and Hermanson (2004) and Rudewicz (2011), a successful fraudster could lie effectively and consistently. They could lie to the higher authority such as investors and auditors convincingly without

being suspected. They also have to be cunning and smart in order to keep track of their lies so their storyline remains consistent.

Furthermore, a vital characteristic of a fraudster is the ability to handle immense amount of stress because committing a fraud and managing a scam over a long period of time can be stressful. A fraudster has to be smart to maintain their calm and keep their act concealed to avoid detection.

The impact of high-level fraud can affect an organisation in several ways such as financial impact, deterioration of reputation and employee morale. The main consequence of fraud is loss of funds or equipment followed by damage to reputation. This may negatively impact long term reliability and deter future clients and customers. In addition, fraud committed at the highest hierarchical could damage internal trust of existing employee.

In conclusion, by understanding the reasoning behind a fraud using the Fraud triangle theory, an organisation should be able to cultivate good practice and measures to deter and detect frauds.

An organisation must establish and maintain internal controls specifically designed to prevent and detect fraud before it is too late. It can conduct regular audits in high-risk departments such as financial, procurement or inventory department.

Another method of preventing fraud from occurring is by implementing an information security management system (ISMS) in an organisation. Fraud can occur due to ineffectiveness of the current Information Security Controls which can be caused by the weakness in people, process and the technology governance as well as valuable business data. For instance, if an employee is able to alter the data, this may lead to a fraud meaning the basic information security principle of confidentiality, integrity, and availability has been breached. Therefore, key security control areas of data access and management are extremely crucial for fraud prevention.

An organisation can also establish strict hiring procedures to conduct a thorough background investigation on a prospective employee's educational and employment history. Training should also be provided to all employees on how to prevent fraud and they should be trained to be aware of the procedures for reporting suspicious activity by co-workers, vendors, or even customers. The organisation can conduct

regular audits in high-risk departments such as the financial, procurement or inventory department.

It is a challenge to manage fraud especially if the person committing is someone from a high hierarchical position within an organisation. The capability, which is the fourth element in the Fraud Diamond theory, states that hierarchical power such as position or role allows a person to abuse the privilege given in the company to commit a fraud. The person also has to have the confidence they can get away without being caught.

It is hoped that capability element will be used effectively to fight against fraud and as a step towards shifting from a trust-based model to a process-based model. For example, an organisation could take precautions and make sure that no one is in the Fraud Diamond category and also to create awareness among employees that fraud, by all means, is an ethical breach and a crime.

References

1. <http://www.businessdictionary.com/definition/fraud.html>
2. <https://www.lynxinvestigations.com/services>
3. <https://www.hrzone.com/hr-glossary/what-is-the-fraud-triangle>
4. <https://www.lexico.com/definition/rationalization>
5. Rabi'u ABDULLAHI and Noorhayati MANSOR (2015) *Fraud Triangle Theory and Fraud Diamond Theory. Understanding the Convergent and Divergent for Future Research*
6. Achen, Paris. "Expert Tells How to Spot, Prevent Elder Abuse." *Columbian, Columbian Publishing Company*, 14 Feb. 2014, p. C.1.
7. <https://kaufmanrossin.com/blog/5-methods-of-detecting-fraud-in-organizations/>
8. <https://www.greerwalker.com/look-employee-fraud-triangle-beyond/>
9. <https://www.haywoodhunt.ca/understanding-why-fraud-occurs-the-fraud-triangle/>

Malware On Android Is Not A Myth

By | Kamarul Baharin bin Khalid, Muhammad Edwin bin Ambo Rifai, Ahmad Aizuddin Aizat bin Tajul Arif

Malware attacks are progressively becoming a real threat on Android devices. Malware or any potentially harmful application (PHA) labelled by Google has been haunting Android users for quite some time now. While most PHAs are not harmful, some do have malicious intention of abusing permission or worse, stealing a user's data especially online banking related credentials or two-factor authentications (2FA).

This becomes increasingly dangerous for victims with rooted devices as it provides a leeway for the hackers to install a more malicious code that carries the ability to control the victim's device. Figure 1 shows an increasing number of users who have been attacked by stalkerware.

Victims with rooted devices are exposed to even higher risks as they are more vulnerable to malicious features including ability to control a victim's device.

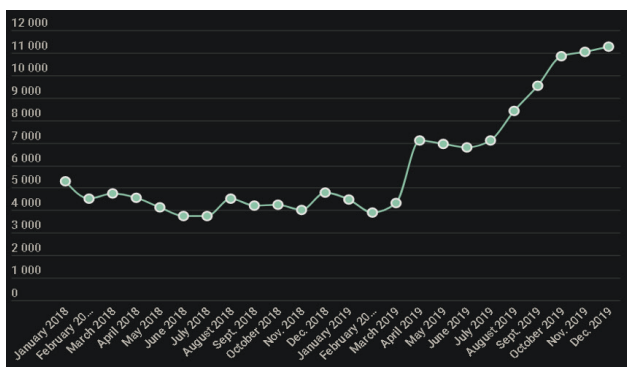


Figure 1: Number of unique users attacked by Stalkerware in 2018–2019

(Source: <https://securelist.com/mobile-malware-evolution-2019/96280/>)

Types Of Potentially Harmful Application (PHA)

Google has categorized these PHA based on motives, functionalities, and damages caused by malware once it has penetrated a user's device. The categories are as follows:

1. **Backdoor:** Allows the execution of unwanted, potentially harmful, remote-controlled operations on a device.
2. **Billing fraud:** Automatically charges the user in an intentionally deceptive manner.
3. **Commercial spyware:** Transmits personal information from the device without any notice or consent and it does not display any notifications regarding this occurrence.
4. **Denial of service:** Executes, without the knowledge of the user, a denial-of-service (DoS) attack or is a part of distributed DoS attack against other systems and resources.
5. **Hostile downloaders:** While it is not harmful on its own, but hostile downloaders bring other PHAs into a user's device.
6. **Non-Android threat:** This does not cause much harm to the Android user or device but contains components that are potentially harmful to other platforms.
7. **Phishing:** Pretends to come from a trustworthy source, which requests for user's authentication credentials or billing information, and then sends the data to a third-party.
8. **Elevated privilege abuse:** Compromises the integrity of a system by breaking the application's sandbox, gaining elevated privileges, or changing or disabling the access to core security-related functions.
9. **Ransomware:** Takes partial or extensive control of a device or data on a device and demands that the user makes a payment or perform an action to release control.
10. **Rooting:** Roots a device and execute other actions that apply to other PHA categories.
11. **Spam:** Sends unsolicited messages to the user's contacts or uses the device as an email spam relay.
12. **Spyware:** Transmits personal data off the device without notifying and getting consent from the user.
13. **Trojan:** Appears to be benign, but it performs malicious actions against the user.
14. **Uncommon:** Classified as uncommon if

Google Play Protect does not have enough information to clear them as safe.

Due to increasing malware threats on Android devices lately, it is highly recommended to only install applications from Google Play Store and only download trusted applications. Downloading applications illegally or from an untrusted source remains the primary means for distribution of PHAs.

Why Trusted Sources

While Google Play Store may not be perfect, it is still the safest and trusted available means of application installation platform for Android ecosystem. Other mobile phone manufacturers may also have their own trusted app store. So why trusted sources?

1. Applications hosted checked by Google security team

Google has teamed up with other security companies to help identify malicious applications before they are published on Play Store to avoid the potential harm for Android users. All Android applications must undergo rigorous security testing before it can be published on Google Play Store. Google goes to the extent of screening every application developer and does not hesitate to suspend those who violate their policies.

2. Google removes any app found suspicious

Google Play Protect is a software created by Google to automatically scan various applications every day in order to remove any suspicious applications. While there is certainly room for improvement, Google is constantly learning and improving on its protection software.

What Is Google Play Protect?

Google Play Protect is a malware protection service developed by Google and deployed on the Google Play Store. It is also made available on every Android device by default. This is to protect Android users from downloading malicious applications.

1. Anti-malware by Google

This is one of the services provided by Google Play Protect to verify the applications. This service scans devices every day for any known

signature of PHA. A warning will then be displayed for the users to respond when Google Play Protect detects a violation of malware policy. This is to let the user know that a PHA has been found and prompts the user to remove the application before any malware infects their device. In cases where the PHA has no benefit to the users, Google Play Protect can remove the PHA from infected devices and block any future installs.

2. Integrated into Google Play Store

As mentioned earlier, Google Play Protect scans a vast number of applications every day. Through these daily scans, Google Play Protect is able to respond quickly to any detected threat and thus, reduces the user's device from being infected. About 93% of PHAs are discovered by the on-device daily scan. To conserve data transmission, these daily scans only contact Google servers to request a verification when a suspected PHA is detected.

Google Play Protect works in the background and only needs user interaction when a PHA is detected. Users can check when their device was last scanned and view the list of scanned applications in the Google Play Protect section of their Google Play application.

3. SafetyNet Attestation API

For application developers, the SafetyNet Attestation API is very useful as this anti-abuse API allows application developers to check for any security threats in the Android devices which their application is running on. The API is used as a part of the application's abuse detection system module that helps the developers determine if the device has any security issues. This application can help determine whether their servers are interacting with genuine and unmodified applications that are running on a trusted and an unrooted Android device.

This is extremely important especially if the application is handling sensitive information that includes the user's name, address, identification number, bank account number, or even dealing with payment methods.

Malware Infected Android App

Android phones can fall victim to malware, just as computers do. Malware creates glitches and slows down the user's device, thus making it difficult to use the phone.

The good news is that all applications installed on Android devices need user consent before installing. The bad news is that not all users are security savvy enough to detect malware from normal applications.

Attackers will always try to infect android installers with malware and share the installer. They just need to deceive a user into installing the malware by:

1. **Infecting a legit Android app with malware.** With this method, the users assume that they are installing or updating a legitimate application but it is unknown to the user that malware is also being installed in the background.
2. **Creating an interesting application and attaching it with malware.** With this method, the attacker makes a trendy application that appears to be interesting in order to attract users to install it. Once it has been installed, the malware will then be installed in the background.
3. **Creating a malware which will pop up as an application update.** When the user reads the pop-up notification, they would assume that they are installing an update, rather than a malware.

Due to its malicious behaviour, all malware cannot be hosted in Google Play Store. However, there are several ways that a malware can directly infect Android devices;

1. **Installed from a third-party app store.** Third-party app stores do not have any verification method to certify applications that are hosted on their server. Attackers can easily host their malware here.
2. **Installed from a direct link.** Attackers can subscribe to any web hosting or cloud services to host the malware on the platform. The service providers do not verify any application that is hosted on their server which means that the attacker only needs to share the link of the malware with the victim.
3. **Installed from a shared installer.** The attackers can share the malware installer files directly onto the social networking or social media platforms. Not all service providers will verify shared applications.

Things To Look For And Precautions

1. When purchasing a new Android smartphone, it is important to make sure that the Android operating system is the latest version. This will ensure users that their device is protected with the latest security update. To check if your device's Android version is the latest. Follow the steps below:
 - II. Open device's **Settings** app.
 - III. Go to **About phone > Software Information**
 - IV. The Android Version displayed will be the version used in the smartphone. The latest Android version is **10**.
2. Check if your device's security is up to date. Follow the steps below:
 - a. Open device's **Settings** app.
 - b. Go to **About phone > Security patch level**
 - c. The date displayed is when the last security update was released. Newer Android OS receives monthly security updates.
3. When installing an application, look out for any suspicious permission request. For example, there is no necessity for a calculator application to request for the Internet access which might be a malware installing pop-up. The figure below shows an example of the unnecessary permission requests.

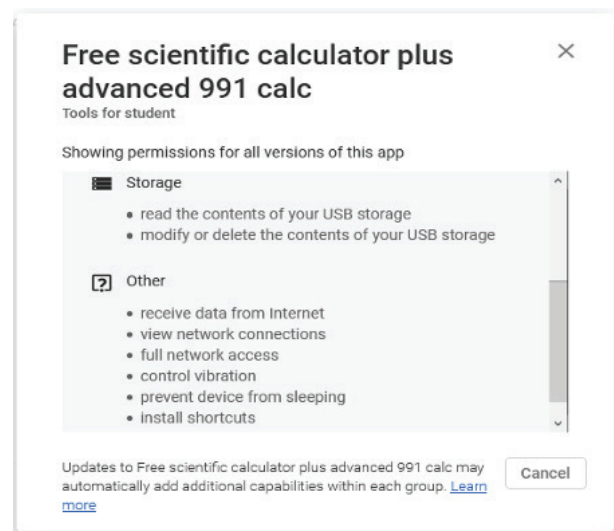
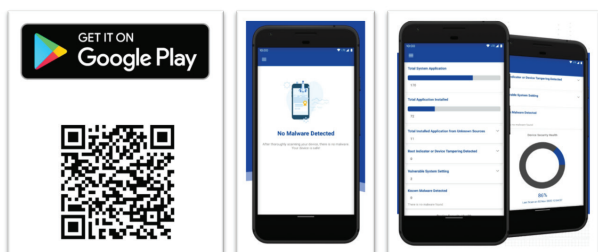


Figure 2: Example of Unnecessary Permission Request

4. When installing an application update, an error pops up when trying to overwrite the originally installed application. This means that the new update installer is not the original installer but a modified installer that is not approved by the original developer certification.
5. Only install applications from trusted source/App Store/Play Store. Do not install applications from a direct link or from a shared installer because a trusted source will vet through all applications for malicious malware.

Recommendation

1. Consider installing antivirus/anti-malware solutions that is offered in Google Play store for extra protection.
2. Install MASSA, Android application by Malaysia Computer Emergency Team (MyCERT) or CyberSecurity Malaysia to automate the Android devices' misconfigurations and risks identification. Reports that are generated by MASSA will be useful for a security analyst to help investigate any Android incident.



Conclusion

All Android devices with Google Play store are installed with a set of endpoint and mobile threat prevention services that protects the device against common threats. It is always running in the background to protect the user's device from malware and it has an automatic update with the latest bug fixes.

In general, Google Play Protect analyses all the applications that are newly installed and existing applications already on the user device in order to check if any app contains threats.

- Keeping device safe, 24 x 7
- Securing device even if it has been lost or stolen
- Scanning and verifying before installing an application
- Helping the users to navigate the Internet safely

References

1. Google Transparency Report - Android ecosystem security - <https://transparencyreport.google.com/android-security/overview>
2. Potentially Harmful Applications (PHAs) - <https://developers.google.com/android/play-protect/potentially-harmful-applications>
3. Malware categories - <https://developers.google.com/android/play-protect/phacategories>
4. SafetyNet Verify Apps API - <https://developer.android.com/training/safetynet/verify-apps>
5. SafetyNet Attestation API - <https://developer.android.com/training/safetynet/attestation>
6. App security improvement program - <https://developer.android.com/google/play/asi>
7. Cloud-based protections - <https://developers.google.com/android/play-protect/cloud-based-protections>
8. Google Play Protect - App Defense Alliance - <https://developers.google.com/android/play-protect/app-defense-alliance>
9. Stay Safe With SafetyNet Attestation API in Android - <https://www.netguru.com/codestories/stay-safe-with-safetynet-attestation-api-in-android>
10. MASSA in Google Play store - <https://play.google.com/store/apps/details?id=mycert.ctrc.massalite>

iPhone Bug Breaks Down Wi-Fi Features

By | Mohd Alif Erfan Bin Mohd Efendi, Ahmad Azizul Iqram Bin Musa

Introduction

The Internet has become a necessity in today's modern life. People connect to the Internet either through mobile data or Wi-Fi. However, when we are running low on mobile data, we tend to connect our device to any free and open Wi-Fi networks.

To avoid becoming the next hacking victim, it is not recommended to connect your devices to unknown open Wi-Fi networks. When you already have access to an open Wi-Fi, you are at risk. For example, hackers can distribute malicious script into your device and wreak havoc.

There is also another risk related to Wi-Fi connectivity. Based on recent findings, connecting to an unknown network through an iPhone can result in denial of service for the device.

Background

A newly discovered iPhone bug was found by Carl Shou on Friday, 19th June 2021. On his Twitter account, he posted a video about his phone not being able to connect to the Wi-Fi after he tried connecting it to his personal hotspot named "%p%s%s%s%n".

Apparently, the Wi-Fi on his iPhone was disabled and unable to connect at all for unknown reasons. Carl Shou stated that the issue happened on his iPhone XS running on iOS 14.42. According to the video, his iPhone's Wi-Fi features stuttered, trying to connect to other networks and then it disables the device's Wi-Fi. Shou tried to fix it by changing the SSID and restarting his device, but both options did not resolve the issue. [1]

Bleeping Computer, a website for technology related news also tested the newly found bug on iPhones that uses the latest iOS version - iOS 14.6, and the same issue occurred. The Wi-Fi feature cannot be used after trying to connect to a strangely named SSID on the Wi-Fi network.

Cause of Issues

Security researchers that saw Schou's tweet believed that the bug occurred because of an input parsing issue, likely a string format vulnerability. When a string with '%' symbols exist in Wi-Fi hotspot names, iOS may be mistakenly interpreting the letters following the '%' sign as string-format specifiers when they are not.

In C language, string format specifiers have a special meaning and are processed by the language compiler as a variable name or a command instead of plain text. For example, the '%s' is specified for string format and '%d' is specified for decimal in C language, which is often used with the printf and scanf function.

In this situation, the SSID has been named without any function before the '%' sign which may have caused this type of bug to occur.

When asked why Schou named his Wi-Fi hotspot with a 'unique' name, he said:

*"All my devices are named after format strings to f*** with poorly developed devices." [2].*

Security Risks

The newly found bug has the potential to become a security risk as it could allow hackers to launch free Wi-Fi hotspots to the public allowing iPhone users to connect to them and cause their device this type of problem. The bug could not be replicated on Android devices, therefore this is specifically for iOS operating system only.

Some security experts believe that the '%' character in the SSID confuses the operating system with programming commands or variables causing the operating system to be in an unusual state.

Jake Moore, cybersecurity specialist at ESET said:

“Although iOS is extremely intelligent, the ‘%’ character can trip up an operating system by confusing it into thinking it’s an alter command from another language. Luckily this bug isn’t permanent but with a devilish mind, malicious actors could exploit those who click on it and take advantage of their situation.” [3].

New Net Technologies, Dirk Schrader stated that format string bugs are very common and also a major issue in web applications development. He also stated that string handling is one of the first lessons any developer learns before developing a system.

Schrader explained that this bug can be exploited because a system that is unable to process a given string correctly will end up in an undefined state. The outcome of this undefined state will mostly lead to resetting the application or the device.

Some experts disagree that the bug’s potential can be used as an exploit. China-based security researcher, Zhi Zhou wrote about this format string bug. He stated that he does not believe this bug is exploitable to achieve code execution because it requires users to connect to Wi-Fi hotspots to trigger the bug.

Following the statement by Zhi Zhou, Schrader refined his earlier statement and agreed with Zhi Zhou saying that this is “a funny exploit and embarrassing for Apple, but not exploitable.”

Hank Schless, senior manager of security solutions at Lookout, stated that it is still early to decide whether the bug found is exploitable or not. But from a consumer’s point of view, there is nothing to be worried about for the time being about this bug. Schless also reminded users to keep their iPhone updated as most software updates today focusses on fixing security bugs [4].

How To Fix

As stated before, simply restarting the iPhone will not fix this issue. Luckily the bug is not permanent and can be fixed without having to reset the entire device.

The good news is that the fix to resolve this newly found bug does not require a lot of steps. One simply needs to reset the network settings on iPhone by going to Settings > General > Reset > Reset Network Settings. This will reset all the network settings back to default and restart the device. Once the device has restarted, the user can reconfigure the Wi-Fi settings again [2].

Conclusion

The bug in iPhone on SSID string format vulnerability can lead to Denial of Services (DoS) attack as it does not allow the user to use any Wi-Fi features after trying to connect to the SSID named “%p%s%s%s%s%n”. DoS prevents users from accessing certain features on the devices. In this situation, Wi-Fi services were disabled after connecting to the unique SSID.

It is recommended that iPhone users avoid connecting to random Wi-Fi hotspots especially those with the % character. In general, it is a best practice for all of us to avoid any unknown hotspots to ensure our device is secured. If possible, always use a VPN connection for optimum security.

For Wi-Fi providers, it is suggested to avoid using special symbols, specifically the character ‘%’ in the SSID to prevent any security incident towards Wi-Fi users using an iPhone.

In addition, newly found bugs will always have the probability to be exploited by hackers unless security patch update is available from the developer. It is advisable to always update your software with the latest security features to keep your device and software more secure.

References

1. C. Schou, *Twitter.com*, 19-Jun-2021. [Online]. Available: https://twitter.com/vm_call/status/1405937492642123782.
2. A. Sharma, “iPhone bug breaks Wi-Fi when you join hotspot with unusual name,” *BleepingComputer*, 19-Jun-2021. [Online]. Available: <https://www.bleepingcomputer.com/news/security/iphone-bug-breaks-wi-fi-when-you-join-hotspot-with-unusual-name/>.
3. K. O’Flaherty, “New iPhone bug breaks your Wi-Fi: Here’s the fix,” *Forbes Magazine*, 20-Jun-2021. [Online]. Available: <https://www.forbes.com/sites/ka-teoflahertyuk/2021/06/20/new-iphone-bug-breaks-your-wi-fi-heres-the-fix/>.
4. L. Vaas, “iPhone Wi-Fi crushed by weird network,” *Threatpost*, 21-Jun-2021. [Online]. Available: <https://threatpost.com/iphone-wi-fi-weird-network/167075/>.

Cyber Insurance: Review Of Proposal Assessment Questionnaire

By | Shaifullah Bin Mat Swadi

Cyber insurance is pivotal for the survival of digital dependant business operations. With the great reset of global reliance on online e-commerce platforms worldwide ever since the onset of Covid-19 pandemic, cyber insurance has become a necessity for companies to operate efficiently. Based on Organisation for Economic Co-operation and Development (OECD), the cyber insurance market size in 2016 was estimated to be in the range of USD2.5 billion to USD 3.5 billion. The market size is projected to grow at around 20-25 percent annually, reaching USD20 billion in premiums by 2025 (Paul, Matthew , Matthew, & Arturs, 2017). Hence, it is imperative to ensure companies procure accurate cyber insurance premiums to protect against business operation exposure. Proposal questionnaire forms are the main assessment method for cyber insurance providers to evaluate companies' cyber security posture. This is in accordance with findings by a study that self-assessment questionnaires presented client function in assessing their security posture (Sasha , Lillian, Andreas, & Therese, 2019).

An in-depth understanding on the questionnaires by the Malaysian cyber insurance companies is vital for the cybersecurity industry business' ecosystem in supporting the pre and post cyber insurance procurement cycle. This paper dives in to review the list of questionnaires by two local insurance carriers on policy writing and premium price. Similar studies on proposal questionnaires based in UK and US by Woods et al (Woods, Agraftotis, R.C Nurse, & Creese, 2017) provides an insight on what to look out for in the proposal forms provided by local cyber insurance companies.

Among the 22 licensed insurance companies and takaful operators sanctioned by Bank Negara Malaysia (Licensed Insurance Companies & Takaful Operators, 2021), only four companies offer cyber insurance. Table 1 depicts two companies that provide proposal forms via online: AIG Malaysia Insurance Berhad and Chubb Insurance Malaysia Berhad. Both proposal forms are available for download via public domain from <https://www.aig.my/business/products/financial-lines/cyber-insurance> and <https://www.chubb.com/my-en/business/cyber-insurance.html>.

No	Company	Ownership	Submission
1	AIG Malaysia Insurance Berhad	Foreign	Manual
2	Chubb Insurance Malaysia Berhad	Foreign	Manual
3	MSIG Insurance (Malaysia) Bhd	Foreign	To Contact
4	Tokio Marine Insurance (Malaysia) Berhad	Foreign	To Contact

Table 1 Licensed Insurance Companies Offering Cyber Insurance

Cyber insurance is pivotal for the survival of This paper compares questionnaires provided by AIG and Chubb to review the variety of data collection required by the companies. Briefly, both proposal forms (in line with the practices of most companies) employ self-assessments as part of the underwriting process (Rainer, Stefan, & Markus , 2019). This is to reduce uncertainties by considering the existing accumulation aspects and developing adequate pricing approaches

(Dirk, Tino, & Johann, 2020). Review on this matter is vital because all parties involved in providing cyber insurance are interested in an efficient assessment process. Some clients tend to provide as little data as possible which poses a challenge. However, if too much data is requested, potential clients may choose a competitor. On the contrary, if too little data is requested, it may increase the risk to the insurers (Arnau, Ioannis, Louise, & Jason, 2020).

Findings

Table 2 reveals the spectrum of differences in terms of general and subtopic proposal questionnaires between AIG and Chubb. AIG questionnaires are straightforward with five main sections covering company information, data protection procedures, data access & recovery, outsourcing activities, and claims information. Briefly, the questions probe general practices and controls with regards to information security that the proposer (applicant) have in place. In the data protection procedures sections, key questions include data protection policy availability, compliance (staff), compliance (legislation), policy review cycle and availability of dedicated responsible staff in this domain which falls under process category.

In data access & recovery section, the inquiry covers more on technological implementation in preventing unauthorized access from external networks and computer systems within internal networks. The questions also found on type of tools, equipment, controls, ecommerce modules, encryptions requirements, backup, and recovery procedures. Remote user authentication is also covered in the list of queries. In the outsourcing activities section, the questions focus outsourcing of network, computer system or information security of the company processes, indemnification, compliances, and equipment. Lastly, the claims information section touches on company history (if any) with regards to investigation or audit in relation to data protection by a data protection authority and other relevant issues.

AIG MALAYSIA INSURANCE BERHAD		CHUBB INSURANCE MALAYSIA BERHAD	
# QUESTIONNAIRES		# QUESTIONNAIRES	
1	Company Information	1	Details of Applicant
2	Data Protection Procedures	2	Details of Business
3	Data Access & Recovery	3	Information Systems
4	Outsourcing Activities	4	Information Security (IS)
5	Claims Information	4.1	Security Policy and Risk Management
		4.2	Information Systems Protection
		4.3	Network Security and Operations
		4.4	Physical Security of Computing Room
		4.5	Outsourcing
		5	Personal Data Held by the Organisation
		5.1	Type and Number of records
		5.2	Personal Information Protection Policy
		5.3	Collection of Personal Data
		5.4	Personal Information Protection Controls
		6	Insurance History
		7	Claims Experience
MONETARY ELEMENT		MONETARY ELEMENT	
# Desired coverage based on benefits		# Request (range) insurance coverage	
1	CyberEdge	1	Limit of Insurance Required
2	Cyber Extortion	2	Excess/Deductible Requested
3	Media Content		
4	Network Interruption		

Table 2 List of Proposal Questionnaires

Chubb questionnaire covers detailed probing with majority through a yes or no answer option with a combination of small numbers of qualitative objective answer scheme. The main sections are details of applicant, details of business, information systems, information security (IS), personal data held by the organisation, insurance history and claims experience. In the Information Security (IS) section, there are five* subcategories, which

are security policy and risk management, information systems protection, network security and operations and physical security of computing room. While in the personal data held by the organisation section, it is sub divided into four subcategories, namely type and number of records, personal information protection policy, collection of personal data and personal information protection controls. In the details of business section, the question is

specific to the business operations with probing question on e-commerce activities if any. Among the highlighted question is the outage period before adverse impact on the company's business. Such question provides valuable input for assessment in policy writing and premium pricing. In the information systems section, the proposer must provide the number of end points and website service with e-commerce elements (if any) together with the revenue share from e-commerce. Majority of proposal questionnaires reside in the information security (IS) and personal data held by the organisation section. In the information security (IS) section which consists of five subcategories, the list of questionnaires consists of policy, processes, audits, staff trainings, risk management availability, information system protection and network security as well as operations technologies. The yes or no options provide an easy quantitative assessment to produce the required result for premium pricing. This section also covers physical security of computing room capability with active/passive architecture and consists of details of outsourcing operation that also covers Service Level Agreements (SLA) for incident and change control and penalties in case of noncompliance with the SLA. Details of asset and service that is outsourced with a yes or no option together with objective answer options provides a thorough landscape of the outsourcing philosophy. The personal data held by the organisation section is subdivided into four subcategories covering complete probing of the viewpoint of how the proposer or applicant company manages personal data. But what really differentiates this section is a question on the number of records that need to be insured which is further subdivided into six main region and categories/property of personal data that consists of commercial, financial and health data segmentation. In the following sections, the questionnaire covers personal information protection policy subsection which comprises policy formalization, awareness training, confidentiality agreement, monitoring, audit, and data breach response plan. The questionnaires focus on understanding the type of sensitive or confidential information that an applicant collects, stores and processes. While in the insurance history section, the probe is quite simple with enquiry on whether proposer has similar insurance along with details and status of coverage. Lastly, the claims experience section traces the company history (if any) with regards to lawsuits or any potential claim and relevant disciplinary action or investigation by any authority.

Conclusion

AIG and Chubb questionnaires portray substantially different approach in data collection. Simplicity seems to be the overall approach for AIG questionnaires, while Chubb chose a more rigorous regime. Despite the differences, the questionnaires seem to provide one common purpose, which is to provide insight into the security technologies and management practices (Sasha, Lillian, Andreas, & Therese, 2019). One similarity is request for required monetary coverage by the clients with direct coverage option for AIG. In Chubb's case, the coverage is very objective and customised. The extreme difference seen from data collected through the questionnaires were also reviewed by James Sullivan and Jason R C Nurse; in which they highlighted that one area that requires further examination which is the varying approaches that these cyber insurers take to assess cyber risk within organisations. While some may take a high-level strategic approach to risk management (such as audits or questionnaires), including the use of a variety of cyber risk-management frameworks, other cyber insurers may take a more technical deep dive into the risk held within an organisation (James & Jason, 2020). This extreme varieties in questionnaires also conforms to the findings by a report done by the European Insurance and Occupational Pensions Authority. According to the report, one widely recognised difficulty for the cyber industry is the lack of commonality in risk assessment language, which becomes evident in various aspects from coverage to underwriting questionnaires (Understanding Cyber Insurance A Structured Dialogue with Insurance Companies, 2018). Moving forward, it is crucial to have a standard guideline on minimum threshold for cyber insurance proposal questionnaires to cover the three main cybersecurity elements: people, technology, and process. This is to enable cyber insurance solutions to stay dynamic in the industries. There must also be systems in place to capture data and design platforms where data can be easily searched and analysed (Arnau, Ioannis, Louise, & Jason, 2020) to compensate for extreme variation in questionnaires between cyber insurance providers. Other related potential research is how to balance between acquiring data from client and securing cyber insurance business in the context of risk assessment that allows visualisation of the probability of occurrence and extent of damages due to cyber risks (Dirk, Tino, & Johann, 2020) in pricing the cyber insurance premium accurately.

References

1. Arnau, E., Ioannis, A., Louise, A., & Jason, R. (2020). *The Data that Drives Cyber Insurance: A Study into the Underwriting and Claims Processes*. 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA).
2. Dirk, W., Tino, S., & Johann, M. (2020). *Affirmative and silent cyber coverage in traditional insurance policies: Qualitative content analysis of selected insurance products from the German insurance market*. *The Geneva Papers on Risk and Insurance - Issues and Practice* (2020) 45, 657–689.
3. James, S., & Jason, R. (2020). *Cyber Security Incentives and the Role of Cyber Insurance*. Royal United Services Institute for Defence and Security Studies.
4. *Licensed Insurance Companies & Takaful Operators*. (2021, 7 29). Retrieved from Bank Negara Malaysia: <https://www.bnm.gov.my/general-business>
5. Paul, M., Matthew, S., Matthew, M., & Arturs, K. (2017). *Seizing the cyber insurance opportunity*. KPMG.
6. Rainer, B., Stefan, L., & Markus, R. (2019). *A Fundamental Approach to Cyber Risk Analysis*. *Variance* 12:2, 161-185.
7. Sasha, R., Lillian, A., Andreas, K., & Therese, J. (2019). *Content analysis of cyber insurance policies: How do carriers price cyber risk?* *Journal of Cybersecurity* 5(1).
8. (2018). *Understanding Cyber Insurance A Structured Dialogue with Insurance Companies*. Luxembourg: Publications Office of the European Union.
9. Woods, D., Agrafiotis, I., R.C Nurse, J., & Creese, S. (2017). *Mapping the coverage of security controls in cyber insurance proposal forms*. *Journal of Internet Services and Applications*, 8:8.

Fintech: Risk And Security Perspectives

By | Sharifah Nurul Asyikin Binti Syed Abdullah, Sarah Khadijah Taylor, AkmalSuriani Binti Mohamed Rakof, Ummu Ruzanna Binti Abdul Razak, Nur Syahirah Binti Azhar

With the recent technological developments and advancements, we would like to provide an overview on Financial Technology to all readers, with the aim of addressing an increasing numbers of cybercrimes in Malaysia.

What is Financial Technology? Financial Technology, also known as “Fintech”, refers to the intergration of technology in offerings by financial services companies. Over the years, Fintech has revolutionized traditional financial services, products and services. It involves alternative financial services built by startups that would eventually disrupt the existing, traditional financial system.

In today’s technology, Fintech is easily and readily accessible via smartphone, through the Internet and various applications. Following are several Fintech services that are extensively used globally.

a. Mobile Payment

Due to its convenience and user friendliness, mobile payment is the favourite among users. e-Wallets such as Touch and Go, Boost and Shopee coin is an example of mobile payment. It provides the users options to either pay over the counter or online using such applications. By using such mobile applications, users no longer need to carry a lot of cash with them. At the same time, there are also features to collect points and redeem rewards when they transact using mobile payment.

b. Crowdsourcing

Crowdsourcing such as Kickstarter, Patreon and GoFundMe are platforms used by stakeholders to collect fund for investments in various projects. This mostly benefits startups or founders as they are only required to upload their proposal and projects on the platform and launch it to gain interest.

c. Cryptocurrency

Cryptocurrency such as Bitcoin, Ethereum and Tether is a unique and highly secured Fintech. It is a digital or a virtual currency managed by the

Internet users by leveraging on cryptography technology. Its transactions are transparent, and the integrity of the transactional data are publicly visible among blockchain explorers. However, the identity of the senders and receivers remain private, which distinguishes it from traditional currency.

d. Stock Trading and InsurTech

Stock trading such as Robinhood, Binance and TradeStation is another form of Fintech platform for services to trade stocks without paying any commission. It provides RoboAdvisor services for users to request free consultancy according to individual risk appetite.

InsurTech such as ChatBots, Mobile Apps, iMoney and FatBerry is an innovation that can enhance user experience in the insurance industry. Insurance company leverages on technology such as artificial intelligence, wearable device, and smartphone applications to facilitate insurance operations which eventually reduces the operational cost. Fatberry for instance, enable users to compare insurance prices.

What are the advantages of Fintech?

Fintech provides similar services as the banks through a different platform. Users can easily download various Fintech applications and use it like a bank account where all transactional activities take place. It is also an alternative financial service which benefits individual without a permanent address or individuals that have lost access to financial institutions due to bankruptcy.

Cryptocurrency platforms such as Binance and Huabi provides cryptocurrency loan services to borrowers without a fixed income who previously faced difficulties applying loan from the banks.

In Kenya, M-Pesa, a mobile payment application, enables small businesses with a limited access to financial institutions, to send and receive money. It also accommodates users without

transport, facilities and staying in remote areas to continue doing business by performing transactions through the application.

In addition, Fintech offers reward points that can be redeemed through applications such as Shopee coins and Setel Petronas.

What is the RISK when using Fintech?

The three main risks using Fintech: losing money, data breach and product or services that do not meet expectations.

a. Loss of Money

According to recent statistics by Royal Malaysian Police (PDRM), from 2017 to June 2020, cryptocurrencies reported RM400 millions loss with the highest 32%, related to illegal investments which involved BitKingdom and Bitcoin Actionnode. Other cases include ransomware, crypto wallets hack and illegal cryptos trading.

BitKingdom is a platform to invest in Bitcoin. Initially, investors are guaranteed a high return in investment. However, once they have invested through the platform, the provider would convert Bitcoin to Aereus currency of no value. Over 100 investors were scammed by the provider with a total loss of RM30 million. Next is Fintech Gold, which was another platform investing in cryptocurrencies that started its operation in April 2020. Investors were promised a 10-15% return monthly, which can be monitored via the platform. In December 2020, investors had reported they were unable to access the platform. An estimated RM2.8 million was lost to this scam.

b. Risk of Data Breach

Data breach happens when irresponsible site or application providers share or expose personal information such as username, password, transactional record, house address, IC number or even personal photos to public without an individual's consent. Such act leads to an increase in phishing email or spam messages, causing the social media or mobile applications that is storing sensitive information to be susceptible to cyber-attacks.

c. Risk of Product or Services Not Meeting Expectation

Today, online shopping has revolutionized the way we shop. It is convenient and saves a lot of time. Yet, users need to be cautious when registering on these online platforms. Buyers should avoid buying from unregistered platform or unauthorized sellers to avoid being scammed as they are not monitored by any regulated bodies, so they are not obligated to fulfill users' expectations leading to unsatisfactory experience.

Fintech Safety Steps - Do's & Don'ts

a. Applications

Use Legitimate & Regulated Platform	
1	Download legitimate applications. For iPhone users, the automatic filters in the Apple Store can identify illegitimate application. For Android users, read reviews and application ratings before download.
2	Use regulated platform like Luno, T&G Wallet, Setel Petronas, Alipay and iPay88.
3	Conduct thorough research before using any unregulated platform.
4	Ensure service providers are registered with Suruhanjaya Syarikat Malaysia.
5	Ensure customer service and support is trustworthy.
6	Be prudent and vigilant in investment to avoid risk of losing money.
7	Be wary of scammers.

Use Application with Multi-Factor Authentication (MFA)	
1	When launching an application, ensure a password request.
2	When making transactions, ensure pin code is requested for security purposes.
3	Account verification is critical to verify any transactions.
4	MFA provides another security layer if the platform is hacked. With additional security pin code, hackers are restricted from accessing the account.

b. Smartphone

Ensure smartphone is free from virus	
1	A smartphone is similar to a computer, which is susceptible and vulnerable to viruses.
2	When the smartphone is infected by virus, users' details such as credit card information is modified and shared discreetly to other parties without consent.
3	Spyware is a malware installed on a computing device without a user's knowledge. It steals sensitive information and Internet usage data, and relays it to advertisers, data firms or external users.
4	To prevent virus threat on smartphones, CyberSecurity Malaysia developed a security application called MASSA , specifically for Android smartphones. It is capable to scan, detect and report any data breach on smartphones.

c. Internet

Do not use public WiFi to communicate confidential information and conduct transaction	
1	Public WiFi is not secure as it is widely accessible to the public including hackers.
2	Hackers are able to monitor and steal confidential information transmitted via public WiFi on devices to other parties without consent.

What is Our Readiness Level to Face the Risks?

a. Malaysia Government and Law

Malaysian government under the Ministry of Communications and Multimedia Malaysia (MCMC) has introduced various incentives under the Malaysia Digital Economy Blueprint to drive Fintech industry. The eRezeki program under Malaysia Digital Economy Corporation (MDEC) has enabled citizens, especially low-income groups, to generate additional income by doing digital work via online crowdsourcing platform. eRezeki participants are matched with digital work in line with their respective skills.

Fintech Booster, on the other hand, is a capacity building program by MDEC, in collaboration with Bank Negara Malaysia (BNM) to assist Fintech companies, local and foreign, to develop products and services via three strategically crafted modules, Legal & Compliance, Business Model, and Technology. This one-of-a-kind initiative is able to assist regulatory sandbox preparation for Malaysia. CyberSecurity Malaysia recently introduced Digital Upskilling Programme to Law Enforcement Agencies as well as universities students by offering certification training and capability program module to increase awareness and strengthen skills to participate in Digital Economy.

From an investigation perspective, Royal Malaysia Police (PDRM) has developed its own Cryptocurrency Unit to focus on cases involving Fintech. This unit has since actively investigated all cryptocurrency cases in Malaysia and several cases have progressed to legal proceedings.

Through these new platforms and initiatives introduced by the government, Malaysia is committed to expand and strengthen its competencies to ensure a healthier digital economy.

b. Users

Malaysians require more awareness programs to understand financial technology. Generally, we should keep abreast with local news and cyber security trends to learn about Fintech before enrolling, to avoid falling victim to scammers.

What is the Outlook for Fintech?

Fintech is a new technology that is being accepted globally. It leverages on artificial intelligence (AI) and data analytics making it a user-centric system. We believe that Fintech will continue to evolve over the years. However, users are advised to be cautious on Fintech trade-off risks and constantly learn about new technology. We hope this article provides an overview of financial technology to help users better understand its pros and cons.

Introduction To Money Laundering

By | Mohamad Hafiz bin Rahman

Introduction

Money laundering is the process by which criminals attempt to conceal the origin and ownership of proceeds from their illegal activities. Criminals attempt to convert the proceeds of their crimes into funds that appear to be of legal origin through money laundering. If successful, this process gives validity to the transaction committed by the criminal. Money laundering can range from a relatively simple process conducted locally or nationally, to a very sophisticated process that leverages the international financial system and involves many financial intermediaries over various jurisdictions. Money laundering is necessary for two reasons. First, the perpetrator attempts to disassociate from a crime that gives rise to the outcome of a crime (known as a predicate offence) and additionally, the perpetrator could use the outcome as if it was permissible by law. In other words, money laundering disguises the criminal origin of financial assets so that they can be used freely. Figure 1 below explains the process of money laundering.

Money Laundering Process

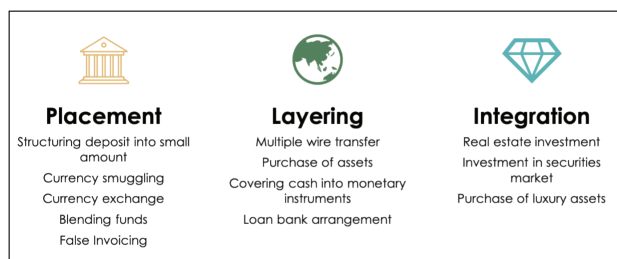


Figure 1: Process of money laundering.

1. Placement Stage

In the first stage, the launderer introduces the illegal profit into the financial system. This is the platform where the criminal breaks up a large amount of cash into less conspicuous smaller sums that are deposited into a bank account, or by purchasing a series of monetary instruments which will be collected and put into an account in another location.

2. Layering Stage

In the second stage, the money is converted or moved further from the original source by channelling it through the purchase and sales of investment instruments, or the launderer may simply wire the funds through a series of accounts at various banks around the world.

3. Integration Stage

In this final stage, the launderer will join a legitimate business economy. The most common example is where the proceeds are injected into a legitimate business that has a high percentage of cash sales such as investments, business ventures, and luxury assets.

Tactic And Technique

In each stage of the process, money laundering can use a variety of financial methods and instruments to disguise the illicit nature of the crime proceeds. The methods vary from purchase of simple luxury goods to more sophisticated techniques that involve transfer of money through transnational networks of banks and other financial institutions.

To deal with all illegal proceeds, money launderers can use financial or non-financial mechanisms, that is, institutions that (intentionally or unintentionally) participate in the money laundering process. The most commonly used method is to work through a banking institution, especially in the first stage of money laundering. Besides banks, other sectors were also used, especially financial intermediation, with a higher interest on invested capital leasing (the process of granting use or occupation of property during a certain period in exchange for the lease to be determined), and factoring (the practice of receiving accounts that can be accepted as a short-term loan guarantee). Other financial institutions, such as wire-transfer companies and exchange offices, are also often used to launder illicit profits.

Lastly, money launderers will use the gold market, casinos, and gambling houses. The instruments used for money laundering operations are also very wide ranging. Besides cash, the instruments most commonly used are stocks, life insurance policies, letters of credit, bank cheques, wire transfers, and precious metals.

Effects Of Money Laundering On The Economy

Money laundering damages financial sector institutions, which are essential for economic growth by promoting crime and corruption, which will ultimately slow economic growth and reduce efficiency in the real economic sector. Money laundering is the main problem not only in the world's major financial markets, but also in emerging markets. As emerging markets grow their economies and financial sectors, they are becoming ideal targets for money laundering activities. Money laundering also causes large fluctuations in international capital flows and exchange rates, as well as unpredictable changes in the demand for money.

In financial institutions, sudden changes can occur in the assets and liabilities of their financial position that are perceived to be used in money laundering. This will create risks for the institution. News of money laundering by these financial institutions may attract the attention of the authorities. In addition, audit pressure on these institutions will increase, and the reputation of those institutions will be damaged.

These illicit proceeds could dwarf government budgets of some developing market countries, leading to the loss of government control over economic policy. In certain situations, the sheer size of the laundered profits asset base may be leveraged to corner markets or even small economies.

Money laundering can also have a detrimental effect on currencies and interest rates as launderers reinvest funds where their schemes are less likely to be detected, while rates of return are higher. This could increase the threat of financial instability due to the misallocation of resources from artificial distortions in assets and commodities.

Money laundering will reduce tax revenue because activities taking place in the underground economy are undeclared. This has a negative impact on the economy as a

whole and gives illegal businesses an unfair competitive advantage over those operating legitimately. It will also result in reduction in tax revenues. If this income is low, it will raise the possibility that public revenues will not meet public expenditures, thus causing budget deficits.

Anti-Money Laundering (AML) In Malaysia

The Anti-money Laundering, Anti-terrorism Financing and Proceeds of Unlawful Activities Act 2001 (AMLA) is the primary statute governing the AML/CFT regime in Malaysia. The Act was gazetted as law on 5th July 2001 and came into force on 15th January 2002. The AMLA provides for the offences under money laundering and terrorism financing and the measures to be undertaken for the prevention of money laundering and terrorism financing offences.

The AMLA provides wide-ranging investigation powers, including powers for law enforcement agencies and public prosecutors to freeze and seize properties that are involved or suspected to be involved in money laundering or terrorism financing offences, and the power of the court to forfeit properties derived from the proceeds of serious crimes.

The maximum penalty for a money laundering offence under section 4 of the AMLA - *"any person who commits a money laundering offence and shall on conviction be liable to imprisonment for a term not exceeding 15 years and shall also be liable to a fine of not less than 5 times the sum or value of the proceeds of an unlawful activity or instrumentalities of an offence at the time the offence was committed or five million ringgit, whichever is the higher"*. In addition, not only money laundering will be punished, but failure to comply with anti-money laundering regulations will also be punished. In the case of minor non-compliance, the relevant regulatory agency may issue a warning letter to the relevant reporting agency. Although Malaysian banks and financial institutions are subject to anti-money laundering regulations, some institutions must also comply with anti-money laundering regulations. This is because these institutions have money laundering risks.

Conclusion

Money laundering has evolved to become a successful tool for criminals because the financial system failed to eliminate the possibilities. If

criminals were provided with the opportunity to make concessions, the system could be misused and abused. Financial transaction systems are designed to provide a more secure payment system for businesses around the world. It generates detailed and permanent records of all financial transactions. Regrettably, oversight standards, rules, and laws are not applied consistently and universally. Flexibility is the key to money laundering success. The lower standards and weak legislation found in many countries provide the needed flexibility for criminals to exploit the system to launder criminally earned profits. In conclusion, money laundering is not a profitable undertaking but a destructive one. Therefore, we must always be mindful of the consequences that we will face and never get involved in this crime.

References

1. *Malaysia Anti-Money Laundering & Counter Financing of Terrorism Regime. Aml/cft. (n.d.).* <https://amlcft.bnm.gov.my/AMLCFT02bi.html>.
2. *AML/CFT Law and Policy. Aml/cft. (n.d.).* <https://amlcft.bnm.gov.my/AMLCFT07.html>.
3. *Money laundering. IBA Anti-Money Laundering Forum.* https://www.anti-moneylaundering.org/Money_Laundering.aspx.
4. *LAWS OF MALAYSIA Act 613 Anti-Money Laundering and Anti-Terrorism Financing Act 2001*

SiberKASA Initiative During The Pandemic

By | Ruhama Bin Mohammed Zain

CyberSecurity Malaysia (CSM) is the national technical and specialist center for cybersecurity matters which currently comes under the Ministry of Communications and Multimedia. This article will describe how CyberSecurity Malaysia has contributed to the nation's cybersecurity including human capital development and is continuing to spur and nurture the training industry, especially during the present pandemic.

The Covid-19 pandemic has left many economies and nations in disarray. People have lost their jobs and companies are struggling to keep afloat. The series of lockdowns and slowed business activities have led to a series of retrenchments that affected many people. To add to the dire situation, hackers and cyber attackers have been taking advantage of the work-from-home situation by exploiting the new normal and the increased risk when people bring their work home. This causes the organization's security perimeter to expand to include the employee's home network. Clearly, now is not the time for the country to let its cybersecurity guard down.

CyberSecurity Malaysia has played a key role in setting up the SiberKASA initiative in order to ensure the cybersecurity of our country remains strong and resilient during this challenging time. SiberKASA is a holistic approach that covers the three components of people, processes and technology which should always be the basis for policy formation and strategic planning. It is an initiative aimed at developing, empowering, sustaining and strengthening cybersecurity infrastructure and ecosystem in Malaysia to ensure cybersecurity readiness.

The SiberKASA initiative also includes upskilling those who have been affected by layoffs caused by the economic downturn. These people will be offered cybersecurity training courses with the goal of providing them with new skills so that they may become employable again. The Global Accredited Cybersecurity Education Certification Upskilling is a skill enhancement training and cyber security capacity building programme. To date, there are 384 people who have successfully undergone cybersecurity training in diverse areas such as penetration tester, security operations center analyst, data security

analyst and others. The training is conducted through collaboration and partnerships with training providers from industry. By working together with training partners from industry, the SiberKASA initiative is directly contributing to generating economic activity in one segment of the industry. Recently, CyberSecurity Malaysia has upped the ante by introducing a special on-the-job training programme together with the possibility of industry job placement for people who have lost their jobs during the pandemic. By focusing on the human aspect, which is always the weakest link in cybersecurity, the SiberKASA initiative is addressing a very crucial element in ensuring cyber resilience.

Apart from training the cybersecurity technical workforce, the general public has not been left behind. The first Cyber Security Gallery in the country called CyberSAFE LiveGaleri was established with the goal of becoming a learning hub for products and services provided by CyberSecurity Malaysia. With the increased public awareness of products and services, it is hoped that the public will reach out to CyberSecurity Malaysia for advisory and technical assistance. This will significantly improve communication between the general public and government agencies which results in greater cyber resilience overall for the country. The CyberSAFE LiveGaleri also serves as a one-stop shop in CSM's effort to nurture cybersecurity awareness amongst primary and secondary school students through various interactive activities as well as functioning as a co-curriculum activity center under the Ministry of Education.

The next component of the SiberKASA initiative is a set of cybersecurity guidelines for the industry. There are seven guidelines developed to provide cybersecurity advice for both public and private sectors. These guidelines cover the current and future trends of cybersecurity growth areas.

- Industrial Control System Cyber Security
- Secure Software Development Lifecycle
- Internet of Things Cyber Security
- Fourth Industrial Revolution Cyber Security
- MyKad Enhanced Biometric Access (EBA)

Ecosystem Cyber Security

- Cloud Computing Usage Security
- Recommended AKSA MySEAL Cryptographic Algorithm

From the list of guidelines, we can see that they cover the whole gamut of present and near future cybersecurity pain points, including a niche but important area which is cybersecurity for the MyKad Biometric Access Ecosystem.

In addition to people (upskilling) and process (guidelines) components, the SiberKASA initiative also covers the technology component in the form of specific cybersecurity technological solutions. The list of products includes CamMuka 2.0 which is an automatic biometric facial recognition system for forensic use. CamMuka 2.0 uses machine learning developed through the combined expertise and innovation by CyberSecurity Malaysia. It enables facial matching between a sample picture in collected evidence against a picture of an individual under investigation through a combination of IoT devices and cloud computing processing.

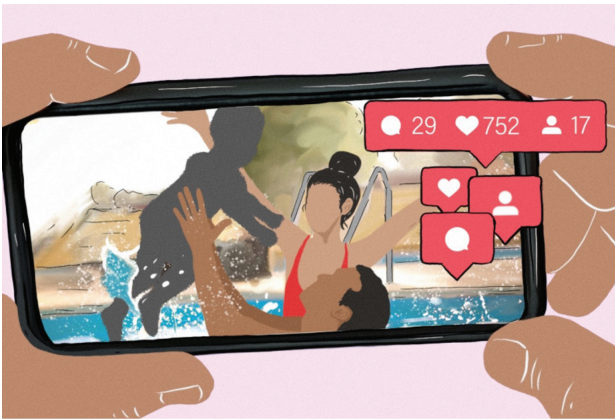
The SiberKASA was officially launched by the Honorable Dato' Saifuddin Bin Abdullah, Minister of Communications and Multimedia on 23rd March 2021 at Menara Cyber Axis, Cyberjaya. This underscores the full support from the ministry and government. Since the launch, the SiberKASA programmes have been carried out despite the challenges of Movement Control Orders and physical restrictions imposed by the SOPs. The SiberKASA initiative is well on track to meet its goals and objectives.

CyberSecurity Malaysia has demonstrated leadership and vision by initiating and leading the SiberKASA initiative throughout the inception, design and implementation phases. This is evidenced by the support from numerous external and internal stakeholders as well as the many technical experts involved in delivering the programmes, products and guidelines. It takes exceptional coordination and resourcefulness to pull all the elements and components together to realize the goals of this initiative.

To sum up, the SiberKASA initiative by CyberSecurity Malaysia is a collaboration and coming together of training providers, cybersecurity experts, educators, government agencies and the Malaysian public towards greater cyber resilience and information security for Malaysia.

Over-Sharenting: How Much Is Too Much?

By | Yuzida Md Yazid



Caption: Lil Sarah's first swimming session (location tagged, together with a photo of Sarah, the cute little girl). Click Post!

Sharing and documenting every bit of our lives has become a social norm, but how much is too much? This question becomes essential when it concerns parents and their posting habits about their children online. This habit is called 'sharenting' whereby parents obsessively share details about their children's lives on social media. Parents do not only share the photos of their children on the social media platform, but they also interact with other parents to discuss about parenting. These parents go to the extent of even documenting their child's first day of life after being born on social media. Now, even toddlers and infants have online presence. Unlike adults, children have limited ability to consent or object to their information being shared on social media. Some parents find it difficult to maintain control due to peer pressure from well-intentioned friends and family who share their children's pictures on their respective social media feeds.

The term sharenting, as mentioned above, is a term derived from the words '**share**' and '**parenting**'. It was defined by Stacey Steinberg (2017) in her paper 'Sharenting: Children's Privacy in the Age of Social Media' to refer to the manner in which many parents share details about their children's lives online. The phenomenon of sharing too often or too much of their children's lives on social media through the posting of text, images, photographs, and videos that convey personal information about their children is referred to as 'over-

sharenting.' The act of 'over-sharenting' by the parents, will unwittingly create a child's digital representation. Sharenting usually starts with sharing pictures of their children online, then followed by videos and status updates. Some parents share with good intentions, for example, in a support group, especially in children health-related groups. Some parents share their children's milestones to document memories. With sharenting, long-distance families who could not meet often always stay in touch. Despite these reasons, parents must be wise to know the limit on how much to share. However, how much is too much?

Is sharenting bad?

Since early last year, the world was struck by an ongoing global Covid-19 pandemic. As a result of the outbreak, many of us are now living in a new norm, being largely confined to our homes for a long period of time. Many have started to work from home. During this new norm, some parents turned to their children to produce social media content by pulling numerous pranks on them and documenting in video blogs (vlogs) that went viral online. Parents should always be aware that posting these embarrassing photographs and videos of their children might leave a negative emotional impact on them. The negative impact may not be immediate as their child may be too young to understand the effects and consequences. Parents must bear in mind that the pictures and videos that they find adorable, might not sit well with strangers who could post adverse comments about them.

Sharenting is also regarded to be an infringement on the child's right to privacy, which has been a rising concern. The protection of children's privacy is a subject that requires extra attention in this digital era, as excessive personal information on the Internet or online endangers a child's privacy. Some parents tend to record every single moment of their child and later share the photos or videos on social media. While some parents are aware that their children hate sharenting, they still continue the practice, citing their own right to share anything about their own children on social media.

Digital Kidnapping

The act of excessive sharing or overexposing by parents about their children's lives may pose several risks. These risks include interfering with a child's sense of privacy, as well as their safety. Digital kidnapping is one of the ways that could endanger them. Digital kidnapping occurs when a stranger steals a child's photo from the Internet and impersonates as the child or their parents by uploading it as their own. They will then share these photographs on their respective social media feed, rejoicing in the 'likes' and 'comments' that they receive. The most common reason for digital kidnapping is to expose private or sensitive information that will leave a detrimental mark on the child's life, such as making it difficult for them to get into college or exposing them to bullying. In rare circumstances, a kidnapper may impersonate as a parent and convince the followers that they are the child's parents. These impostors can then obtain information regarding the children by posing as a peer and utilize that information which may eventually lead to physical kidnapping.

Emma Nottingham in 'Dad! Cut that Part Out' used the term 'generation tagged' to refer to children who have been exposed on social media by their parents (Nottingham, 2019). As a result, many children already have a plethora of photos, videos, and updates about their everyday life on social media before they can even walk. Most parents will post hundreds of their child's photos before the kid turns five. These photos are usually accompanied by hashtags and location tags which can lead to the child's profile being tracked. This can be detrimental if the information falls into the wrong hands from pedophiles to kidnappers.

Sharenting – A Support System and a Coping Mechanism

Sharenting is a convenient way to keep in touch and for faraway family and friends to convey well-wishes and share information about the well-being of family members. With sharenting, parents can create a support network with other parents, to discuss parenting experiences, and how to solve common problems. They can even get some tips through sharenting that might help them improve their parenting skills. Sharenting tips can range from dietary tips, how to discipline kids, behavioral problems, and so on. Parents nowadays are open in discussing their children's health and parenting issues on social media. This shows that sharenting could

play an important role by helping parents access a support network.



Smart Sharenting

Although sharenting has become common nowadays, it does not mean that parents should neglect any safety tips. Below, are some safe practices that every parent should follow before posting any content about their children online.

1. Before posting on any social media platforms, make sure you understand and are comfortable with their terms of service.
2. Set all your social media accounts to private, so that only followers you approve can see what you share. If your account is public, set it to 'Restricted' or 'Closed Group' when sharing a personal post or photo.
3. Set up google alerts for your kid's name, and keep an eye on their online presence
4. Avoid sharing content with location information.
5. Avoid posts that show your kids in any state of undress or partially undressed.
6. Resist the urge to upload or share personal photographs that are too personal such as a child on a potty.
7. Avoid including hashtags such as #pottytraining #bathtime #nakedkids
8. Give older kids rights over images, quotes, and other information related to them.
9. Consider the potential impact a post could have on your kid's wellbeing— either present or the future.

10. Think about whether the material shared can be misused, not only in the present day but also in the future.
11. Always remember that once the material or information is shared, you will not have control over how it will spread.
12. Create family sharing guidelines with older children and stick to agreed-upon rules when posting.
13. Reduce the frequency of sharenting. Updates need not be daily.
14. Practice **ethical sharenting** - a collaborative process that involves parents and children making decisions together in weighing all factors, motives, and any specific needs.

Despite the risks of sharenting, it is hard to object to its use as we are living in a hyper-connected world. Moreover, sharenting is a great way to share the latest photos and milestones of the kids with our loved ones, especially during times when lockdown prevents traveling and visiting. It can also help update our children's development and progress to other family members. However, parents must always remain alert and refrain from over-sharenting which could jeopardize their children's safety. Parents who are aware of privacy concerns should prevent over-sharing information about their children on social media. As gatekeepers of their children's personal information, parents must decide and control what and how much information is safely shared and disclosed to the public.

Remember!

Any time you post images of your child, you just don't know who is seeing them and what they are going to do with it.

References

1. "Sharenting" Even When They Know The Dangers - Forbes <https://www.forbes.com/sites/jessicabaron/2019/07/29/vulnerable-moms-engage-in-sharenting-even-when-they-know-the-dangers/?sh=34373be24751>
2. Sharenting: Children's Privacy in The Age of Social Media <https://scholarlycommons.law.emory.edu/elj/vol66/iss4/2/>
3. Choi, G. Y., & Lewallen, J. (2017). "Say Instagram, Kids!": Examining Sharenting and Children's Digital Representations on Instagram. *Howard Journal of Communications*
4. Nottingham, E. (2019). 'Dad! Cut that Part Out!' Children's Rights to Privacy in the Age of 'Generation Tagged': Sharenting, Digital Kidnapping and the Child Micro-Celebrity' https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3602712
5. A Guide to Smart Sharenting: Controlling Your Child's Digital Footprint. <https://kinzoo.com/blog/child-safety-online/a-guide-to-smart-sharenting-controlling-your-childs-digital-footprint>
6. Azhar, A. N. M., & Md Salleh, A. S. (2021). Sharenting During Covid-19 Pandemic: Yay or Nay. *International Journal of Law, Government and Communication*, 6 (22), 159-167.

Purple Team: The Missing Piece To A Complete Puzzle

Muhammad Azri Rafiuddin bin Basri, Imran bin Hasnan & Lukman Hakim bin Abd Rahman

Introduction

Developing a viable cyber security monitoring practice has been a challenge. As attack surfaces become more complex, every organization needs to be more vigilant. However, the development of new technologies and software has definitely made cyber security monitoring much easier. A successful security monitoring work can be accelerated by utilizing the new purple team exercises. Organizations need a viable security monitoring practice that can be utilized for procedures and processes that are sustainable.

Purple teaming is a security methodology in which red and blue teams work closely together to boost cyber capabilities through continuous feedback and knowledge transfer. One of the foremost successful ways to find framework vulnerabilities and foil conceivable cyber threats is through the skills and expertise of both red teams and blue teams.

What is Purple Team?

Purple team is developed to help the security teams track the progress, viability and effectiveness of vulnerability detection, threat hunting and network monitoring by accurately simulating common threat scenarios of unused procedures that are outlined in order to anticipate and distinguish modern threats. Some organizations perform purple team exercises as a one-off focus engagement, whereby security goals, timelines, and key deliverables are clearly defined by the security team, with a formal process in evaluating lessons learned over the course of an operation. This practice includes recognising offensive and defensive shortcomings, outlining future training and technological requirements. An alternative approach within the security industry is to view purple teaming as a conceptual framework that runs throughout an organisation

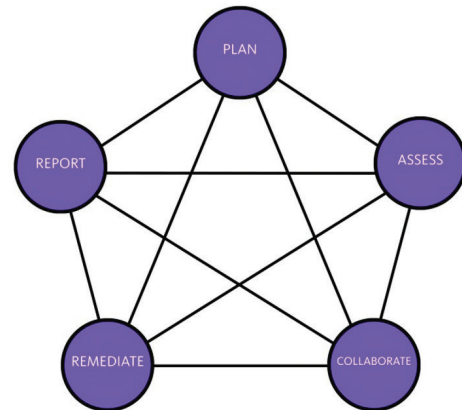


Figure 1.0: Activities of Purple Team

What are Red, Blue, And Purple Team?

A red team exists to attack, while the blue is to defend. The purpose is to fortify an organisation's security by learning from the resulting combat and getting ready when the real threat comes. A purple team is set up as an option to support the process. The red and blue team exercises can be extremely useful because it creates an opportunity to realistically challenge an organisation's defences.

Red Team

The red team is typically the independent security system of a company (target), and it is hired to covertly test its defences. The team comprises skilled ethical hackers whose objective is to distinguish and securely exploit vulnerabilities within the target's cybersecurity or physical perimeters. By mimicking sophisticated real-world threats, the exercise is highly realistic. A red team deploys bleeding-edge hacking tools and techniques designed to infiltrate the security systems and premises. This may expand to include writing malware and formulating modern techniques as noxious malicious hackers would do. Some organisations will be confident that their systems are hard to penetrate as they have a variety of vigorous security measures in place. But a red team only needs to find a weak link to break their perimeters apart. This could

include spear-phishing (social engineering) the employees or replicating the target's external services in a lab to discover zero-day exploits.

The red team objectives include:

- Compromising the target's security by extricating data, invading its frameworks or breaching its physical perimeters.
- Dodging detection by the blue team. Numerous attacks can occur over a transitory period of time, making it highly dubious for the blue team to neutralise any threat before the 'damage' is done.
- Exploiting bugs and weaknesses in the target's infrastructure. This highlights any gaps in the organisation's technical security that requires fixing, thus improving its security posture.
- Starting a hostile action - including sophisticated penetration testing - giving a reliable assessment of the blue team's defensive capabilities.

Blue Team

A blue team is typically stationed within a Security Operations Centre (SOC). The SOC consists of highly trained analysts who work on defending and improving their organisation's defences around the clock. The blue team is expected to detect, oppose, and weaken the red team. The mock assault situation is outlined to upgrade their aptitudes by preparing for a real-world attack. The blue team will detect and neutralise more advanced assaults and closely monitor any current and imminent dangers to pre-emptively defend the organisation.

The Blue team objectives include:

- Understanding each stage of an incident and responding appropriately.
- Noticing suspicious traffic patterns and identifying indicators of compromise.

- Quickly closing any indicator of compromise.
- Identifying the red team/threat actors' command and control (C&C or C2) servers and blocking their connectivity to the target.
- Undertaking analysis and forensic testing on diverse working frameworks their organisation's run, by utilizing third-party systems.

Purple Team

A purple team is not permanent as it provides transitory work to supervise and advance the red and blue team exercise. It is typically formed by security analysts or senior security staff within the organisation. If the red and blue teams work well together, a purple team may become redundant. It can be more of a concept than a function, driving the red team to test and target specific elements of the blue team's defence and detection capabilities.

The Purple team objectives include:

- Working alongside the red and blue teams, dissecting how they work together and prescribing any vital modifications to the current work out, or noting them for future reference.
- Seeing the big picture and accessing the mentality and obligations of both teams. For example, a purple team will collaborate with the blue team to audit how occasions are being identified. The team members at a certain point will move to the red team to address how the blue team's location capabilities can be subverted.
- Analysing results and overseeing necessary remedial actions, for example, patching vulnerabilities, implementing employee awareness training, and deriving maximum value from the previous exercises by applying, learning and then ensuring stronger defences.

	Blue Team	Red Team	Purple Team
Goal	Detect and mitigate cyber attacks	Test resilience against real attacks	Improve security posture
Scope	Entire organizations	Entire organizations	Predetermined systems employees
Test Method	N/A	Realistic simulation	Efficient improvement of security posture
Used Tools	EDR and SIEM	Sophisticated tools to remain undetected	Sophisticated tools to remain undetected and detection software
Tested Controls	N/A	Focus on detective and responsive controls	Focus on detective and responsive controls
Positioning	24*7, continuous	Periodically	Periodically

Table 1.0: Characteristics of blue team, red team, and purple team

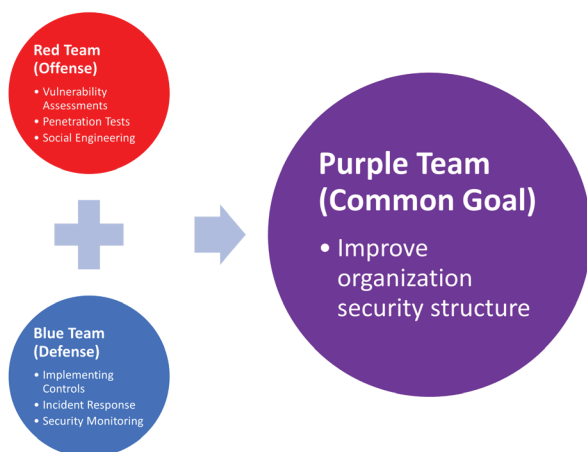


Figure 1.1: Relationship between the roles of Red, Blue and Purple teams

Impact of Purple team within an organization

The Purple team set up will benefit an organization. The team prepares and defends any threats that could leave an impact to the organization. For example, in some cases, a breach incident could take place by bypassing all defences, without having the blue team even noticing. This does not mean there is any lack in expertise or technology on the part of blue team, rather it demonstrates the complexity of an attacker's techniques and sophistication of their attack vectors. The purple team exists to eliminate such possibility. Red and blue teams work together and engage in a constant knowledge transfer to conduct simulation mimicking real life attack scenarios. The red team will help improve the organization's vulnerability management process, while the blue team helps in implementing controls, understanding attackers' mindset, creating and developing a better incident response programs and vulnerability detection processes. The ultimate goal for both red and blue teams is to improve an organization's security defences, in accordance with the organization's goal which is to foster a better, more robust cyber security culture.

The primary incentive of a strong purple team is to regularly communicate between the offense and defence (blue and red teams). The Purple team provides a constant flow of information and a symbiotic work that could be done properly in organization. In addition, a purple team does not have to be a newly assembled team. It can function as an exercise between the two existing teams. The most crucial aspect is to empower communication and collaboration between team

members, in order to advance the organization's cyber security culture consistently. One of the most important advantages of the purple team is that it can set up a viable security posture for the organization. Without the purple team's constant communication, standard security reviews, new defence techniques, threat hunting, vulnerability management, and development of improved security infrastructure and policies, organizations would not stand a chance against malicious actors. After all, each team works together to help the organization better prepare for any future cyber threat.

Best practice of Purple team in an organization

If an organization is looking to improve current red team and blue team practices, with the implementation of a purple team, there are several factors which they need to consider. The organization needs to make sure that everyone understands their roles. Communication and collaboration are key because it is important for both teams to share their findings and help each other. They should never expect the red teams to engage in full vulnerability management process or to hold the blue team responsible as expert hackers. Establishing clear roles and expectations for each team, while keeping communication open goes far in ensuring a successful and effective purple team methodology. To realize the benefits from these exercises, it is important to plan well before executing the purple team exercises. Start the plan by defining goals, work on improving security alerts, security policies and processes. However, the plan need not be fixed. Continuously allowing adaptation might uncover any shortcomings which were never considered or planned during a threat-hunting demonstration. However, do set objectives and goals that are measurable. In this way, at the end of these exercises, their effectiveness can be easily assessed. Last but not least, before implementing these security remediations, make sure to revise and verify them. The team exercises need to be tracked at each and every step of the way, with every task assessed before moving on to the next step. Always follow up with actions. Reviewing each moderation continuously will help each side learn from each other, help close out any gaps, and permit for prioritized remediation rules. This will alleviate the red team with less monotonous shortcomings and direct the blue team towards uncovering more complicated threats.

Summary

The purple team exercise can help improve the viability of effectiveness in vulnerability detection, threat hunting and network monitoring by accurately simulating common threat scenarios to anticipate and distinguish evolving threats, technology and knowledge. Understanding and applying the concepts of purple teaming can benefit all organizations. A common mistake committed by organizations in adapting and assembling a purple team is not fully understanding its position and role to fit in along with red and blue teams, making the purple team exercise redundant and expensive, as opposed to providing higher value benefits if executed with proper conceptual understanding. Many organizations are already familiar with red and blue teams and have started to observe and realize some gaps from the exercises. Therefore, it can be concluded that purple teams is the missing piece to complete the cyber security puzzle within an organization.

References

1. <https://danielmiessler.com/study/purple-team/>
2. <https://www.itlab.com/blog/understanding-the-roles-of-red-blue-and-purple-security-teams>
3. <https://securitytrails.com/blog/purple-team>

Information Technology (IT) Books For Babies

By | Nur Qurratu 'Aini Bt Rohizan and Lukman Hakim B Abdul Rahman

Introduction

Information Technology has become an important part of our lives bringing in unfathomable and unexpected changes. After the invention of the computer and the Internet, the world has changed significantly. Just a press of a button or a swipe can get you many things that you want. You can chat with those living miles away or communicate with people in different countries through video conferencing. You can even buy groceries and food from websites, just by sitting at home. Sharing knowledge and gathering of information has become much easier, faster, cheaper, and enjoyable. The major benefits of IT has made the world a much better place to live in. It is now clear that the introduction and education of IT knowledge at the early stages of human development can be critical in ensuring the advancement of human and machine to grow in parallel for the benefit of mankind in the future. This article intends to explore and review some of the reading materials designed for babies and infants, and also to understand the philosophies and concepts used in the books.

1. ABCs of the Web

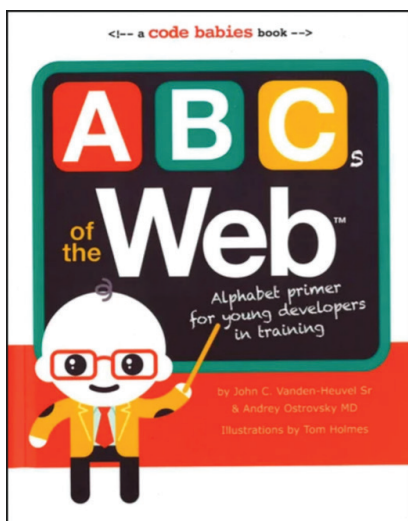


Figure 1: Front cover of ABCs of the Web

Written by a pediatrician and web designer, this book introduces basic coding and web concepts in alphabetical order with rhymes. For example on page 3: "C is for Cookie, Fade a C, Cascade with C,

What begins with C? Cookies store your page views, and track your activity". The book also mentions computer virus under the alphabet V: "V is for virus, Unlock a V, Block a V, What begins with V? Viruses are bugs that make computers cough and sneeze".



Figure 2: Content of the book

2. Web Colours



Figure 3: Web Colours book cover and first page with flap and RGB colours

From the same writer of ABCs of the Web, this book is about colour shapes and varieties that make up web-based programming language. The book is also interactive as it has flaps which encourage hand-eye coordination and good for fine motor skills. Also suitable for a baby who has developed object permanence.

RGB (Red, Green, Blue) colour values are hues of light that can be mixed together to create different colours. The colours are reproduced using numbers or values from 0-255. For example, to get the colour of black, all the RGB values are set to 0, as shown in bottom right page of the book in Figure 3. So when RGB value is set to 255, it will produce colour white.



Figure 4: Hex colour value of green shades with flaps. Hex values always start with # sign.

3. Baby Loves Coding



Figure 5: Cover page of Baby Loves Coding

This bright color board book is about the concept of logic, sequencing, and problem solving.



Figure 6: The page explains sequencing and what is algorithm



Figure 7: This page explains that a computer language is called code

Referring to Figure 7, the page explains ‘A programmer writes an algorithm in a language the computer can understand. The language is called code. The computer reads the code and follows the steps in the algorithm’. The colorful image in a white bubble on top of the train is a code in form of block. It is called as block programming or block coding.

Block programming is an entry-level game where a player needs to drag and drop block of codes. Examples of websites that provide simple and fun block programming is <https://code.org/> and <https://blockly.games/>. More information of block programming has been described at an article Let's Learn Programming Through Gaming under the eSecurity Bulletin Volume 44 (1/2018): https://www.cybersecurity.my/data/content_files/12/1860.pdf



Figure 8: Let's Learn Programming Through Gaming: block of codes to navigate Minecraft character in completing a goal.

4. Web Design for Babies (Volume 1 – 3)



Figure 9: Front covers for the 3-volume set of the "Web Design for Babies" series

From the same writers of "ABCs of the Web" and "Web Colours", the Web Design for Babies is a 3-volume set of books that aims to introduce to babies the 3 major scripting languages and components that used in Web Design: HyperText Markup Language, or HTML, Cascading Style Sheets, or CSS and JavaScript.

Author John C. Vanden-Heuvel Sr which is also a web designer himself, started out to design the series of books for his own baby, with the aim to introduce Web Design to babies in the early stages. The contents of the books are large prints and brightly colored text and syntaxes, in the proper formatting as used for the 3 components of Web Design mentioned previously.



Figure 10: Contents of Web Design for Babies Vol. 1 - HTML for Babies book

For example, the contents of the first volume, "HTML for Babies" consist of 16 pages of positive messages, printed in bright colors and in well-formed HTML, like `<div class="go" id="homesweethomelife"></div>` on pages 7 and 8. Different to the contents shown in the 2nd volume "CSS for Babies" which shows different parameters and syntaxes in the proper CSS standards compliant layout also in large and brightly colored text.



Figure 11: Contents of Web Design for Babies Vol. 2 - CSS for Babies book

5. Web Design for Babies 2.0 - Geeked Out Lift-the-Flap Edition

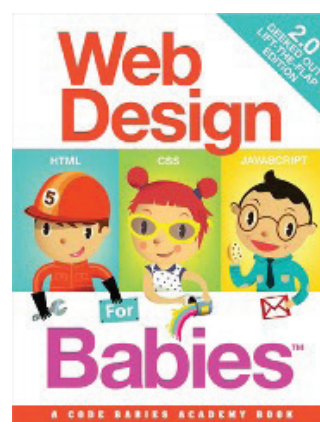


Figure 12: Front cover of Web Design for Babies 2.0 - Geeked Out Lift-the-Flap Edition

Designed and written by the same author of the previous version of **Web Design for Babies**, **Web Design for Babies 2.0 - Geeked Out Lift-the-Flap Edition** is not only content rich but combines three major components of Web Design: HTML, CSS and JavaScript all in a single book. This version has imaginative characters and beautiful illustrations designed by Cristian Turdera. It is more interactive as it features "lift-the-flap" contents for enhanced interaction with the babies.



Figure 13: Contents of Web Design for Babies 2.0 - Geeked Out Lift-the-Flap Edition

This version of the book is more guided as it introduces the real concepts of Web Design in a simple and relatively easy way for babies and infants to read and understand. Every parameter, syntaxes and functions are properly introduced and explained in a relatively elaborate paragraph that can allow babies and infants to properly identify and understand each of the syntaxes and their functions.

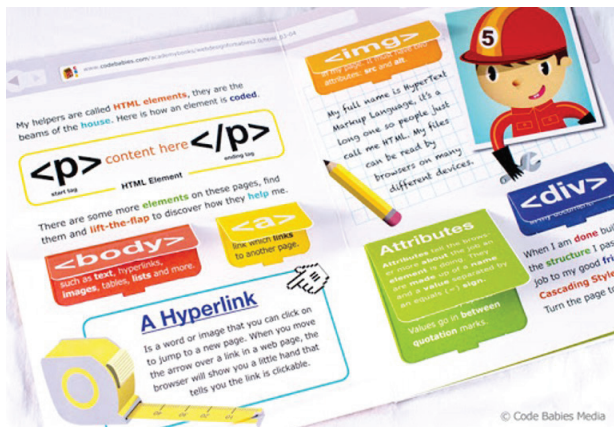


Figure 14: Page showing the “flaps” contents feature of the book

Conclusion

One can find a lot of reading materials designed to introduce and educate the concepts of Information Technology such as programming for babies and small infants. Authors and content designers will have plenty of opportunities to develop and design more reading materials that can touch on the plethora of IT elements for young audiences. There should be a slow paradigm shift from the general perception that Information Technology and the concepts of computer programming are difficult and considered as advanced topics of knowledge, removing any negative assumptions towards it. Information Technology is now accessible for audiences of all ages, which in turn, can play an important role in empowering IT knowledge and skills for the betterment of the society that we live in.

This article only reviews and explore one of the many materials designed to teach and allow babies to learn about coding and programming. Of course, there may be other publications and materials in a variety of forms that are yet to be reviewed.

References

1. John C. Vanden-Heuvel Sr. and Andrey Ostrovsky MD (2013). *ABCs of The Web*. Weldon Owen Publishing.
2. John C. Vanden-Heuvel Sr. (2016). *Web Colours*. Weldon Owen Publishing.
3. Ruth Spiro (2018). *Baby Loves Coding!*. Charlesbridge.
4. John C. Vanden-Heuvel Sr. (2017). *HTML For Babies*. Code Babies.
5. John C. Vanden-Heuvel Sr. (2012). *Web Design for Babies 2.0: Geeked Out Lift-the-Flap Edition*. Code Babies.

Securing Your Video Conferencing Meeting

By | Alifa Ilyana Chong Binti Abdullah & Nur Haslailly Binti Mohd Nasir

The COVID-19 pandemic outbreak has changed the way we receive education, engage in social relations and work, with millions of people across the globe adapting to distance learning, online social relations and remote work. Employees have adapted to a work from home policy which allows them to work from home—either full-time or when it is most convenient for them. This is in accordance with the government's Standard Operating Procedure (SOP) for COVID-19. Work from home aka WFH entails an employee working from their place of residence, rather than the office.

Video teleconferencing tools have made it easier for colleagues to communicate and stay in touch, regardless of their geographical location. Many organizations have opted for video-enabled meetings to carry out their business for


internal/support functions as well as external functions. Consequently, it is essential to secure the privacy of video-enabled meetings to prevent hijacking aka “**Zoombombing**” which refers to incidents of unwanted and disruptive intrusion by hackers where they hijack Zoom video teleconferencing sessions and broadcast inappropriate or sensitive material to the attendees. Such incidents have resulted in Zoom taking measures to increase security of its video teleconferencing solutions.

Tips for Securing Your Privacy on Video Teleconferencing Meeting

The infographic below explains some tips to help you enjoy greater privacy and to maintain control during video teleconferencing meetings.

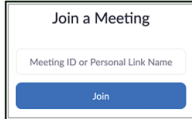
1. Security Strategy

- Choose a meeting platform with good security settings/features.
- Meeting organizers should evaluate the meeting sensitivity and adjust security protocol accordingly.
- An example of video conferencing applications: Google Meet, Microsoft Teams and Zoom.



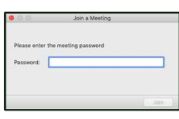
2. Unique Meeting IDs

- Apply a unique meeting identifier to increase security.
- Never reuse same meeting IDs, especially for important business meetings.
- This is to prevent anyone that was invited to a previous meeting can join all future meetings.



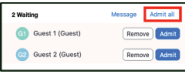
3. Meeting Password/ PINs

- For an extra layer of security, set a meeting passwords or PINs.
- Apply strong password consist a combination of uppercase and lowercase letters, numbers and special symbols.
- Don't create an easily guessable password like "123456".




4. Waiting Room Features

- Use the waiting room features to manage those requesting to join.
- The host of the meeting to admit only people who are supposed to be in the room. Keeping those unauthorized people from knowing the confidential information been discussed in the meeting.



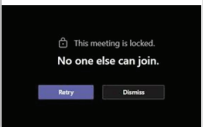
5. Limit Screen Sharing

- Don't allow participants to share screen by default.
- Turn off screening feature for all participants so only the presenter can use it.
- Once meeting has begun, the host can allow specific participants to share when appropriate.



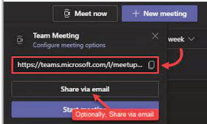
6. Lock Your Meeting

- Lock meeting features is very useful to ensure meetings are completely private.
- Once invited attendees are joined the meeting, locked the meeting to keep out unknown attendees.



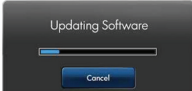
7. Don't Share Links

- Don't share meeting links via social media posts.
- Invite attendees from within the conferencing software.
- Inform attendees do not share the links too.



8. Keep Software Up To Date

- Security vulnerabilities are likely to be exploited more often on older software versions.
- Make sure your meeting software is installed with the latest patches/ updates.



Conclusion

A spike in online meetings due to the pandemic will result in new threats appearing more regularly. Therefore, it is crucial for the business owners or meeting hosts to be aware of the importance of security. Habitually applying the '*Tips for Securing Your Privacy on Video Teleconferencing Meetings*' will greatly protect any sensitive information, data and privacy of attendees during video teleconferencing/online meetings.

References

1. *How to Make Sure Your Online Meeting is Secure:* <https://www.arvigbusiness.com/for-business/how-to-make-sure-your-online->
2. *Do's and don'ts of videoconferencing security:* <https://www.computerworld.com/article/3535924/do-s-and-don-ts-of-videoconferencing-security.html>

Privacy Issues In Big Data

By | Ts. Suraya Hani Binti Ahmad Zaki & Siti Fairos Binti Mat Husin

The definition of big data could vary greatly. Big data refers to data sets that are so large or complex that traditional data processing applications are not able to process. It is a large volume of data—both structured and unstructured—that overwhelms the business on a day-to-day basis.

Nevertheless, the evolving nature of 'Big Data' concept can be defined by using the notion of 5Vs. 'Volume' is the large amount of data that is either consuming huge storage or entailing a large number of data records. 'Velocity' is the frequency or speed of data generation or frequency of data delivery. 'Variety' means data is generated from a large variety of sources, formats and contains multidimensional data fields including structured and unstructured data. 'Value' denotes the importance of extracting economic benefits from the available Big Data and 'Veracity' is to highlight the importance of quality in data and the level of trust in various data sources. Figure 1 shows the 5 Vs of Big Data.

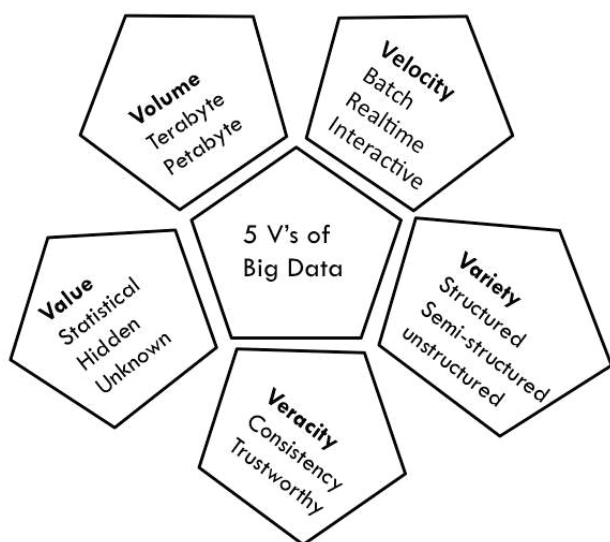


Figure 1: 5 Vs of Big Data

Big data applications are utilized across various sectors, including healthcare, finance, energy, media, and public services. Thus, bringing a new set of security challenges to preserve the confidentiality, integrity and privacy of any data that may be compromised during collection and analytical processing [1]. This article will attempt to analyze existing literature in relation

to various privacy threats issues in different big data applications and present a summary of the study.

Big Data Privacy and Global Security Challenges

Huge amounts of data are generated every day from various sources like sensors and location data from mobile phones and other consumer electronic devices such as Internet data from web searches and social media from Facebook to Twitter. Since the number of devices connected through the Internet of Things (IoT) is increasing exponentially, big data is gaining more attention as these large amounts of data can be transformed into valuable information.

Emerging technologies heightens the privacy and security concerns. From a regulatory aspect, Edward Snowden, a whistleblower for the National Security Agency (NSA) in United States (US), raised these long-standing security issues. This discovery revealed that the US government has been gathering and processing data from the web for years, and not simply for economic reasons.

The value of data privacy and transparency is defined as being open about data privacy assurances and safeguards, as well as transparency of data collection, management, storage, retention, disclosure, and routing practices. Transparency in data privacy enables more accountability and safe data access when it comes to how data is acquired.

Similarly, the United States Department of Homeland Security issued a set of Strategic Principles for Securing the IoT to assist consumers and businesses in making decisions about their connected devices. These guidelines lay out proposed concepts for consumers, businesses, service providers, and other stakeholders to consider while creating and producing contemporary technology gadgets. Although big data technologies can boost productivity, ease of use, and integrated functionality, they are also vulnerable to unauthorized users gaining physical access to the device users. By regulating privacy and security characteristics

of commercial connecting devices for big data technologies sources may not always allow complete access to and from the Internet.

In a Big Data environment, security issues of outsourcing and the use of third-party tools create dependency on service providers and other third-party tools vendors. There may be a need for organizations to outsource some part of the tools and applications that support data storage, sharing and access. Cloud storage, for instance, also draws data security problems (e.g., requirements of data integrity checking) that lead to privacy issues when the datasets are hosted in a server that is publicly accessible. Hence, information privacy becomes harder to secure and protect when data is being multiplied and stored on various servers around the world.

The most critical issue in Big Data is the changing of security laws in Europe. On May 25, 2018, the EU's General Data Protection Regulation (GDPR) became effective supplanting the 1995 Data Protective Directive (DPD). This new law influences the E.U. and nations in the European Economic Area (EEA), paving for data security guidelines in the advanced age (Because of Brexit the United Kingdom has a different Data Protection Act 2018 that mirrors the principles in the GDPR).

The information controlled by the GDPR relates to people; it does not make a difference to information about associations. Although GDPR holds a significant part of the old DPD arrangements, yet it accommodates expanded fines for information stockpiling, requires straightforward security for data subjects, allows demand erasure of their substance, how their information will be utilized, privilege to have their data expelled and can demand for their information not to be used. The results of Big Data analysis are statistical findings

that process anonymous data which conforms to all requirements of GDPR. The increasing availability of large data sets from various sources in combination with the development of advanced analytical tools for Big Data makes it more difficult to ensure privacy. Enforced by law and regulation, organizations use strategies such as data encryption and data de-identification to ensure privacy. Although encryption can protect the privacy of an object itself, however, it still can be vulnerable against side information attacks, such as traffic analysis attack against anonymous communication systems.

This leads to the essential needs on controlling Big Data from a policy-making perspective and the threats from machine learning in designing policies and programs of balance the goals of protecting privacy and ensuring fairness with those of reaping benefits for government organization, scientific research, individual and public health.

Privacy Issues in Big Data Applications

According to Gartner, by year 2023, the financial impact of cyber-physical system attacks resulting in fatal casualties will reach over \$50 billion, 10 times higher than 2013 levels of data security breaches. Security and privacy issues in big data can be magnified by the volume, variety, and wide area deployment of system infrastructure in supporting Big Data applications.

Table 1 summarizes the mapping of privacy issues in various Big Data applications based on the literature reviews using big data security challenges, privacy and security, data privacy, security, and privacy management keywords.

Big Data Applications	Discussion on Privacy Issues
Healthcare	Privacy of medical data i.e. invasion of patient privacy information systems due to the emergence of advanced persistent threats and targeted attacks coerces organizations to verify if their applications conform to privacy agreements and whether sensitive information is kept private regardless of changes in applications and/or privacy regulations [2].

Public Sector	<p>The accumulation of unsolicited data across administrative boundaries may reveal highly sensitive, personal and security information when combined with various other data sources that would compromise an individual's private information and national security.</p> <ul style="list-style-type: none"> • Access rights to the required datasets for an operation must be justified and obtained. • A notification or a license must be obtained from the Data Privacy Agency when a new operation is performed over existing data. • Data separation is required in this scenario to preserve anonymity. • Individual privacy and public security concerns must be addressed before open data sharing. • Impose the public sector cloud computing regulation engage only to trusted cloud providers. • The lack of big data cloud computing providers is also a barrier for adoption.
Finance and Insurance	<p>In big data analytics, a third-party information is deemed to be confidential data.</p> <ul style="list-style-type: none"> • Financial service organizations need to ensure compliance with their agreements • Any use of such data would not breach their confidentiality or regulatory responsibilities. <p>In European Union (EU), legal requirements rule for financial services organizations are significant:</p> <ul style="list-style-type: none"> • Personal data must be processed for specified and lawful purposes • The processing must be adequate, relevant, and not excessive. • Increased costs for financial services organizations as they must attain consent from individuals that holds the right to remove or refrain from processing their personal data in certain circumstances. • This removal of data may lead to the dataset being distorted due to certain individual awareness of their rights than others. • Relevant disclaimers need to be applied due to the risk of misinterpreting the massive information produced. <p>Banking and financial institutions need to secure the storage, transit, and use of:</p> <ul style="list-style-type: none"> • Corporate and personal data across business applications • Online banking and electronic communications of sensitive information and documents. <p>Financial services organisation needs to comprehensively address global data security and privacy throughout the entire supply chain:</p> <ul style="list-style-type: none"> • Data is not constantly stored in-house but with third parties. • Data stored in commercial "cloud" services locations poses potential privacy and security issues as the terms of service for these products can be misunderstood.

Table 1: Literature Review of Privacy Issues in Big Data Applications

Conclusion

Big Data is transforming the business and commercial landscape, most significantly in the field of users' data protection and privacy preservation. In an ever changing global order, there is a greater need than ever before, to reflect about the standards supporting the right of our society, and to strengthen the realization of rights to data protection as a fundamental human right of each individual.

Incorporating privacy into the design of a system minimizes the risk of privacy breaches. By reducing trust in processors and data collectors when handling sensitive data and leaving the duty to secure the data in the system itself, there should be an initiative that drive the drafting of governance framework for Big Data in Malaysia.

References

1. J. Moura and C. Serrao, "Security and Privacy Issues of Big Data," 2019, pp. 1598-1630.
2. K. Abouelmehdi, A. Beni-Hessane, and H. Khaloufi, "Big healthcare data: preserving security and privacy," *Journal of Big Data*, vol. 5, no. 1, p. 1, 2018/01/09 2018.
3. Tan Zhai Yun, *The Edge Malaysia*, "Malaysia Digital Economy Blueprint: Boosting cloud capabilities in Malaysia" <https://www.theedgemarkets.com/article/malaysia-digital-economy-blueprint-boosting-cloud-capabilities-malaysia>
4. Jose Maria Cavanillas et al., "New Horizons for a Data-Driven Economy. A Roadmap for Usage and Exploitation of Big Data in Europe", *SpringerOpen*, 2015.
5. C. Perera, R. Ranjan, L. Wang, S. U. Khan, and A. Y. Zomaya, "Big Data Privacy in the Internet of Things Era," *IT Professional*, vol. 17, no. 3, pp. 32-39, 2015.
6. T. Mulder and M. Tudorica, "Privacy policies, cross-border health data and the GDPR," *Information & Communications Technology Law*, pp. 1-14, 2019.
7. S. A. Aaronson, "Data is different, and that's why the world needs a new approach to governing cross-border data flows," *Centre for International Governance Innovation, CIGI Papers No. 197 — November 2018*.
8. D. K. H. A. Mohamad et al., "Establishing Information as Tangible Asset," *Sciences*, vol. 9, no. 6, pp. 539-547, 2019.
9. M. Islam and M. Karim, "EXTRATERRITORIAL APPLICATION OF THE EU GENERAL DATA PROTECTION REGULATION: AN INTERNATIONAL LAW PERSPECTIVE," vol. 28, p. 2020, 12/28 2020.
10. N. Sidek and N. a. Ali, "Internet of Things-based Services Implementation and Challenges in Malaysia: A," 2019.
11. W. A. Günther, M. H. Rezazade Mehrizi, M. Huysman, and F. Feldberg, "Debating big data: A literature review on realizing value from big data," *The Journal of Strategic Information Systems*, vol. 26, no. 3, pp. 191-209, 2017/09/01/ 2017.

Website Preservation: Better Than Zero

By | Ts. Tajul Josalmin Bin Tajul Ariffin, Muhammad Umar Bin Shahbuddin, Muhammad Bin Mohd Roslan & Muhammad Muzammil Bin Abdul Rashid

Introduction

Website preservation is among one of the most important tasks as a Digital Forensics First Responder. This method is to assist in preliminary investigation and during preservation process in Digital Forensics Methodology. To perform this task, it is important as a first responder to understand the conceptual and modularity of website components. This is to compliment the knowledge before performing the task.

A structured and proper step in performing this task is also vital. This is to ensure that evidence integrity is properly maintained. This is to ensure the collected data and potential evidence are admissible in the court if required.

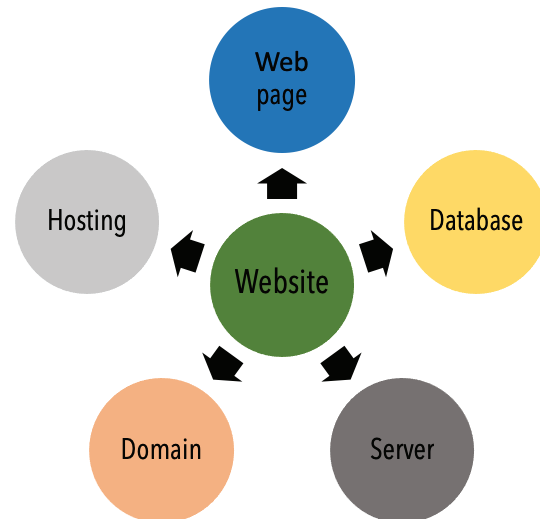


Figure 1: Website Components.

Website Components

Website is defined as a collection of publicly accessible, interconnected Web Pages shared in a single domain name. It can be created and maintained by individuals, groups, businesses, or organization to serve a variety of purposes.

It is very important to understand the key components on the website. It will assist the first responder in understanding the workability of a website. Below is a diagram that explains the components in a website.

Web Page

A web page is a form of a document that the World Wide Web that identifies by a unique uniform resource locator (URL). A web page can be accessed through a web browser. The data on a web page is either in HTML or XHTML format. It usually contains other resources such as style sheets, scripts, and images for representation. It also allows user to navigate to other pages through hyperlinks. There is a variety of programming languages used for website development such as Hypertext Markup Language (HTML), JavaScript, Cascading Style Sheets (CSS), Common Gateway Interface (CGI), Asynchronous JavaScript and XML (AJAX), Active Server Pages (ASP), ASP.NET and Java Server Pages (JSP).

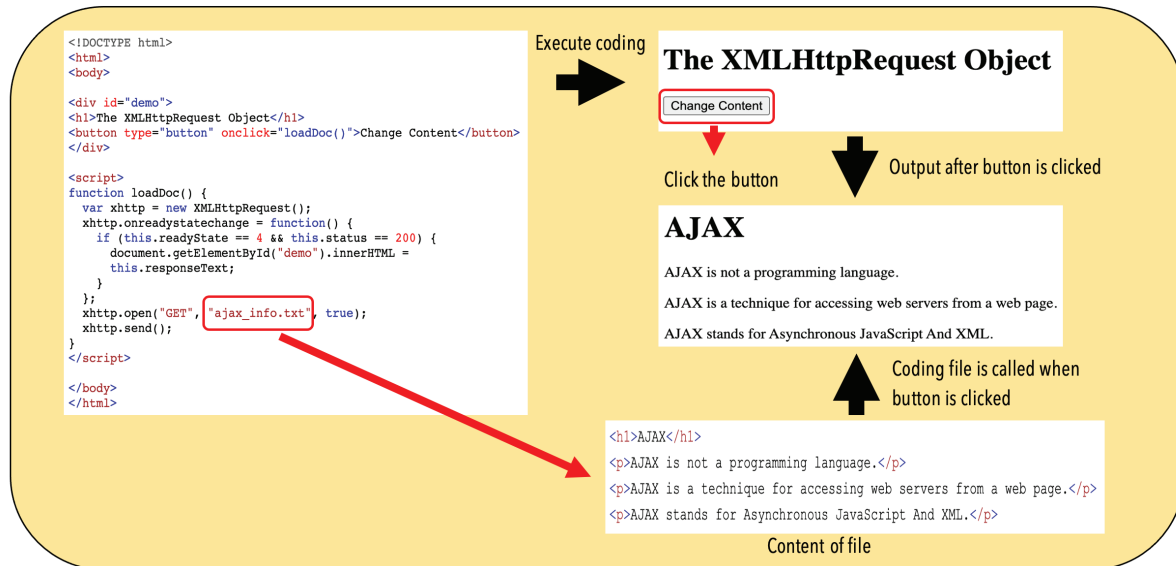


Figure 2: Example of Asynchronous JavaScript and XML (AJAX) coding.

Below are the differences between static and dynamic webpage.

Static	Dynamic
Page remain same unless manually changed	Content are different to cater to different visitors
Simple	Complicated
Rare changes of information	Frequent changes of information
Require less time for loading	Require more time for loading
No database	Contains database
No application program	Contains application program for different services
Less work and cost	More work and cost

Table 1: Differences between static and dynamic web page.

Database

Database is explained as an organized electronic system that allows data to be easily accessed, manipulated, and updated. A database is used as a method of storing, managing, and retrieving information. Modern day database is managed by using a Database Management System (DBMS). There are two types of databases that are Structured Query Language (SQL) and NoSQL. SQL is widely used where it allows handling information using tabular and querying the tables and other related objects. Meanwhile

NoSQL is a non-relational database and does not require structured schema that defines each table and related columns.

For SQL Database, it is common to see the usage of MySQL, Microsoft SQL, IBM DB2 and Oracle. Meanwhile for NoSQL, MongoDB, BigTable, Redis and RavenDB are among the variety used. Below are the differences between SQL and NoSQL database.

SQL	NoSQL
Relational	Non-relational
Use structured query language and predefined schema	Dynamic schemas for unstructured data
Vertically scalable	Horizontally scalable
Tabular based	Document, key-value, graph, or wide-column stores
Better for multi-row transactions	Better for unstructured data (Documents or JSON)

Table 2: Differences between static and dynamic web page.

Web Server

Web server is defined as a system that delivers content or services to end users on the Internet. It consists of physical server, server operating system (OS) and software used to facilitate HTTP communication. Among types of web server are Apache HTTP Server Web Server, Internet

Information Services (IIS) Web Server, Lighttpd Web Server, Sun Java System Web Server, Jigsaw Server Web Server, LiteSpeed server Web Server and Node.js Web Server.

Browser

Browser is an application used for retrieving, presenting, and traversing information on the World Wide Web. User will access the website hosted by browsing through the web browser. Common web browser are Google Chrome, Mozilla Firefox, Safari, Opera and Microsoft Edge and Internet Explorer.

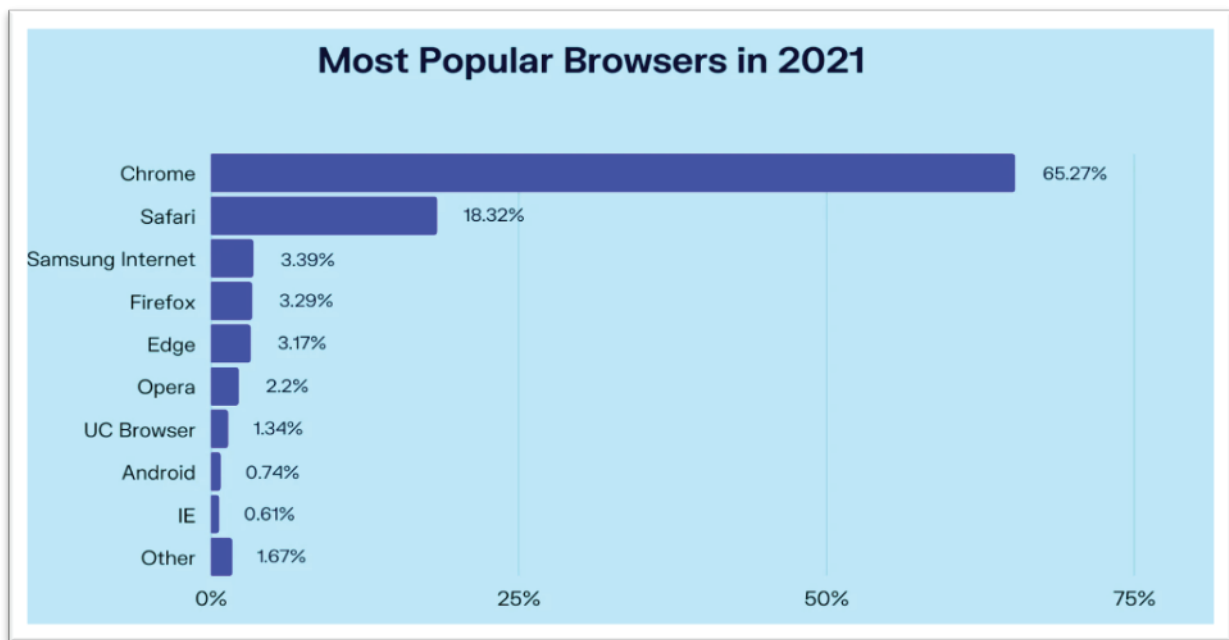


Figure 3: Most popular Browser in 2021.

Domain

Domain name is defined as an Internet resource name that is universally understood by Web server and online organizations and provides all pertinent destination information; while a sub-domain is part of a larger domain under the Domain Name System (DNS) hierarchy. Usage of sub-domain includes website content organized according to category, sharing the allotted domain space with other users by providing sub-domains and a dedicated username and password with varying levels of feature access and shorten long links and easing user to remember.

Domain Name Server (DNS) is referred to as a phonebook of the Internet. It translated domain name to specific IP address when user types a domain name and point it to the correct website. It also manages domain name system/ protocols, matching domain names and IP address. Below is illustrated on how a DNS works.

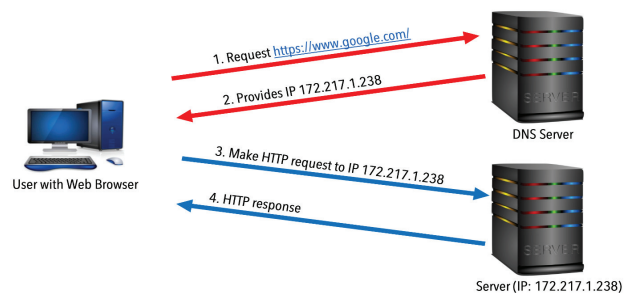


Figure 4: How Does Domain Name Server works.

Web Hosting

Lastly is web hosting. Web hosting is defined as an organization that sells or leases memory space on its servers. It is typically done in a data centre and provides services to clients that enables them to publish websites on the Internet. A web host can also provide data centre space and an Internet connection for servers owned by others. Services provide by a Web Host is commonly called Web Hosting. Below is the illustration on how Web Hosting works.

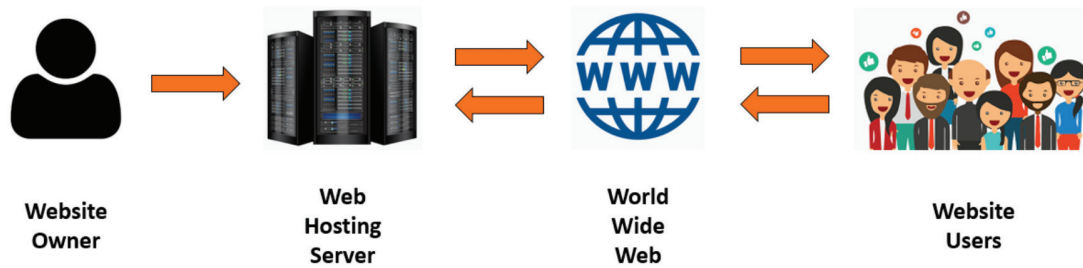


Figure 5: How Does Web Hosting works.

There are several types of web hosting:

1. Shared

- Numerous sites are hosted in one shared server.
- It will minimize the operation cost of the customer/ client.

2. Reseller Hosting

- Clients from shared hosting allowed to be web host themselves.
- Clients sell their hosting space to other customers.

3. Dedicated Hosting

- Dedicated server exclusively per customer.
- Customer has the full control of the server (Server not owned).
- Hosting provider will maintain the server.
- Higher operation cost for the customer.

4. Managed Hosting

- Customer manages data using File transfer Protocol (FTP) or remote tools.

- Customer does not have full control of the server.

5. Cloud Hosting

- Powerful, scalable, and reliable based on load balanced server.
- Customers pay/charged as per usage of resources.
- No disruption during natural disaster.

6. Cluster Hosting

- To cater customers that need high availability and scalability (e-Commerce and online portals).
- Offers better resource utilization by hosting same content on multiple servers.

7. Grid Hosting

- Distributed hosting where a cluster of server's acts like grid which consists of multiple nodes.
- Best suited for high online traffic websites.

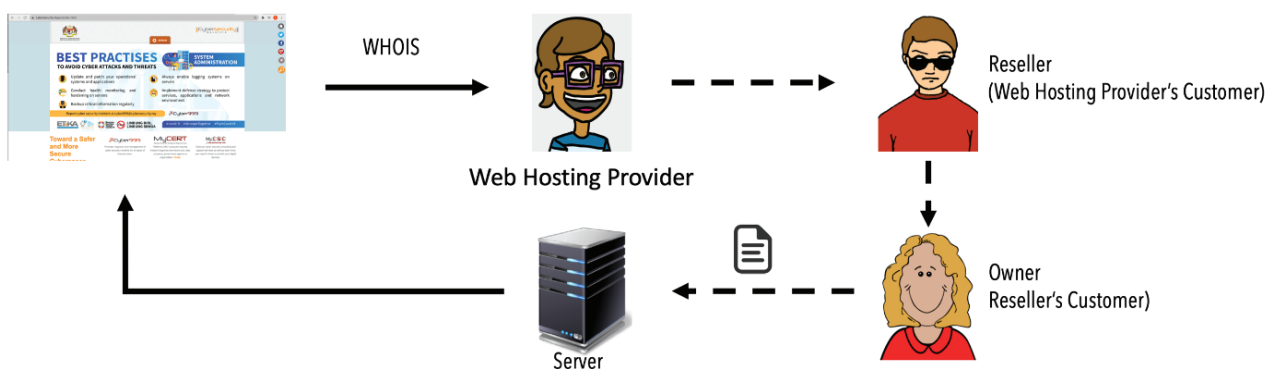


Figure 6: How Does Reseller Hosting works.

Website development and deployment cycle usually contains a live platform and production platform. Production platform is where all necessary web application is stored. This is when there are changes deemed identified and needed, the production platform will test and execute it before is deployed at live platform. Live platform is where users interact with the application and website services. Below illustrates the cycle of website development and deployment:

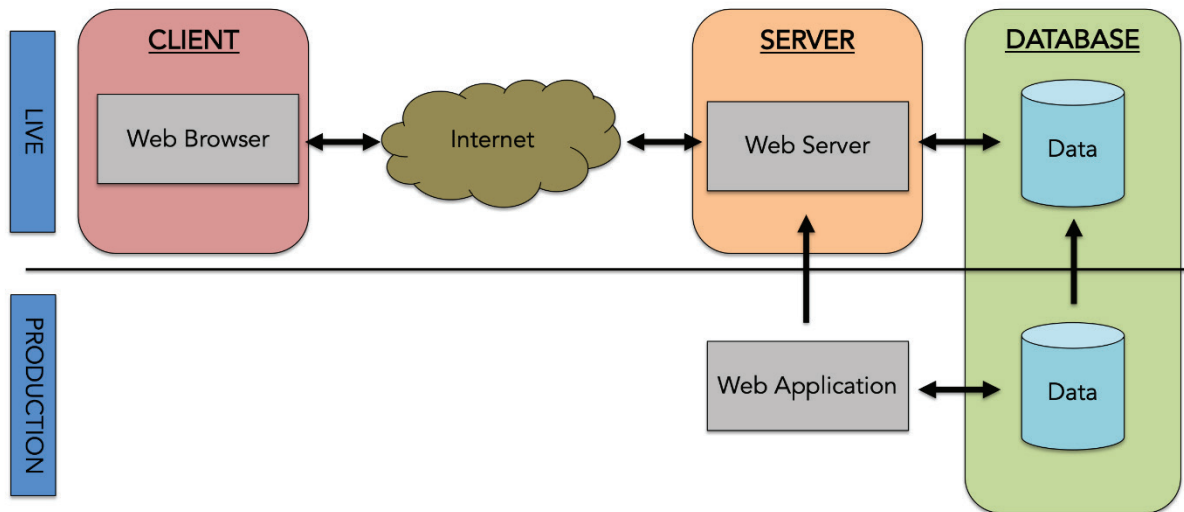


Figure 7: Cycle of website development and deployment.

Website Preservation

Website preservation is the practice of taking a copy of a website or content published on the website to act as a record. Preservation of website is necessary to put on record information such as illicit sales, sales offences (weapons, medicine, drugs), inappropriate content, illegal investment.

The importance of preserving a website is ensure the information and data are preserved according to digital forensics method before the website is taken down. It is also to ensure there are no modification after the offences has been determined. Other than that, it is especially important to capture website content when it is the only version of a record. Many records published on the web may be archived discretely. For instance, an organisation may archive reports or other documents through local records management. In other cases, an organisation may share content through their website that is not captured anywhere else.

The website preservation is a preliminary information gathering which is in IDENTIFICATION AND COLLECTION PHASE on Digital Forensics Methodology.

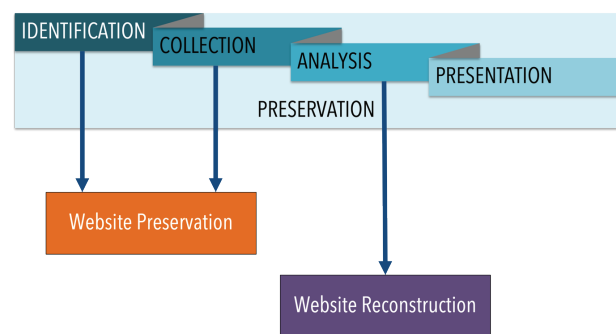


Figure 8: Digital Forensics Methodology.

Identification Phase

The main objectives of website preservation in identification phase are to identify important information from a website related to the offences and verify the information from a preserved website. It is to ensure the data should be preserved and extracted and the extracted data is relevant with case background/objectives

In identification, analyst should understand the case background and obtain the information such as website URL and dirty keyword list. Hence, analyst can determine what information needs to be extracted with list of keywords related to the offences.

Perform website preservation by creating unique screenshot of the website and its source

code for reference. Therefore, analyst can perform comparison and identify if there is any modification after the preservation.

WHOIS is a widely used Internet record listing that identifies who owns a domain and how to get in contact with them. This information will be preserved along the previous information. Another purpose of the information are to verify the correct IP/ Server related and the hosting server of targeted website. Next, the information will be used to proceed to the next phase which is collection phase.

To complete the process, analyst will have to summarize the finding by:

1. Save all findings in one (1) folder.
2. Verify the findings and screenshots.
3. Compress and archive findings.
4. Hash the zip files.
5. Burn the Zip file in a dedicated media storage.

Collection Phase

At collection phase, analyst will be performing on-site investigation at the website application and database hosting server. The website and its database will be preserved and extracted using Computer Forensics procedures. Before an analyst proceeds to the preservation and extraction phases, the target will go through the confirmation process as following:

1. Ensure the correct website application and its location.
2. Observe the server configuration (from the web server folder).
3. Ensure the location of database dump and data files.
4. Observe the web configuration folder file (from web application folder).

Then, next steps need to be taken for preservation and extraction:

1. Collect database files from the database server application folder.
2. Collect web application files from the web server folder.
3. Extract and compressed all files. (*.zip, *.tar, and many more).

After completing the process, create hash on the compressed files to establish evidence integrity. Then, store the extracted files to a dedicated media storage (eg: DVD, Thumb drive, External Hard Disk) and perform digital forensics procedure in seizing the media storage as evidence.

This is an appropriate process in handling cases related to website. The process will be able to help the investigation and digital forensics analysis. By performing this process, the information and data can be preserved and presented in the court of law.

Conclusion

To avoid any inconvenience caused during proceedings in court, a proper understanding on website technologies is deemed important. There is a possibility that the first responder needs to design a diagram to show on how the website or system work during presentation to stake holders.

Other than that, a proper method and steps need to be performed to avoid any tampering on potential evidence. This is to smoothen the prosecution process if it involves administrating digital evidences to the court of law.

References

1. <https://www.techopedia.com/definition/5411/website>
2. https://www.w3schools.com/xml/ajax_intro.asp
3. <https://www.techopedia.com/definition/1185/database-db>
4. <https://my.oberlo.com/statistics/browser-market-share>
5. <https://www.mydreamhosting.com/what-is-web-hosting/>
6. <https://www.domaintools.com/support/what-is-whois-information-and-why-is-it-valuable>

Understanding Spyware: Types And Effects

By | Mohamed Anwer Mohamed Yusoff & Muhammad Nazmie Mat Nasir

Introduction

Spyware is a type of software that can be installed and run on a computer, without the user's knowledge, consent, or control. Spyware can change the computer's settings, monitor online activities, and gather information about the user, which could include personal information (D Anil Kumar, Sisira Kumar Kapat, Susanta Kumar Das, Satya Narayan Tripathy, 2019). According to Avast.com - "Pegasus is a remote access tool (RAT) with spyware capabilities." Its Android variants are capable of extracting data from popular messengers such as WhatsApp, Facebook, and Viber as well as email clients and browsers.

A spyware is capable of remote surveillance through the phone's microphone and camera, as well as taking screenshots and keylogging the user's inputs. It can steal private data from a phone, sending the target's messages, passwords, contacts, photos, and much more—to whoever initiated the surveillance. It can reportedly even turn on the phone's cameras or microphones to create covert recordings. Recent versions of it have reportedly been able to do this without having to get the user to do anything — a link will be sent to their phone, without a notification, and Pegasus will start collecting information.

In other cases, the spyware has reportedly relied on users to click phishing links which then delivers the Pegasus payload. Pegasus is a spyware developed by the Israeli cyber-arms firm, NSO Group. Current Pegasus software can exploit all recent iOS versions up to iOS 14.6. The spyware is named after the mythical winged horse Pegasus because it is a Trojan horse that can be sent "flying through the air" to infect phones.

Types of Spyware

Spyware is not just confined to one type of program, but several types. Some are capable of attacking user's a computer and steal personal information. The various types of spyware include the following:

Adware

Adware is a software that is normally installed accidentally by the end-user and is a common part of free software, for example, document sharing applications. It gathers data about the user that can be utilized for designated ads in the form of banners, pop-ups, and security intrusion through the following of treats to associate online behaviour to distinguish a particular person, which aids in targeted attacks. Adware is quite often the software itself that is created in relation to e-mails. Be alert when opening your e-mail because someone else might be benefitting from your email and mull over downloading from your Internet, email, or web search. In addition, adware is also known as 'ad promoting virus, adware, and spyware' which is a component that checks for harmful software. It monitors the user's online activities and serves the advertisements as it believes the user's likes based on that data. Although innocuous in comparison to other types of spyware, adware may have a negative impact on a device's functionality as well as being an annoyance.

Trojans

A Trojan is a malicious software that appears to do a desirable function but in fact performs undisclosed malicious functions that give the opportunity for unauthorized access to a victim's computer. A Trojan's victim may unwittingly install a file posing as an official software, allowing the Trojan to get access to the computer. The Trojan can destroy data, encrypt files for ransom, or leak the user's information to unauthorized individuals. They look for delicate data after landing on a device, for example bank account information and send it to a seedy third-party who will use it to steal money, compromise accounts or make fraudulent purchases. They can likewise be controlled by a computer through installation of a backdoor or a remote access Trojan (RAT).

Key loggers

Keyloggers is a program that runs in the background of a hardware, recording all the keystrokes made by user. Keyloggers are hidden in the machine for later retrieval and often used

without the user's full awareness and consent whenever keystrokes are logged. Attacker checks the files carefully in the hopes of either stealing personally identifiable information (PII), login passwords, or critical corporate data. Employers can use keyloggers to monitor their workers' computer activities; parents can monitor their children's Internet usage; device owners can track potentially unlawful behaviour on their devices; and law enforcement agencies can investigate computer-related events.

Keyloggers can be divided into two categories which is hardware and software. Hardware keyloggers are mounted within the computer case, within the keyboard port, or directly within the keyboard itself, while others are plugged into the end of the keyboard cord. This hardware keyloggers are used for keystroke logging, a strategy for catching and recording user's computer keystrokes, including sensitive passwords. Software keyloggers do not need actual access to the user's computer for installation. Software keyloggers are regularly downloaded deliberately by somebody who wants to monitor the activity on a specific computer, or it will be downloaded accidentally and executed as a piece of a rootkit or remote access Trojan. Software keyloggers also track system, obtain the keystroke data within the target operating system, and store them on a disk or in a remote location. This will be then sent to the attacker who installed the keyloggers.

Mobile Spyware

Mobile spyware is classified as a dangerous software program because it tends to monitor and get the information from the users without their permission and knowledge through a Short Message Service (SMS) or Multimedia Messaging Service (MMS) or text messaged. This is normally done without user interaction to execute commands. In addition, the most common way for the user's phone to get infected by mobile spyware is by downloading unauthorized applications. There will be a chance for the user's device to turn into a spying tool. When mobile spyware infects a smartphone or tablets, the phone's camera and microphone will be utilised to keep an eye on nearby activity, record calls, and log perusing activity and keystrokes. The device's owner's location can be monitored by using Global Positioning System (GPS) or the mobile computing device's accelerometer.

Effects of Spyware

The following are the most common effects of spyware infection on a user's computer:

1. Computer Damages

Spyware can harm a user's computer and slow down the performance of a computer. Lack of performance optimization can take up an enormous amount from a computer's memory, processing power, and Internet bandwidth. Therefore, an infected computer might run slowly and hang in between applications or while on the web. More severe cases may experience frequent system crashing or overheating of computer, causing long-term harm. Furthermore, applications that have been affected will result in potential productivity and data loss. Some spywares can also disable Internet security programs.

2. Privacy and Confidentiality Risks

Once a spyware infects a user's computer, it can steal personal information for identity theft. The malicious software has access to every piece of information and data on the user's computer to imitate the identity. The purpose for these information includes browsing history, email accounts, and saved passwords such as for online banking, shopping, and social networks. In fact, spyware can siphon bank account information or credit card accounts should the user visit online banking sites, this information can be eventually sold to third parties.

3. Disruptions Browsing Experience

Spyware can control search engine results and deliver undesirable sites in a user's browser, which can prompt possibly harmful sites or fraudulent ones. It can also make changes to the user's home page and even modify several parts of the computer settings. Pop-up advertisements is another disruption that can be caused by spyware. Advertisements might even show up when offline, prompting certain irritations. It shows that spyware can assert control over the operation of computers in ways that substantially limit the ability of users to use the computers. For example, spyware programs can make a change in the user's browser setting which is often referred to as browser hijacking. It will change the web page display when the browser first launches, i.e., the home page, and frustrate efforts to replace that home page with the user's original home page.

Conclusion

Spyware brings a negative effect on computer security and a user's privacy. It often starts through system start-up, user login, or when the applications such as an Internet browser or other software is launched. Spyware is a malicious program and once it infects a computer, it will spread a copy of the computer program, data files, hard drive, boot sector, etc. This spyware is often accidentally installed without the knowledge and consent of users. This kind of infection is dangerous as it can harm the user's computer by stealing confidential data or damaging hardware function. When spyware is deeply entrenched in a user's computer, it will be tough to remove. It is better to take preventative action and block this infection from interacting with the computer. Users need to be careful and avoid clicking on unknown links to avoid being infected with spyware.

Reference

1. <https://www.ijrte.org/wp-content/uploads/papers/v8i2S6/B10880782S619.pdf>
2. http://www.cs.toronto.edu/~lloyd/howtoDCS/office/email/spam/spywarehome_0905.pdf
3. <https://www.csoonline.com/article/3384100/what-is-spyware-how-it-works-and-how-to-prevent-it.html>
4. <https://www.malwarebytes.com/adware>
5. http://ptgmedia.pearsoncmg.com/images/9780789735539/samplechapter/0789735539_ch03.pdf
6. <https://www.ftc.gov/sites/default/files/documents/reports/spyware-workshop-monitoring-software-your-personal-computer-spyware-adware-and-other-software-report/050307spywarerpt.pdf>
7. <https://blog.avast.com/pegasus-and-spyware-avast>

Embracing and Adapting Early Baby Boomers Into The Digital Age – A Case Study

By | Faiszatulnasro binti Mohd Maksom, Kilausuria binti Abdullah & Norlinda binti Jaafar

Introduction

Nowadays, digital technology is being utilised extensively by all generations from adults, younger adults, teenagers to even children. Older adults, especially baby boomers, are showing growing interest in the digital age as they embrace and adapt to digital technology, proving that technology is not just for the young and tech-savvy generations. But the rapid development of new technology and web series could result in less intuitive and user friendly interfaces which may hinder user experience.

Application and technology developers need to build ease of accessibility from the ground up, including design, text size, physical usability and technical support. If the application developers do not take this into consideration, this can lead to a digital divide between the older and younger generations once new applications are ready for public consumption.

Category	Year between	Age
Baby boomers	1946-1954	57-75
Gen X	1965-1979/80	41-56
Gen Y	1981-1994/96	25-40
Gen Z	1997-2012	6-24
Gen A	2012 & upwards	

Source: kasasa.com

Incident Overview

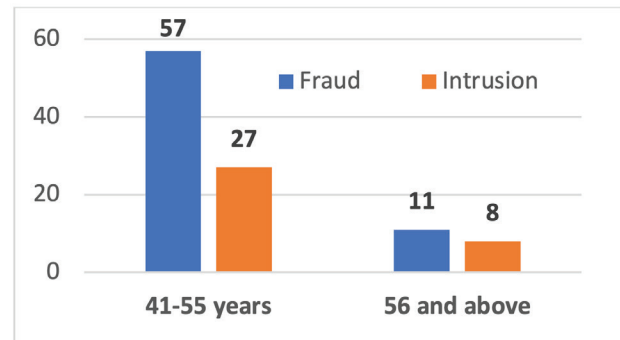


Figure 1: Frequent incidents reported by Gen X and baby boomers

According to Kasasa, Generation X, or better known as Gen X is anyone born between 1965 and 1980 (ages 41 to 56 in 2021) [1]. Gen X are also considered as the 'younger boomers' and they represent the generation change from the baby boomers. In 2021, it has been reported that Gen X has filed more complaints regarding fraud and intrusion incidents to Cyber999 Help Centre, more than baby boomers.

Despite being different in terms of age and digital literacy, based on our observations, there are two common behaviours that are present in both baby boomers and Gen X that render them vulnerable to cybercrime as they are attractive target of cyber-criminal.

The first case study was done based on the similarities of both the cohorts with their computer anxiety development towards the concern of privacy and safety of personal information. The second similarities are the susceptibility and vulnerability to online fraud due to a lack in online safety awareness. These two similarities are divided into two case studies.

CASE STUDY #1

As stated above, the first similarity that was presented by both the cohorts was their development of computer anxiety driven by privacy concerns towards the safety of their personal information, online security, the risk

of their physical safety and their emotional sanity [2]. A person with computer anxiety may experience fear of the unknown, feeling of frustration, embarrassment, failure, and disappointment; hence, resulting in avoidance towards computer usage [3]. Due to this factor, it has caused an individual to have a tendency to be more hostile and argumentative online. Despite owning and utilising their own smart phone and devices, they are constantly suspicious that they are being tracked and monitored by online fraudsters which contribute to their computer anxiety.

Such anxiety towards the usage of computers would lead to distrust and fear towards online activities which includes sending out electronic mails, usage of social media, purchasing items online and any other online activities.

This, consequently, leads to older generations such as the Gen X and baby boomers to be hesitant towards utilising technologies and online platforms that provide abundance of services.

CASE STUDY #2

The second study group is about susceptibility towards persuasion and vulnerability towards online fraud which is caused by a lack in awareness on online safety. According to Statista, there are estimated 29 million smartphone users in Malaysia who spend a daily average of 7.5 hours on the Internet with 2.45 hours on social media alone [4]. A survey done by AARP shows that a combination of online behaviours and life experiences can make an individual more vulnerable to online frauds [5]. According to CYBER999 Help Centre, fraud purchase, romance scam and job scam, as well as investment fraud are the most common incidents reported. Fraudsters often exploit desperation and trust to lure victims. For example, an exceptional good offer with promise of easy money.

Lack of awareness is another key factor contributing to financial and online fraud. Victims are unaware of the common tactics used by fraudsters, thus making them easy targets. At times, fraudsters also pretend to be enforcement officers to manipulate their victims and lure them into providing crucial information such as their identity card number and banking details. This incident was heightened during the beginning of Covid-19 pandemic.

Victims often blame themselves for falling prey to frauds and this has resulted in them to be less

engaging online and reduce their time spent on social media platform.

Challenges

The challenges and hesitations from the older generations will lead to the younger generations being far ahead in technological advancement and being able to adapt faster to development. In a way, the development of technology correlates to the development of the younger generations in order to serve their needs.

Older generations such as baby boomers did not have the necessity for technology which led to slower technological advancement and a limited source of information to focus on. This is different from younger generations who have a higher necessity towards technology.

Younger generations will continue to drive technological advancement and integration faster than previous generations, allowing technology to adapt more quickly to serve the needs of all. They will continue to have more digital distractions from social media, and many potential sources of information to manage.

For older generations such as baby boomers who have lived in a world with less digital technology, they will have less information to manage.

The Internet has certainly created a revolutionary impact in everyday communications and transactions. It has become the fastest mode to perform various task effectively. It has changed the way we lead our everyday life while social media and email have become the most utilized platforms for interaction, entertainment and information search.

Due to limited reach in digital literacy and cyber security knowledge, baby boomers may be more susceptible to online predators. In addition, they may experience information overload [6], leading to possible psychological distress.

Recommendation

Understanding the basic knowledge of security to keep themselves safe online is crucial. For example, these are 8 basic security tips in order to keep their phone safe.

1. Avoid giving out personal information.

2. Use numbered pin, security pattern or a password to keep the phone locked.
3. Download applications only from Playstore or App Store and do not download applications from pop-up advertisements.
4. Always back up data to another source.
5. Keep updated with the latest operating systems.
6. Turn off WiFi and Bluetooth when not in use.
7. Log out from bank applications after payment.
8. Be extra careful towards the possession of the smart phones.

Since the majority of application technology used by baby boomers involve smart phone, and social media such as Facebook, it is recommended that they learn and understand the best practices and security of smart phones and social media. Despite having to catch up on digital technology, baby boomers can count on a consistent support and guidance to leverage new technology.

For Facebook users among baby boomers, they must learn some basic common sense tips to stay safe:

9. Always review the privacy settings.
10. Approve only the friends that you know personally and do not approve friends randomly.
11. Do not click on suspicious app links or sketchy 'quizzes'.
12. Think twice before posting.

Summary

Embracing and empowering baby boomers in this digital age is an excellent initiative to enhance cyber security. In fact, not all baby boomers have low digital literacy, some have in fact become experts. Be that as it may, every digital citizen needs to learn and apply best security practices while using smart phones or accessing social media. Younger generations and application developers are encouraged to be more inclusive of the older generations to close the digital gap.

References

1. <https://www.kasasa.com/exchange/articles/generations/gen-x-gen-y-gen-z>
2. <https://www.igi-global.com/dictionary/computer-anxiety/5019>
3. Achim, N. and Al Kassim, A. (2015). "Computer usage: the impact of computer anxiety and computer self- efficacy". *Procedia - Social and Behavioural Sciences* 172 (2015) 701-708.
4. <https://www.statista.com/statistics/494587/smartphone-users-in-malaysia/>
5. https://www.aarp.org/content/dam/aarp/research/surveys_statistics/econ/2014/Caught-Scammer-Net-Risk-Factors-Internet-Fraud-Victims.doi.10.26419%252Fres.00076.001.pdf
6. <https://www.interaction-design.org/literature/topics/information-overload>
7. <https://www.ncr.com/blogs/baby-boomers-going-digital>
8. <https://www.verizon.com/articles/8-common-sense-tips-to-keep-your-smartphone-secure/>
9. <https://ktconnections.com/blog/4-common-sense-tips-to-stay-safe-on-facebook-1>

The OIC-CERT Global Cybersecurity Award

By | Ahmad Nasir Udin Mohd Zin, Raja Nur Zafira Raja Sharudin & Khairul Akma Mahamad

Introduction

International co-operation and collaboration are essential in mitigating cyber threats in our borderless world. As such, managing international relations is key to strengthening regional cyber security. The International Engagement Department of CyberSecurity Malaysia is responsible for managing international relations for CyberSecurity Malaysia¹, an agency under the purview of the Ministry of Communications and Multimedia, Malaysia. One of the major functions of the International Engagement Department is being the Permanent Secretariat of the Organisation of Islamic Cooperation – Computer Emergency Response Teams (OIC-CERT). One of the key initiatives of the OIC-CERT international collaboration is capacity building through the introduction of the OIC-CERT Global Cybersecurity Award.

The OIC-CERT

CyberSecurity Malaysia has been playing an important role in managing international relations through active participation in the Organisation of Islamic Cooperation – Computer Emergency Response Teams (OIC-CERT). CyberSecurity Malaysia is currently the Permanent Secretariat of the OIC-CERT and has been entrusted with this responsibility since 2012.

The Organisation of Islamic Cooperation – Computer Emergency Response Teams (OIC-CERT) was established with a vision to be the leading cyber security platform and to make cyber world a safer place.² The OIC-CERT is a collaboration of Computer Emergency Response Teams from countries within the Organisation of Islamic Cooperation (OIC) region. It currently has 55 members from 27 countries, and it is managed by the OIC-CERT Board.

The OIC-CERT Global Cybersecurity Award

The OIC-CERT has developed a strategic business plan led by the OIC-CERT Board Members. The OIC-CERT Business Plan consists of 6 strategic pillars. One of the Pillars – Pillar 5 is specifically on Capacity Building which is being led by Cybersecurity Malaysia and one of the action plans in this pillar is organising the Cybersecurity Innovation Competition. In the early 2021, the Board has agreed to establish the OIC-CERT Global Cybersecurity Award³.

The main idea behind this Award is to recognize the best individuals, teams or companies who have developed beneficial and innovative cyber security project. The Board will be judging on the excellence, value propositions and the innovation behind the project as the core criteria to win. The core criteria for the award are excellence, value proposition and innovativeness.

The OIC-CERT Global Cybersecurity Award (Award) is an initiative to encourage international collaboration in the cybersecurity domain and by recognising these innovative cybersecurity projects from around the world, which contribute to the uplifting of the ummah with a positive impact while promoting digital realm. This initiative is congruent with the OIC-CERT's vision to be the leading cybersecurity platform that provides the world with a safer cyber space with a mission of developing cybersecurity capabilities to mitigate cyber threats through global collaboration.

The Award will serve as a recognition for the recipient's exceptional excellence and innovation in accordance with the OIC-CERT vision and mission. The Award will be bestowed on selected project(s) that address one or more key areas, but not limited to the following:

1. People: capacity building abilities, awareness, teaching and learning.

¹ https://www.cybersecurity.my/en/our_services/ge_me/main/detail/2336/index.html

² <https://www.oic-cert.org/en/introduction.html>

³ <https://www.oic-cert.org/en/awards.html>

2. Processes: Policymaking, governance, norms, and entrepreneurship; and/ or
3. Technology: systems, solutions, and innovation.

The Award is open to all entities, members, and non-members of OIC-CERT, representing governments, the private sector, international and regional institutions, civil societies, and the academia.

Theme

The theme of the Award will be decided by the Award Committee on a yearly basis. The theme for the inaugural Award in 2021 is Cybersecurity Innovation Towards Society Prosperity and Wellbeing.

Winner

Only one (1) award will be announced yearly during the OIC-CERT Annual Conference. The winner will be awarded with USD1,000.

Call for Submission

The Award Committee has opened a call for submissions for all related projects for the “OIC-CERT Global Cybersecurity Award” and it will be closed by 31st August each year. Call for submission for the subsequent OIC-CERT Global Cybersecurity Awards will be announced in the OIC-CERT website. As stated above, the Award will be open to all entities representing governments, the private sector, international and regional institutions, civil society and the academia as stated above.

The Award is intended to encourage people around the world to develop and implement innovative cybersecurity projects, regardless of country, that contributes to uplifting the ummah with positive impacts while promoting the digital realm. It is expected that each project will impact the ummah, from the young, women and all other minority groups.

For project nomination, stakeholders are requested to complete a submission form for the “OIC-CERT Global Cybersecurity Award” at the following link: <https://www.oic-cert.org/globalprize/form>.

Rules And Guidelines

These are the official rules and guidelines of the Award:

- a. Submissions must be done through the OIC-CERT websites and all details requested in the questionnaire must be completed based on the project category.
- b. The project descriptions should contain information about the respective goals, a brief overview, results, challenges, and proposed follow-up phases or improvements. Reference for the documents should cite figures and online links.
- c. Initiative submitted should undergone major phases in order to be able to provide evidence of the outcomes.
- d. The deadline for submission is 31st August each year. The submission deadline is strictly adhered to. Late submissions will not be accepted.
- e. All submissions must be in English.
- f. A panel of judges selected by the Award Committee, in its sole discretion, will review all eligible entries submitted during the period.
- g. The decision in relation to every aspect of the contest shall be deemed final and conclusive under any circumstances. No further appeal, enquiry and/or correspondence will be entertained.
- h. By submitting an entry, participants agree to be bound by the Terms and Conditions set forth herein. The OIC-CERT may discontinue or terminate the contest at any time at its sole discretion.

Evaluation Criteria

Each judge from the panel will review their assigned applications independently, using the Evaluation Criteria Scoring Sheet, and identify individual's strengths and weaknesses based on the evaluation criteria outlined below:

- a. Concept and Design including opportunity, conception, method, and development:
 - i. Innovation addressing the needs and solving problems faced by the ummah.
 - ii. Creation of new opportunities for the ummah.

- iii. Overall method and concept development.

b. Impact which includes sustainability, social responsibility, and potential:

- i. The immediate and long-term impact the initiative has on the ummah as a whole.
- ii. How can the initiative be a part of a larger platform for future innovation and development?
- iii. Empowerment of the ummah.

c. Value including the need, differentiation, cost, and achievement:

- i. How does the initiative meet an existing need or create new needs?
- ii. How the offering is different and have game changing advantages over others?
- iii. Unique value proposition, cost and benefits and economic desirability.

d. Delivery includes messaging, engagement, availability, and achievement:

- i. How was the initiative communicated?
- ii. How the ummah was engaged in delivering the initiative and its availability?
- iii. The value proposition of the initiative being achieved, fulfilled, and validated by the ummah.

The Way Forward

All Members of the OIC countries, Affiliate Members and Associates are invited to participate actively in implementing the OIC-CERT Global Cybersecurity Award outcomes, maintained by OIC-CERT and to carry out further adaptation to the information society; as well as to support activities relating to the implementation of the OIC-CERT Global Cybersecurity Award outcome.

For further information, clarification, or any enquiries about the OIC-CERT Global Cybersecurity Award, please contact the OIC-CERT Secretariat at secretariat@oic-cert.org.

Reference

1. <https://www.cybersecurity.my/en/index.html>
2. <https://www.oic-cert.org/en/index.html>
3. <https://www.oic-cert.org/en/awards.htm>

The 2021 Result

For the OIC-CERT Cybersecurity Global Award 2021, two initiatives were selected as the joint-winners of the inaugural OIC-CERT CyberSecurity Global Award. The initiatives were "Making The World a Safer Place with Passwordless Blockchain Secure Authentication" by FNS (M) Sdn. Bhd., Malaysia and "The Dera' Training Initiative" by Huawei Technologies Co.,Ltd, Kingdom of Saudi Arabia. The result was announced during the 13th Annual OIC-CERT Conference 2021 and the 9th Arab Regional Cybersecurity Summit 2021 held on 23-24 November 2021.

Securing Data In Cloud Using BYOE And BYOK

By | Nor Azeala Mohd Yusof

What is Cloud Computing?

Cloud computing has been identified as one of the major emerging components of computer technology providing hosted services over the Internet. Cloud computing services are provided by data centers located in different parts of the world and it can be accessed from any supporting device through a cloud service provider (CSP). Some well-known CSP's are Amazon Web Services (AWS), Google Cloud Platform (GCP), IBM Cloud, Oracle Cloud, and Microsoft Azure.

Cloud computing can be further classified into three models:

a. Infrastructure-as-a-Service (IaaS)

- vendor runs and manages all physical compute resources and the required software to enable computer virtualization
- customer deploys virtual machines in hosted datacenters
- IaaS consumers have control over the configuration and management of operating systems
- Cloud vendor controls the underlying infrastructure
- Example: Azure Virtual Machine

b. Platform-as-a-Service (PaaS)

- customers deploy their application into an environment provided by the cloud service vendor
- vendor takes care of infrastructure management
- customer can focus on application development and data management
- Example: Azure App Service and Azure Cloud Services

c. Software-as-a-Service (SaaS)

- Is a centrally hosted and managed software

- Usually based on a multitenant architecture—a single version of the application is used for all customers
- Can be scaled out to multiple instances to ensure best performance across all locations
- SaaS software is typically licensed through a monthly or annual subscription
- Vendors are responsible for every component in the software stack, therefore customers only need to manage the services provided
- Example: Microsoft 365

Attacks on Cloud Computing

Security vulnerabilities and challenges arise from the usage of cloud computing services. The software, hardware, and infrastructure are maintained and operated by a third party. A research by Aljumah and Ahanger (2020) showed that there are several types of threats against cloud computing. Some of the major threats are:

- Data breaches
- Data loss
- Account or traffic hijacking
- Insecure interfaces and application program interfaces (APIs)
- Denial of services (DoS)
- Malicious insiders
- Abuse of cloud services
- Shared technology vulnerabilities
- Virtualization attack
- Cloud malware injection

Securing Data in Cloud

The shared responsibility model for cloud security can be categorised into two components:

- Cloud infrastructure security (provider's responsibility)
- Cloud data security (customer's responsibility)

Figure 1 illustrates some or all the responsibilities of a provider and customer for components in the computing stack in each cloud computing model. This illustration is an example established by Microsoft Azure.

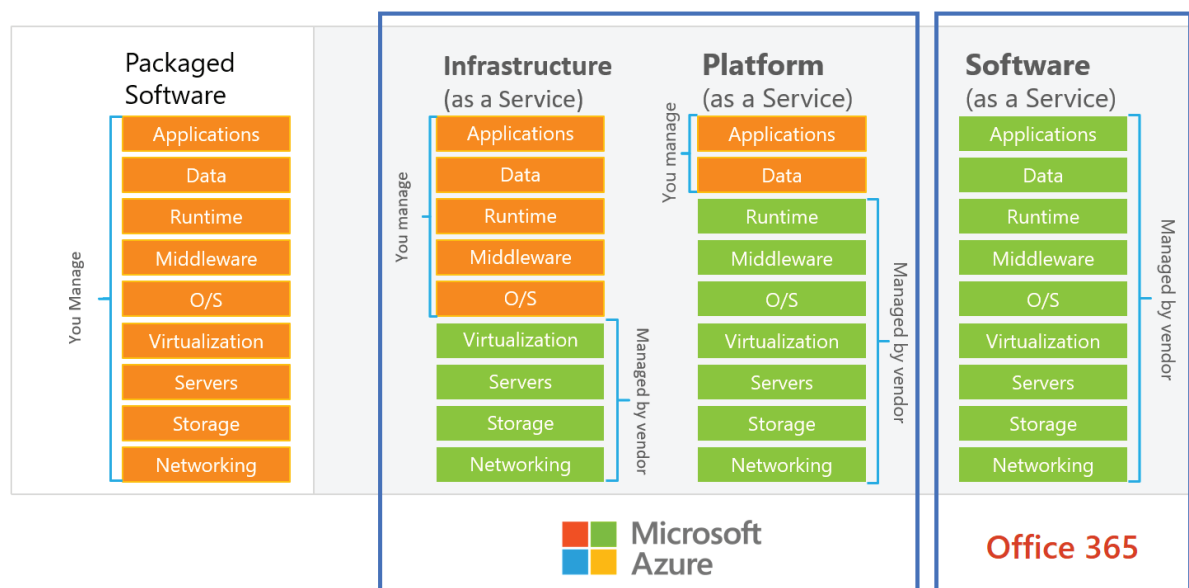


Figure 1: Responsibilities of a Provider and Customer on Cloud Computing Models

All CSPs should support data integrity, confidentiality, and availability. Data security in cloud can be strengthened by implementing the least privileged model, auditing activities across your environment, categorizing sensitive data, using data masking techniques such as encryption, and ensuring cloud providers offer an SLA that meets the availability requirements. Bhati (2020) has classified data security in cloud computing into four stages:

- Stage 1:** Encrypt in software
- Stage 2:** Use cloud Key Management Services (KMS)
- Stage 3:** Bring Your Own Key (BYOK)
- Stage 4:** Bring Your Own Encryption (BYOE)

Numerous encryption methods can be used to perform encryption in a software as mentioned in Stage 1, but this is the minimum way of securing data in the cloud. The second stage is by using cloud KMS which allows data to be secured using a native encryption solution, but

it is fully controlled by the CSP. Therefore, to secure sensitive data, it is recommended to use the BYOK method. Meanwhile, if the data is highly sensitive, it is highly advisable to use the BYOE concept.

Differences between BYOK and BYOE

Bring Your Own Key (BYOK) is a solution for controlling and protecting data in the cloud using cryptographic keys that are securely generated at a customer's premise using the customer's own Hardware Security Module (HSM). This will allow enterprises to control their keys, produce their master key, and rely on their HSM which is then transmitted to the HSM within the cloud. Since the master key lies in the enterprise's HSM and not the cloud service provider's HSM, data owners may believe that their data is secured. Cates (2017) divides BYOK architectures into three types:

a. Customer Master Key Import

This architecture allows customers to create and export keys to cloud providers as a master key to protect either their data or data keys. Figure 2 shows its architecture and the steps are as follow:

1. Create "Import Key" in the cloud
2. Import Public Key to your HSM or OpenSSL
3. Create AES Master Key in HSM or OpenSSL
4. Export Master Key wrapped with Public Import Key
5. Import Wrapped CKM to cloud.

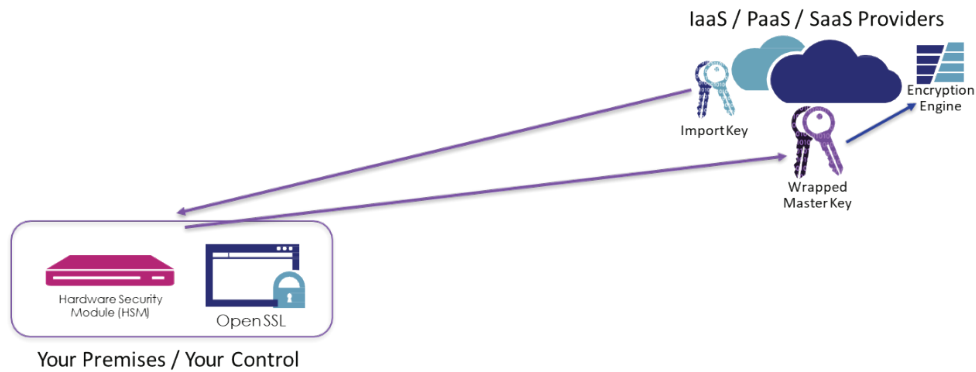


Figure 2: Architecture of Customer Master Key Import

b. Derived Key Creation

This architecture allows customers to deliver Master Keys trusted by the provider to create derived keys for usage in the provider's native encryption. Figure 3 shows its architecture and the steps are as follow:

1. Cloud Provider's Key is encrypting
2. Create your key in HSM or OpenSSL
3. Wrap and send your key to your cloud provider
4. Both keys are combined mathematically
5. New key is controlled by you

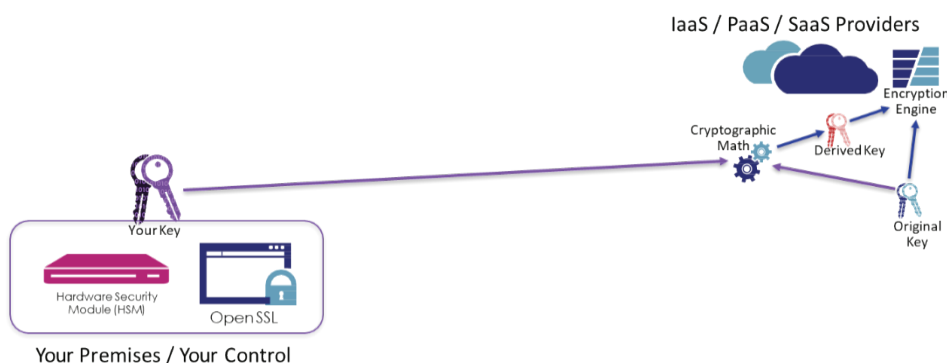


Figure 3: Architecture of Derived Key Creation

c. Hold Your Own Key (HYOK)

This architecture allows providers to call customer-hosted services for encryption, key decryption, or key provisioning services. Figure 4, 5, and 6 shows its architecture in three different scenarios.

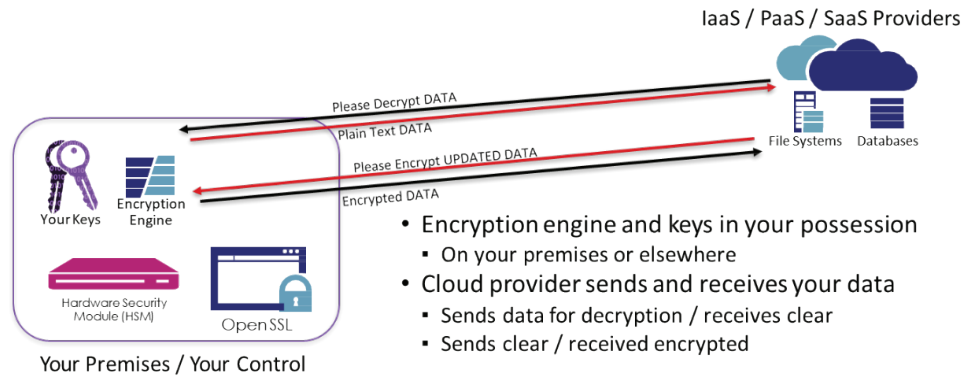


Figure 4: Architecture of Hold Your Own Key (Scenario 1)

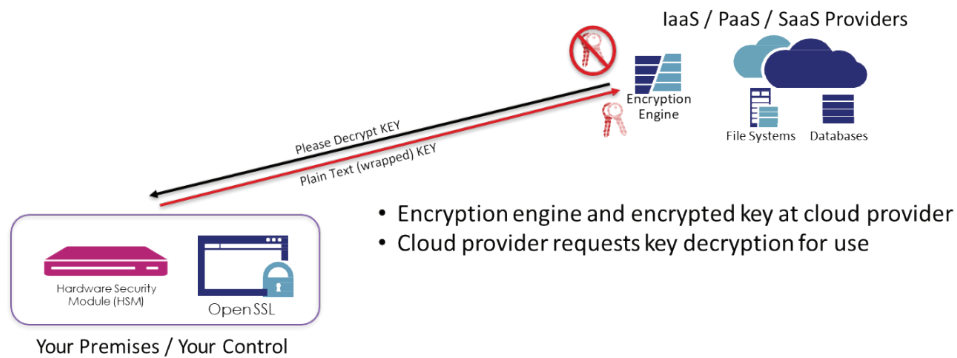


Figure 5: Architecture of Hold Your Own Key (Scenario 2)

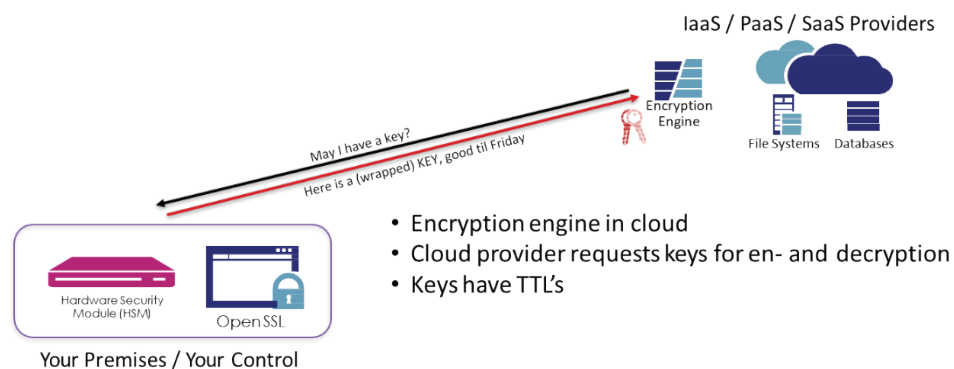


Figure 6: Architecture of Hold Your Own Key (Scenario 3)

On the other hand, Bring Your Own Encryption (BYOE) is a cloud computing security model that allows cloud service customers to use their encryption software, manage their keys, and deploy a virtual instance of their encryption software, alongside the business application they are hosting in the cloud. BYOE can be applied to data at rest, data in motion, and also data in use. Organizations that are required to address regulatory compliance and data privacy are fit to use this BYOE security model due to its ability in avoiding data replication and data loss from a breach. BYOE also offers a new class of privileged users. Some of the cloud service providers that support BYOE are Microsoft Azure, Amazon Web Service (AWS), Google Cloud, and IBM Cloud.

Availability of solutions that support BYOE and BYOK in the market

There are a few products that support BYOK principles available in the market. CipherTrust Cloud Key Manager is one such security solution that supports IaaS, PaaS, and SaaS providers such as Microsoft Azure, IBM Cloud, Google Cloud Platform, and Amazon Web Service (AWS). This solution provides cloud consumers with a cloud management service that delivers strong controls over encryption key life cycles for data encrypted by cloud services. Indirectly, it supports CSP's BYOK APIs, cloud key management automation, and key usage logging and reporting. The details on this product can be accessed at <https://cpl.thalesgroup.com/encryption/key-management/ciphertrust-cloud-key-manager>.

On the other hand, there are various solutions that offer advanced multi-cloud BYOE tools to secure data and reach compliance rapidly and effectively. The cloud security solution give additional security to native encryption provided by CSPs. This allows encryption to happen outside of clouds and ensuring anything entering and exiting the cloud is encrypted. Below is the list of cloud security solutions that supports BYOE with its reference links for extra information:

- Fernetix Vaultcore (<https://www.fernetix.com/>)
- Fortinet Cloud Access Security Brokers (CASBs) (<https://www.fortinet.com/products/cloud-access-security-broker>)

- CipherTrust Transparent Encryption (<https://cpl.thalesgroup.com/encryption/transparent-encryption>)
- CipherTrust Transparent Encryption Live Data Transformation (<https://cpl.thalesgroup.com/encryption/transparent-encryption-live-data-transformation>)
- CipherTrust Application Data Protection (<https://cpl.thalesgroup.com/encryption/application-data-protection>)
- CipherTrust Tokenization (<https://cpl.thalesgroup.com/encryption/tokenization>)
- CipherTrust Transparent Encryption Container Security (<https://cpl.thalesgroup.com/encryption/container-security>)
- CipherTrust Security Intelligence Log (<https://cpl.thalesgroup.com/encryption/transparent-encryption-security-intelligence-logs>)
- CipherTrust Manager (<https://cpl.thalesgroup.com/encryption/ciphertrust-manager>)

Summary

On 8th September 2020, FDPIC, a Swiss data protection authority concluded in its annual review that the Swiss-US Privacy Shield does not provide an adequate level of protection for personal data transfer between Switzerland and the US or other third countries. Based on the findings, FDPIC delivered some practical advice to Swiss companies. Some of the recommendations are:

- a. Swiss data exporters should conduct a case-by-case risk assessment of data transfers in reliance on Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs).
- b. Swiss data exporters should specifically consider whether the foreign recipient company can provide necessary cooperation for the enforcement of Swiss data protection principles. If not, the SCCs cannot be complied with, and cannot alone provide an adequate level of protection.
- c. If the foreign recipient company cannot provide such necessary cooperation, the Swiss data exporter must consider technical measures that effectively prevent authorities in the destination country from accessing the transferred personal data.

From the given examples, the annual review has stated that data stored in the cloud must be protected using any encryption methods by implementing the principles of BYOE and BYOK. Hence, it can be considered that the BYOE and BYOK concepts are among the best methods to secure data in clouds specifically to public clouds that uses native encryption.

References

1. Aljumah, A., & Ahanger, T. A. (2020). *Cyber Security Threats, Challenges and Defence Mechanisms in Cloud Computing*. *IET Communications*, 14(7), 1185-1191.
2. Bhati M. (2020, May). *Bring Your Own Encryption*. BrightTALK. Retrieved from https://www.brighttalk.com/resource/core/272213/bring-your-own-encryption_605321.pdf
3. Cates S. (2017, February 13-17). *BYOK: Leveraging Cloud Encryption Without Compromising Control* [Conference presentation]. RSA Conference 2017, San Francisco. Retrieved from <https://published-prd.lanyonevents.com/published/rsaus17/sessionsFiles/4579/CSV-F03-BYOK-Leveraging-Cloud-Encryption-Without-Compromising-Control.pdf>
4. *Get started for Azure IT operators*. (2018). Retrieved from <https://docs.microsoft.com/en-us/azure/guides/operations/azure-operations-guide>
5. *Swiss Privacy Shield Policy Paper*. (2020, September). Retrieved from <https://www.news.admin.ch/newsd/message/attachments/64261.pdf>

Quick Facts On Privacy Information Management Systems

By | Nahzatulshima Zainuddin & Mohd Haleem Bin Abdul Sidek

ISO/IEC 27701 is the international standard for Privacy Information Management System (PIMS). It was published in August 2019 as an extension to ISO/IEC 27001 Information Security Management System (ISMS) and ISO/IEC 27002 information security controls in the context of privacy management. An organization that goes for PIMS certification must have been certified with ISO/IEC 27001 Information Security Management System (ISMS) or at least to be certified together with ISMS. To better understand PIMS, below are a few important facts to begin with.

5 Quick Facts on PIMS

1 What is PIMS?

PIMS specifies the requirements and provides guidance for establishing, implementing, maintaining and continually improving a privacy information management system (PIMS).

PIMS covers how organizations should implement robust data processes and controls to protect privacy. In addition, PIMS could also assist in demonstrating compliance with privacy regulations that may apply.

2 Who should get PIMS Certification?

PIMS applies to any organization holding responsibility and accountability for PII (personally identifiable information) processing either as PII controllers or PII processors. Organizations of all sizes and types, including public and private companies as well as governmental entities and other types of organization, can benefit from PIMS.

3 What is Personal Information?

Or also known as Personally identifiable information (PII) is any data that can be used to identify a specific **INDIVIDUAL**. IC Number, mailing or email address, medical records and phone numbers are common examples of PII, but technology has expanded the scope of PII to include an IP address, login IDs, or digital images. Geolocation, biometric, and behavioural data can also be classified as PII.



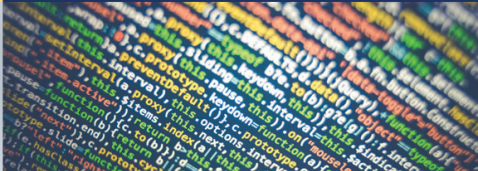
4 What are roles defined in PIMS?

- PII Principal:**
An individual to whom the personally identifiable information (PII) relates.
- PII Controller:**
An entity that determines the purpose and means for processing PII, defines why and how PII is processed, and is responsible for the implementation of privacy and security protocols to meet applicable legal standards.
- PII Processor:**
An entity that processes personally identifiable information (PII) on behalf of and in accordance with the instructions of a PII controller.



5 What are auditable clauses in PIMS?

- Clause 5: PIMS-specific requirements related to ISO/IEC 27001
- Clause 6: PIMS-specific guidance related to ISO/IEC 27002
- Clause 7: Additional ISO/IEC 27002 guidance for PII controllers
- Clause 8: Additional ISO/IEC 27002 guidance for PII processors
- Annex A: PIMS-specific reference control objectives and controls (PII Controllers)
- Annex B: PIMS-specific reference control objectives and controls (PII Processors)



To be certified with PIMS, an organization must first implement an effective management system that complies with the requirements of the standards. Besides the standards, a reference could also be made to ISO/IEC 29100:2011 which provides a privacy framework applicable to any system or service that requires PII processing. It is also important for the organization to set clear targets for implementation and assessment. Before certification, the organization must perform internal audits to identify potential gaps and a management review to review and evaluate the effectiveness of its Management System. One of the most important things to remember is that development, implementation and certification of a management system is a continuous journey, the certification audit representing one element of a continuous improvement process.

References

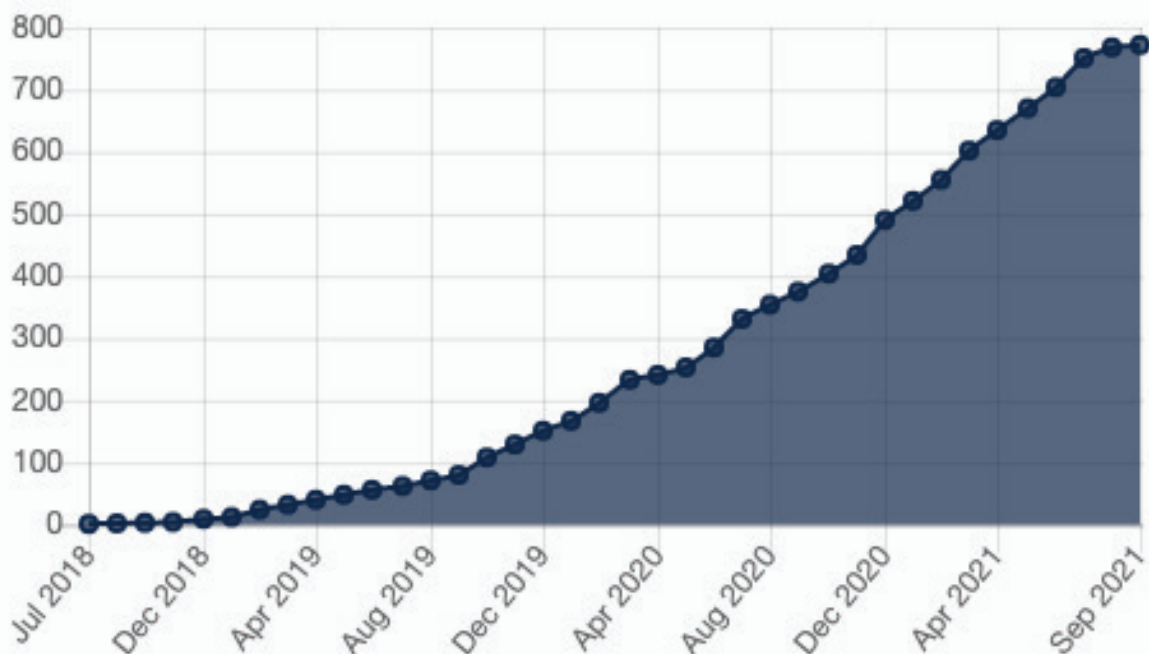
1. ISO/IEC 27701:2019 *Personal Information Management Systems*
2. ISO/IEC 29100:2011 *Privacy Framework*

The Impact Of GDPR Enactment

By | Nahzatulshima Zainuddin & Mohd Haleem Bin Abdul Sidek

Protection of privacy has increasingly become a great concern for many countries all over the world. This is evident through the global proliferation of privacy laws and regulation due to pressures from customer, end-users, investors and regulators on the handling of the personal identifiable information (PII). The enactment of wide-influence privacy law, the EU General Data Privacy Regulation (GDPR), has compelled many organizations to look at the issue of privacy more seriously.

According to a statistics done by The CMS.Law GDPR Enforcement Tracker, the trend shows that the number of fines has greatly increased from only few cases in year 2018 to nearly thousand cases in year 2021. This trend will sooner or later be expanding to other region as well.



Number of GDPR fines from 2018 - 2021

With the number of complaints and fines related to privacy and data protection on the rise, there seems to be a growing need for guidance. ISO/IEC 27701 Personal Information Management Systems (PIMS) is an ideal tool to help organization in complying to the legal requirements as well as in managing privacy risks effectively.

Below are some examples of GDPR recent fines.

TOP 5 BIGGEST GDPR FINES

01

€746M



Amazon (July 2021)

Supervisory Authority :

National Commission for Data Protection (CNDP), Luxembourg

Issues :

Infringements regarding Amazons' advertising targeting system that was carried out without proper consent.

02

€225M



WhatsApp (Sep 2021)

Supervisory Authority :

Data Privacy Commission (DPC), Ireland

Issues :

The platform was not transparent about how it shared data with its parent company, Facebook. This includes information provided to data subjects about the processing of information.

03

€50M



Google (Jan 2019)

Supervisory Authority :

National Commission on Informatics and Liberty (CNIL), France

Issues :

Lack of transparency, inadequate information, lack of valid consent regarding the ads personalization.

04

€35.3M

Hennes & Mauritz – H&M (Oct 2020)

Supervisory Authority :

Data Protection and Freedom of Information (BfDI), Germany

Issues :

The company collected sensitive personal data (employees' holiday experiences, family issues, religious beliefs, and symptoms of illness and diagnoses.) of their employees through whispering campaigns, gossip, and other sources to create profiles of employees and used that data in the employment process.

05

€27.8M

TIM (Jan 2020)

Supervisory Authority :

Italian Data Protection Authority (Garante), Italy

Issues :

TIM, a telecommunication operator has contacted non-customers multiple times (certain numbers over 150 times per month) without proper consent or other legal bases. Few million individuals were affected by their aggressive marketing strategy.

References

1. <https://www.enforcementtracker.com/>
2. <https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9256409>
3. <https://www.nst.com.my/world/world/2021/07/713346/amazon-fined-us880-million-luxembourg-over-data-security>
4. <https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc>
5. <https://www.bbc.com/news/technology-58422465>
6. <https://www.bbc.com/news/technology-54418936>

Redundant Array Independent Disks (RAID): RAID Levels

By | Mohd Nor A'kashah Mohd Kamal, Mohd Faisal Abdullah & Nur Fazila Selamat

What is RAID?

Redundant Array of Independent Disk or also known as, RAID, is a collection of hard drives, one or more controller cards and embedded software to increase the reliability and redundancy of data storage on hard drives [1]. In other words, RAID is a system of storing the same data in different places, across multiple hard drives or solid-state drives (SSDs) to protect the data in case of a drive failure [2]. A RAID system consists of two or more drives working in parallel [3]. These can be hard drives, but there is a trend to also use the technology of SSD (Solid State Drives).

Levels of RAID

Data is distributed across the drives in one of several ways, which is referred as the RAID levels, depending on the required level of redundancy and performance. The different data distribution layouts are named as "RAID" followed by a number, for example RAID 0 or RAID 1. Each RAID level provides different key goals such as different level of reliability, availability, performance, and capacity [4].

Below is an overview of the most popular RAID levels [2][3]:

a. RAID LEVEL 0 – STRIPING

In a RAID 0 system data is split up into blocks that gets written across all the drives in the array. By using multiple drives (at least 2) at the same time, this offers superior input output (I/O) performance.

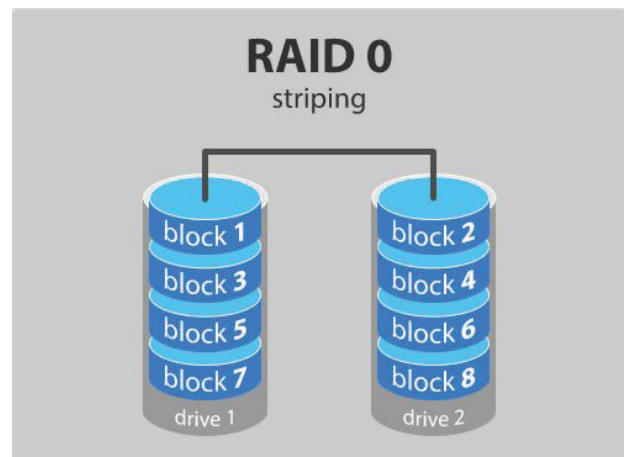


Image 1: RAID 0 – Striping Method

Ideal use

RAID 0 is ideal for non-critical storage of data that has to be read/written at a high speed, such as on an image retouching or video editing station.

b. RAID LEVEL 1 – MIRRORING

Data is stored twice by writing them to both the data drive (or set of data drives) and a mirror drive (or set of drives). If a drive fails, the controller uses either the data drive or the mirror drives for data recovery and continuous operation. You need at least 2 drives for a RAID 1 array.

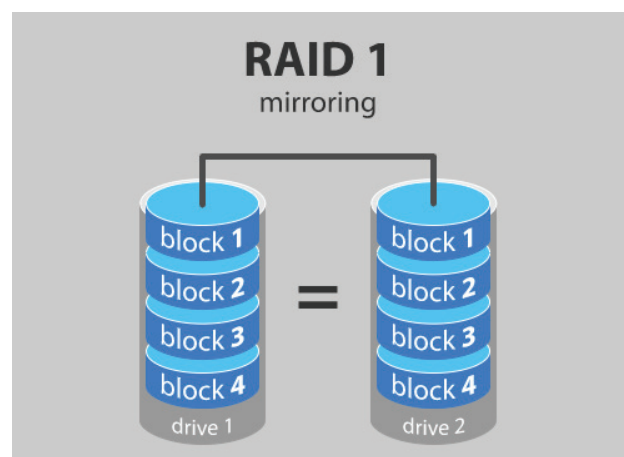


Image 2: RAID 1 – Mirroring method

Ideal use

RAID 1 is ideal for mission critical storage, for instance accounting systems. It is also suitable for small servers in which only two data drives will be used.

c. RAID LEVEL 5 – STRIPING WITH PARITY

RAID 5 is the most common and secure RAID level. It requires at least 3 drives but can work with up to 16. Data blocks are striped across the drives and on one drive a parity checksum of all the block data is written. The parity data are not written to a fixed drive. Rather they are spread across all drives, as the drawing below shows. Using the parity data, the computer can recalculate the data of one of the other data blocks, should those data no longer be available. That means a RAID 5 array can withstand a single drive failure without losing data or the access to data.

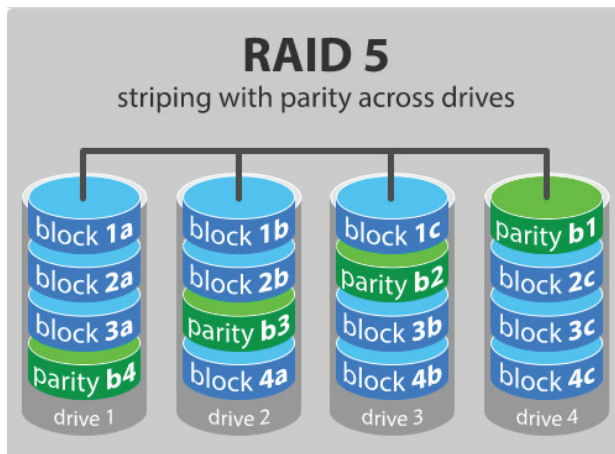


Image 3: RAID 5 – Striping with Parity across Drives Method

Ideal use

RAID 5 is a good all-round system that combines efficient storage with excellent security and a decent performance. It is ideal for file and application servers that have a limited number of data drives.

d. RAID LEVEL 6 – STRIPING WITH DOUBLE PARITY

RAID 6 is similar to RAID 5, but the parity data are written to two drives. That means it requires at least 4 drives and can withstand 2 drives failing simultaneously. The chances of two drives breaking down at exactly the same moment are very small. However, if a drive in a RAID 5 systems fails and it is replaced by a new drive, it takes hours or even more than a day to rebuild the swapped drive. If another drive dies during that time, you still lose all of your data. With RAID 6, the RAID array will even survive that second failure.

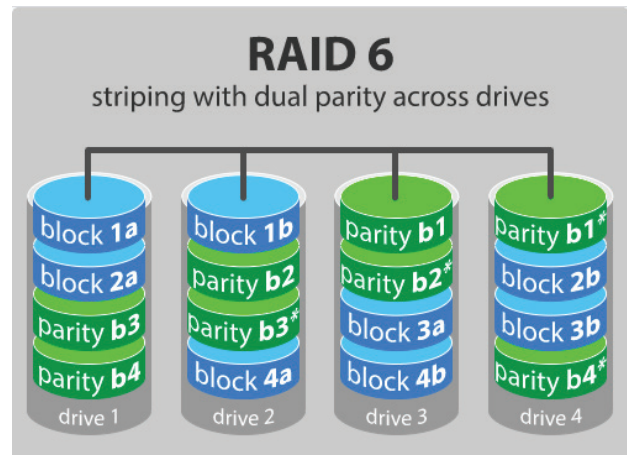


Image 4: RAID 6 – Striping with Dual Parity Across Drives Method

Ideal use

RAID 6 is a good all-round system that combines efficient storage with excellent security and a decent performance. It is preferred over RAID 5 in file and application servers that use many large drives for data storage.

e. RAID LEVEL 10 – COMBINING RAID 1 & RAID 0

It is possible to combine the advantages (and disadvantages) of RAID 0 and RAID 1 in one single system. This is a nested or hybrid RAID configuration. It provides security by mirroring all data on secondary drives while using striping across each set of drives to speed up data transfers.

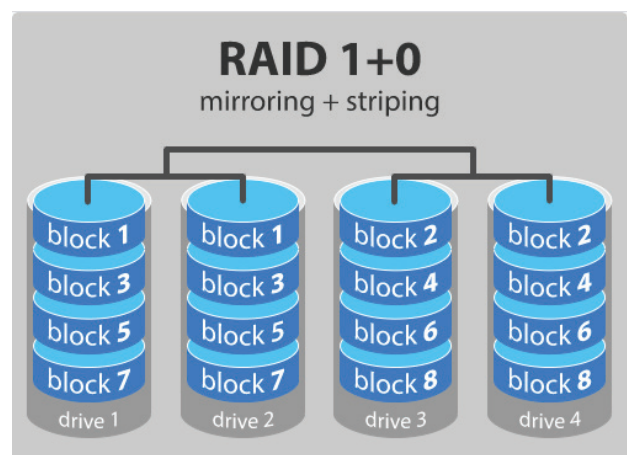


Image 5 : RAID 1+0 – Mirroring and Striping Method

Ideal use

RAID 10 or RAID 1+0 delivers very high input output rates by striping RAID 1 (mirrored) segments. This RAID mode is good for business with critical database management solutions that require maximum performance and a high fault tolerance.

Advantages and Disadvantages of RAID Levels

Each RAID level has its own advantages and disadvantages and also provides different key goals. Below is the comparison table between each RAID levels [5] [6]:-

RAID Level	Method/Description	Key Goal(s)	Advantages	Disadvantages
RAID 0	Striping - Data is split evenly between two or more drives.	Performance	Large size, fastest speed and easy to implement.	No redundancy
RAID 1	Mirroring - Two or more drives have identical data on them.	Data Protection	A single drive failure will not result in data loss.	Speed and size are limited by the slowest and smallest drive.
RAID 5	Striped drives with distributed parity -Data is split evenly between three or more drives. Parity is split between drives.	Data Protection and Speed	Large size, fast speed, and redundancy.	The total array size is reduced by parity.
RAID 6	Striped drives with dual distributed parity - Data is split evenly between four or more drives. Parity is split between two drives.	Data Protection and Speed	Large size, fast speed, redundancy and more protection than RAID 5.	The total array size is reduced by parity. Write data transactions are slower than RAID 5 due to the additional parity data that has to be calculated.
RAID 10	1+0; Striped set of Mirrored Subset - Four or more drives are made into two mirrors that are striped.	Data Protection (High Reliability) and Performance	Larger size and higher speed than RAID 1, and more redundancy than RAID 0.	No parity. Compared to large RAID 5 or RAID 6 arrays, this is an expensive way to have redundancy.

Conclusion

In this era of rapid technological change, technology has offered an array of solutions for data protection specifically in data redundancy and the RAID system is one of the available options that we could think of. RAID is a data storage technology that joins multiple physical drives (HDD or SSD) into a single unit. Depending on how RAID is implemented, it can offer improved input, output, speed and reduced downtime (or a combination of the two – speed and downtime) Moreover, it will be able to increase redundancy to ensure data

safety. RAID 0 is best suited for applications that require high-speed data performance. RAID 1 is best for applications that are not speed intensive but require high data integrity. Meanwhile, RAID 5 and RAID 6 are suitable for applications that require combinations of high-speed and data protection, while RAID 10 is perfect for combination of high-speed data performance and redundancy for application. However, regardless of the benefits that RAID could offer, the choice of solution is still depending on the company or to the individual's preference to meet their level of system reliability, performance and availability.

References

1. *Raid in Industrial Computer Systems*. Retrieved from <https://cp-techusa.com/knowledge-zone/whitepapers/raid-in-industrial-computer-systems/>
2. *RAID (redundant array of independent disks)*. Retrieved from <https://searchstorage.techtarget.com/definition/RAID>
3. *RAID*. Retrieved from <https://www.prepressure.com/library/technology/raid>
4. *RAID*. Retrieved from <https://en.wikipedia.org/wiki/RAID>
5. *What is RAID and what are the different RAID modes?*. Retrieved from <https://www.startech.com/en-us/faq/raid-modes-explanation>
6. *RAID Storage*. Retrieved from <https://shop.westerndigital.com/en-ap/solutions/raid>

What Is Forensic Audit?

By | Miratun Madiah Saharuddin, Wafa' Mohd Kharudin, Ummu Ruzanna Abdul Razak, Fauzi Mohd Darus & Mohd Zukny Mohamed Nor

Forensic auditing has now been established as a dynamic and strategic tool in combating crime, corruption and fraud through the investigation and resolving the alleged fraudulent activities that are taking place. The definition of forensic audit keeps on evolving in response to the growing needs of an organizations and it requires both digital forensics and auditing procedures with the expert knowledge on the legal framework of the audit.

Forensic audit begins with suspicion and doubts and ends with the investigation of the procedures either to confirm the case or dispel the suspicion. Usually, a forensic audit is preferred instead of a regular audit as there is a chance that the evidence collected would be relevant in the event of a court case.

Ethics in Auditing

To help understand the importance of forensic audit, an auditor should possess the necessary qualities and act in accordance with the principles of auditing. Below are the ethics that you need to have as an auditor.

GOOD ETHICAL	
Ethical	Fair, truthful, sincere, honest and discreet
Open-minded	Willing to consider alternative ideas or points of view
Diplomatic	Tactful in dealing with people
Observant	Actively observing physical surroundings and activities
Perceptive	Aware of and able to understand situations
Versatile	Able to readily adapt to different situations
Tenacious	Persistent and focused on achieving objectives

Decisive	Able to reach timely conclusions based on logical reasoning and analysis
Self-reliant	Able to act and function independently whilst interacting effectively with others
Acting with fortitude	Able to act responsibly and ethically, even though these actions may not always be popular and may sometimes result in disagreement or confrontation
Open to improvement	Willing to learn from situations, and striving for better audit results
Culturally sensitive	Observant and respectful to the culture of the audited entity
Collaborative	Effectively interacting with others including audit team members and the auditee's personnel

Auditors should conduct themselves in a manner which promotes co-operation and good relations between the auditors, within their profession.

Normal audit or forensic audit?

Normal audit is basically about compliance and the purpose is to review whether an entity complies with the internal rules, regulations, policies, decisions, and procedures. To determine whether an organization needs a normal audit or a forensic audit, you must consider the following:

The organization may need normal audit if:

- Ethical lapses have occurred
- Requirement of specialized expertise

- The organization does not follow the existing policies and procedures.
- Compliance with laws and regulations is a significant burden
- Occurrence of IT data breaches

On the other hand, forensic auditing has emerged as a specialized field in the industry that requires a specific skill set to detect the crime or fraud. Below are instances in which an entity should call for forensic audit:

- Suspicious violation and theft
- The entity does not own the accounts which are under your entity's name.
- A whistle blower hotline has identified issues such as stolen assets or other blatant violations.

Additionally, the auditors must plan their work in a way that allows them to focus on gathering sufficient objective, verifiable evidence in order to support their report. To obtain the information, the auditor needs to investigate the documents and trace the relevant findings.

There are three (3) key factors that comprises forensic auditing:

a. Forensic Audit Thinking

As a forensic auditor, you must know what you are looking for and be prepared to do something if any incident occurs and to locate the incident. It is a mental shift in which the auditor believes there is a high potential for violation, and the controls could be overridden to achieve that goal.

This involves critical assessment throughout the audit to collect evidence, for example, to be aware if a violation may have occurred, is occurring, or will occur in the future. It is an unbiased evaluation of evidence that gives forensics opinions throughout the audit assessment from start until the end.

b. Forensic Audit Procedures—both proactive and reactive

Forensic audit procedures are more specific as it aims to identify potential significance of non-compliance with requirements in standards, policies and procedures based on the organization.

Those that perform forensic procedures should

either be the auditor or forensics specialists with an investigative mindset where they are more skeptical and have experience in dealing with violation issues.

They also must have the knowledge of investigation, analysis and technology-based techniques on how to gather, analyze and interpret the data.

There are seven (7) forensic investigative techniques that have been used by forensic specialists and examiners (Richard) which are:

- i. Public document reviews and background investigations
- ii. Interviews of knowledgeable person (the witness and the accused)
- iii. Confidential sources and informants
- iv. Laboratory analysis of physical and electronic evidence
 - Physical Forensic Analysis which includes handwriting analysis, fingerprint analysis, ink sampling, simulated forgery of signatures analysis.
 - Computer Forensics which include hard disk imaging, e-mail analysis, search for erased files, analyze use & possible misuse of office computers for personal use, ensure chain of custody for electronic evidence.
- v. Electronic and physical surveillance – CCTV and Access Logs
- vi. Undercover operations
- vii. Analytical procedures

c. Appropriate use of technology and data analysis

With the emergence of digital forensics and its applications in many industries, new tools have entered the market, focusing on various types of forensic investigative problems.

The nature of digital evidence is different from the physical evidence. It is latent, easily altered, can be damaged or destroyed; crosses jurisdictional borders quickly and it can be time sensitive as well. Thus, it is good to analyze using data analysis tools and techniques to ensure the data is accurate and to prevent or detect any irregularities.

Furthermore, digital evidence may provide a clue

to forensic auditor and assist them to recognize the pattern of any violation. The gathered evidence is then analyzed to identify whether a violation occurred. It can also help identify the potential control environment's weaknesses and assist in identifying any potential policy or process violations.

Audit Forensics Process

Next, is the audit forensics process. Unlike regular audit in which the objective is to make sure an organization complies to a certain set of rules and standards, forensic audit involves technical skills to investigate embezzlement and analyze information. Therefore, a forensic audit might have additional steps to be performed on top of the regular audit procedures. These steps are:

1. Planning

In the planning phase, it is crucial for the forensic auditor to understand the subject entity, area or process of the case. The auditor must understand the background of the organization and review documents of previous audit work. This will help the auditor gain a deep understanding thus enabling him or her to conduct the audit efficiently. In this planning phase as well, the audit team must come up with a work or audit plan. The plan must include the objectives and criteria of the audit, method of the audit, medium of communication, facilities requirement, and timeline of the audit. An audit plan should be able to help the audit team members as well as the auditees to know what to expect from the audit.

2. Collection of evidence

Collection of evidence must be conducted based on the audit methods and scope that has been stated in the audit plan. The evidence collected should determine the period when the fraud or criminal activity occurred. Other than that, the evidence with respect to the concealment of fraud and corroborative evidence to prove the fraud must also be gathered. All the evidence will help the auditor review the logical flow of information related to the case.

3. Analysis

Analysis of all information and evidence collected in the previous phase can be done using substantive techniques such as reconciliations and reviewing planned documents. Other than that, analysis can also be conducted by analyzing

comparative data of different segments and by establishing correlation of various data. The auditor should also try to look at the trends over a certain period of time to see if this data can contribute to the finding. Last but not least, analysis and the transfer of various data should also be done through the emails.

4. Internal Controls

In conducting the audit, the auditor should understand the internal controls of the organization or process subjected to the audit. By understanding the internal controls, the auditor will also be able to understand the loopholes which have allowed the fraud to be perpetrated in the first place. A good auditor should then test the operational efficiency of the internal control to check if it's foolproof. Further understanding of internal controls can be gained by interviewing the suspect or staff related to the case. Lastly, the auditor should check the use of software processing in enabling or concealing the fraud, in which digital forensics knowledge would be required to do this.

5. Reporting

A common deliverable out of an audit is an audit report. An audit report is a document comprising comprehensive findings, and it must contain a fact-based interpretation, not assumption. The audit team members must remember the requirements and expectations of the audit in the first place, and therefore this audit report should address and answer all those requirements. Other than that, an audit report should also include a summary of evidence found during the audit. It must also contain explanations on perpetration of fraud and suggestions on improvement to prevent similar cases from happening again in the future. After all, a forensic audit cannot undo the fraud that has already happened, but it could certainly help the entity to avoid the same incident from happening again in future.

To summarize, a forensic audit is a very detailed audit which requires the expertise of not only auditing procedure but also knowledge on digital forensics. Advanced technology has made it possible for an auditor to not only understand the various crimes that were carried out and how evidence can be collected to unearth the crime, but also how to use forensics tools and software to find evidence that is admissible in a court of law.

References

1. Ibrahim, K. (n.d.). *Forensic audit, forensic tools and techniques for internal auditors*. Academia.edu. https://www.academia.edu/27137571/FORENSIC_AUDIT_FORENSIC_TOOLS_AND_TECHNIQUES_FOR_INTERNAL_AUDITORS
2. International Organization for Standardization. (2018). *Guidelines for auditing management systems*. <https://www.iso.org/standard/63787.html>
3. What is the difference between Audit and Forensic Audit? <https://riskprolearning.com/distinction-between-audit-and-forensic-audit/?v=6c8403f93333>
4. General steps involved in Forensic Audit <https://www.caclubindia.com/articles/-general-steps-involved-in-forensic-audit-33474.asp>

Biometric In Forensic Identification

By | Mohammad Zaharudin Ahmad Darus, Nur Afifah Mohd Saupi, Nazri Ahmad Zamani, Yasmin Jeffry & Muhamad Zuhairi Bin Abdullah

Introduction

“Who needs biometric? Why biometric has become crucially important in our lives?”

These days, new emerging and disruptive technologies such as Internet of Things (IoT), Virtual Reality (VR), Augmented Reality (AR), Artificial Intelligence (AI) have become more prevalent especially since the Covid-19 pandemic struck in 2020. For example, society nowadays have started to rely heavily on Internet as medium for communication. Meetings and discussions are conducted online using video conferencing software. Shopping is mostly done on online store platform. In addition, students have been required to continue their studies at home via an online learning systems provided by their institutions.

It is undeniable that these technologies have benefitted us, but we must also be mindful of the harm they could bring. Most of the online activities require us to register and verify ourselves as legitimate user. However, this could lead to digital identification fraud due to cyber-attacks.

“In order to strengthen identify our identity in a digital world, is biometric good enough to securely identify our identity, at least at the authentication level? Now, let’s look at it from a physical security point of view.”

Authorities have started to deploy and adopt biometric technologies for tracking and identifying humans. Authorities like immigration department are using biometric applications to augment security for cross border activity. They require a system that can provide sufficient and automated security on individual identification verification to avoid fraud. For example, Immigration Department of Malaysia

has embedded a chip that contains biometric information of the holder in the travel passport. Our National Registration Department has also placed a chip on MyKad that contains Biometric Data such as our fingerprints minutiae.

At this point of time, it is still hard to tell whether biometric systems can prevent identity fraud. No matter how developed a technology, if it has been categorized under software and hardware, the chances of vulnerabilities are still there due to human factors. This article will focus on adopting biometric technology in forensic identification.

Go by Definition

Before we go in-depth about the Biometrics in forensics identification, let’s look at the definition of forensics science,

“... is the use of scientific methods or expertise in conducting investigation and examining evidence that will/might be presented in a court of law.”

Scientific method as mentioned in the definition involves the processes of making hypotheses, deriving predictions as logical step, and then carrying out experiments or empirical observations based on those predictions. Since forensic science begins at the crime scene, it relies on the scientific method as a series of logical steps used to solve problem, to ensure that the results acquired during analysis are consistent when repeated. Thus, all parameter input during experiments must be recorded and well documented. So, when asked by a judge to repeat the process in court of law, the same results will be attained. Otherwise, the testimony will not be accepted, and the evidence most probably will not be strong enough for conviction of a suspect. Figure 1 shows the generic process flow of forensic science.

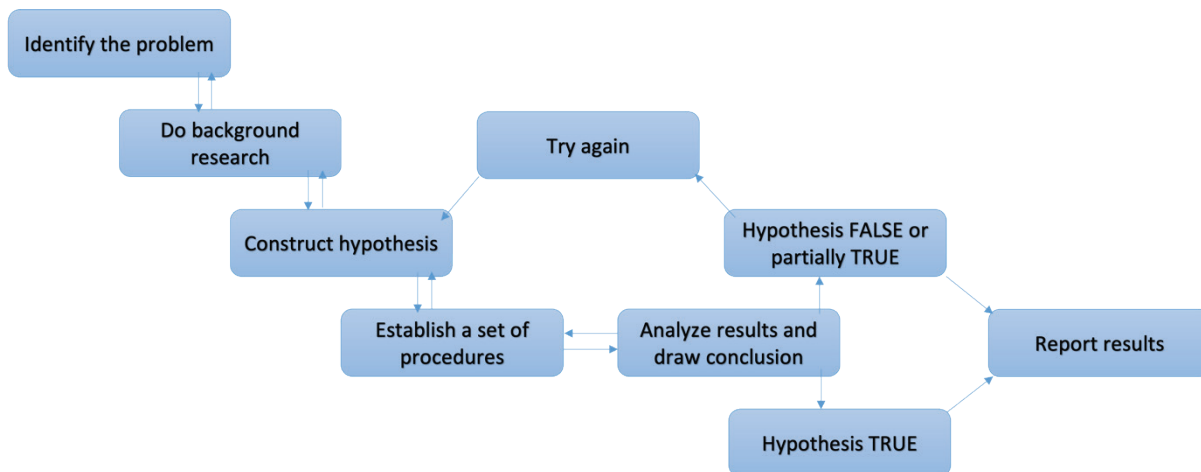


Figure 1: General Process Flow of Forensic Science

Biometrics is defined as the measurement of biological, physical, or behavioral characteristics that can be used to identify a subject. Biometrics is also a technology that can identify a subject's unique biological characteristics. Biometrics recognition is an automated recognition of an individual's based on their biological and behavioural characteristics. The usage of biometrics are as follows:

- Identify and verify a subject.
- Authenticate a subject to give appropriate rights of system operations.
- Keep the system safe from unethical handling.

Forensic biometric applications can be seen as an automated biometric method that is used to analyze and interpret the biometric data. There are four types of applications that can be applied for biometric in Forensic Identification as follows:

- Demonstrate the existence of an offence - To detect an illegal act from forensics point of view in which the process of detecting and identifying the existing crime such as hacking, murder, and any other type of crimes.
- Investigate offence(s) - To create a forensic timeline based on the investigation or intelligence gained. Able to identify and investigate the starting point of the crime up until the point it has occurred and after it happened.
- Individualize the perpetrator - To do a forensic evaluation at source level. For example, the process to conduct biometric analysis in order to identify the suspect.

- Describe the Modus Operandi - To do a forensic evaluation at activity level and able to identify and describe the method that had been used by the perpetrator or suspect.

Biometric System

Biometrics system is a pattern recognition device that acquires physical or behavioural data from an individual, associating the traces of an individual that is stored in the database, ranking the identity of a person, and selecting subdivision of person from which the trace may originate. In general, there are four modules in biometric system as follows:

- Sensor module - This module is where the process of acquiring raw data of individual by scanning and reading. For example, camera or any devices that are capable in capturing image or video stream.
- Quality Assessment and Feature Extraction Module - Raw data is subjected to signal enhancement algorithm to improve its quality and then stored in the database referred to as template. For further processing, the quality of the acquired raw data is then assessed.
- Matching and Decision-Making Module - The extracted templates are then matched against the stored templates and a matching score will be given. Based on the matching score, the identity of a person is validated or ranked. The comparison process takes place when you compare the data with existing template from the database or if there is no template, then a new registration and enrolment is required.

- d. Database Module - The storage of biometric system. During the enrolment process, the template is extracted from raw biometric data that is stored in the database along with some biographic information (such as name, address, etc.) of the user.

Biometric System Process Flow

A generic process flow of biometric system has six processes that starts with sensor and ends with results in either a positive or a negative match. Figure 2 below shows a generic process flow in biometric system.

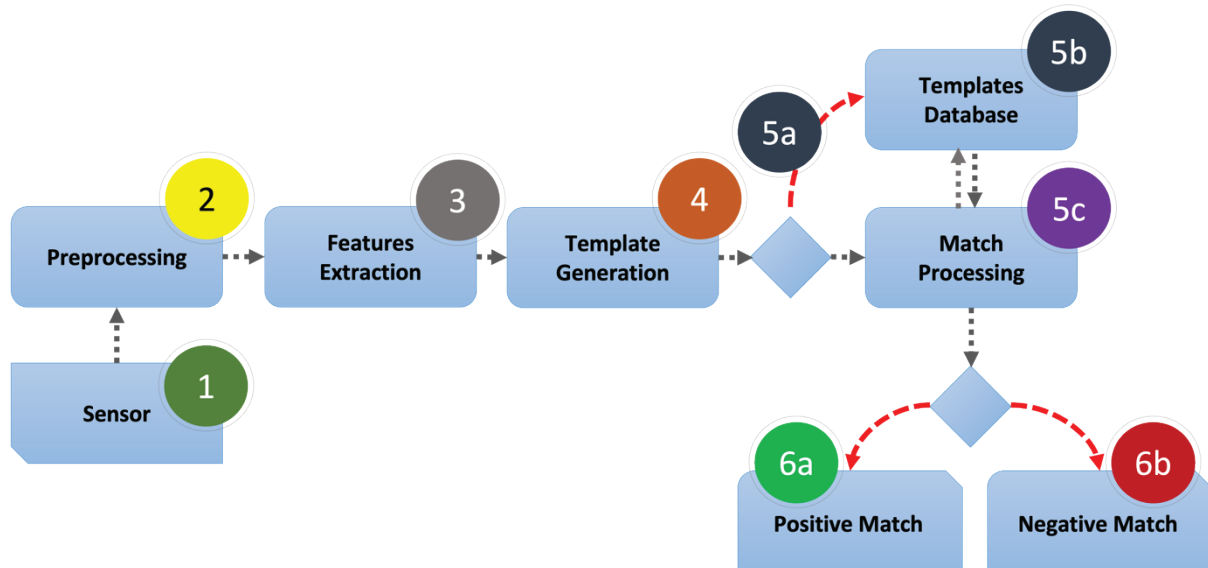


Figure 2: Generic Process Flow of Biometric System

- Sensor - A device such as camera will act as sensor to capture stream or image by motion and convert it to digital form.
- Pre-processing - Process of converting the image captured into digital form, doing the segmentation and normalization process as well as to filter and cut out irrelevant information of the said data and also carrying out the quality measures.
- Feature Extraction - This step is when the system selects only the main important features as well as to cut any irrelevant information of the said data.
- Template Generation - This process will generate template in a structured way for matching purpose or enrolment.
- Template Database - All structured templates will be stored in database and retrieved for matching purpose during matching process.
- Matching - Matching will be done during the process where it compares the data that is captured with the structured template in database.
- Result - Once the matching process is done, result of the process will come out as positive or negative. However, we also need to be aware of the false positive and

negative results which means a test result that wrongly indicates a negative match positive match and vice versa. This happens due to the quality of data collected during data aggregation process. It could also be attributed to the computer algorithm itself which was not well implemented during system development.

Biometric Modalities Use in Forensic Identification

There are three possible ways to prove an individual human identity. One, it is "WHAT WE HAVE" such as identity card, license, passport, bank card. Second, is "WHAT WE KNOW" such as password, bank pin code or door safety code. Lastly, "WHO WE ARE" which are our physical body traits or biometric traits. Biometric traits are unique for each person and as such, it can be very useful and practical for forensic investigation.

There are two categories of biometric modalities: physical and behavioral. Physical modalities are something that humans are born with and will remain unaltered throughout the person's life. It can be divided into two types which are morphological such as fingerprint, face and

vein and another one is biological such as blood, saliva, and urine. Another modality is behavioral that pertains to the behavior exhibited by people, or the way they perform tasks. Example of unique behavioral modalities are gait, voice, and handwritten signature.

Other than using only physical or behavioral modalities which is unimodal biometrics, there are also the usage of multimodal biometrics where it combines more than one or at least two biometric traits. The purpose of multimodal is to strengthen security from multiple traits identification.

Type of Biometric Modalities

There are many biometric traits within a human body. In this article, we will only focus on four traits which owing to technology readiness and devices on retrieval, are easy to acquire as well as deploy at the scene. For example, fingerprint devices can easily be acquired via online shopping platform. The four traits that we will be focusing are fingerprint, palm print, face, and voice.

a. Fingerprint

Fingerprints as a biometrics trait have been used widely for centuries and emerged as an important tool in criminal investigations due to its robustness and uniqueness. A fingerprint is a unique pattern on the surface of a fingertip.

To match a print, a fingerprint analyst digitalizes or scans the print obtained at a crime scene and computer algorithms of a biometrics system will locate all the unique minutiae and ridge points of a print in question. These unique feature sets are then matched against a stored fingerprint database. Whenever fingerprints are obtained from the crime scene, they are matched with the fingerprint from database and with the fingerprints of the criminal that is already enrolled in the database. Figure 3 shows a flow for detecting a suspect's fingerprints.

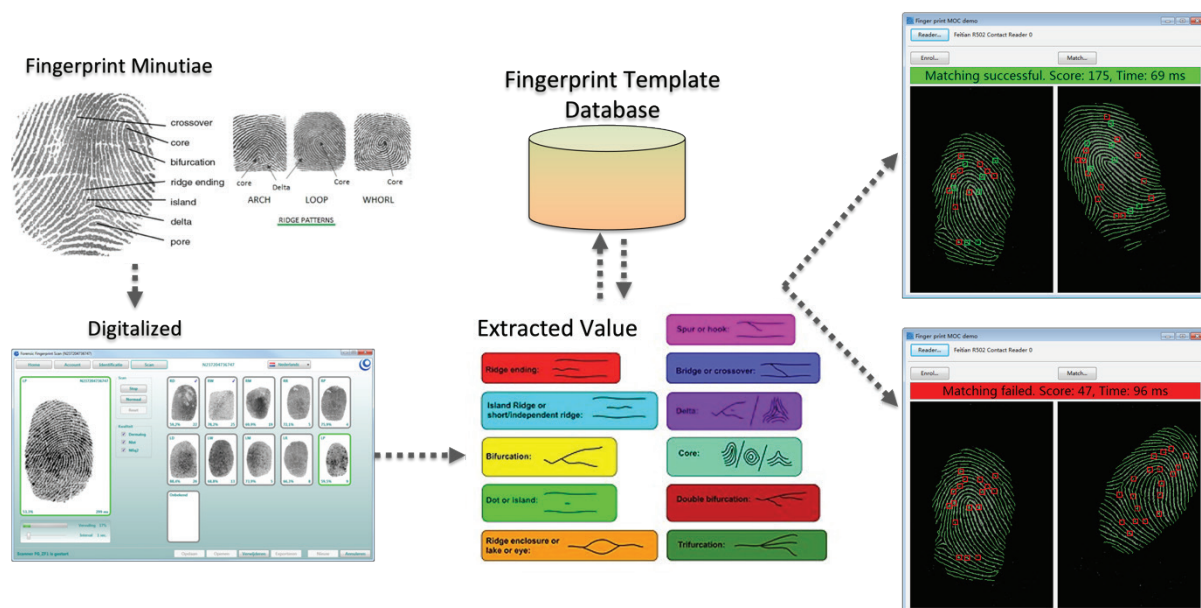


Figure 3: General Process Flow of Identifying the Fingerprints

b. Palm print

Same as fingerprints, the palm of the human hands also contains unique pattern of valleys and ridges. The area of palm is much larger than the area of finger. As such, palm prints are expected to be even more distinctive than fingerprints. Palmprint provides crime investigators an important additional investigative tool. Palm would give more information regarding the individual, more than just ridges and minutiae like the finger, but in the thenar, hypothenar and interdigital.

To match a palm print, the analyst will need to digitalize the palm captured and compare the features

with the template that is stored in the database and the system will show the result whether it is a negative or a positive match. Figure 5 shows the general process flow of identifying a palm print.

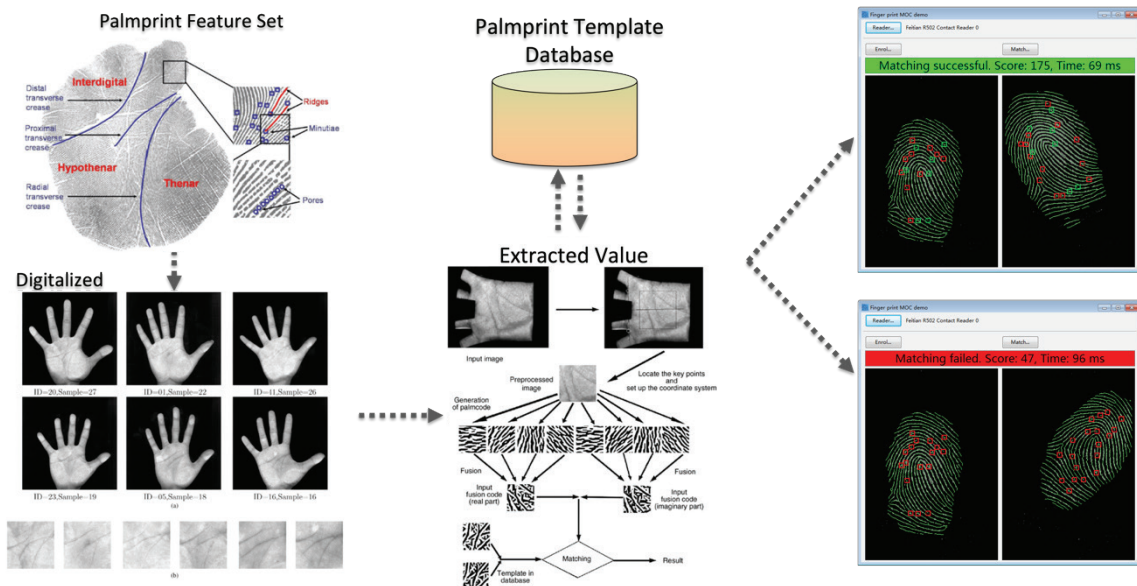


Figure 5: General Process Flow of Identifying the Palmprints

c. Face

Face recognition technology plays an important role in law enforcement agencies. Facial recognition is a computer-based system that automatically identifies a person's face based on image or video which is then matched to the facial image stored in the facial biometric database. It is based on determining the shape and size of the jaw, chin, shape and the location of the eyes, eyebrows, nose, lips, and cheekbones. 2D facial scanners will read face geometry and record it on the grid.

Once a face is detected, the system will then perform normalization where it will cut out all irrelevant information and then through extraction, it will identify the fiducial point of the face and then compare the data with the template in the database to find a matching result. Figure 6 shows a general process of identifying a face.

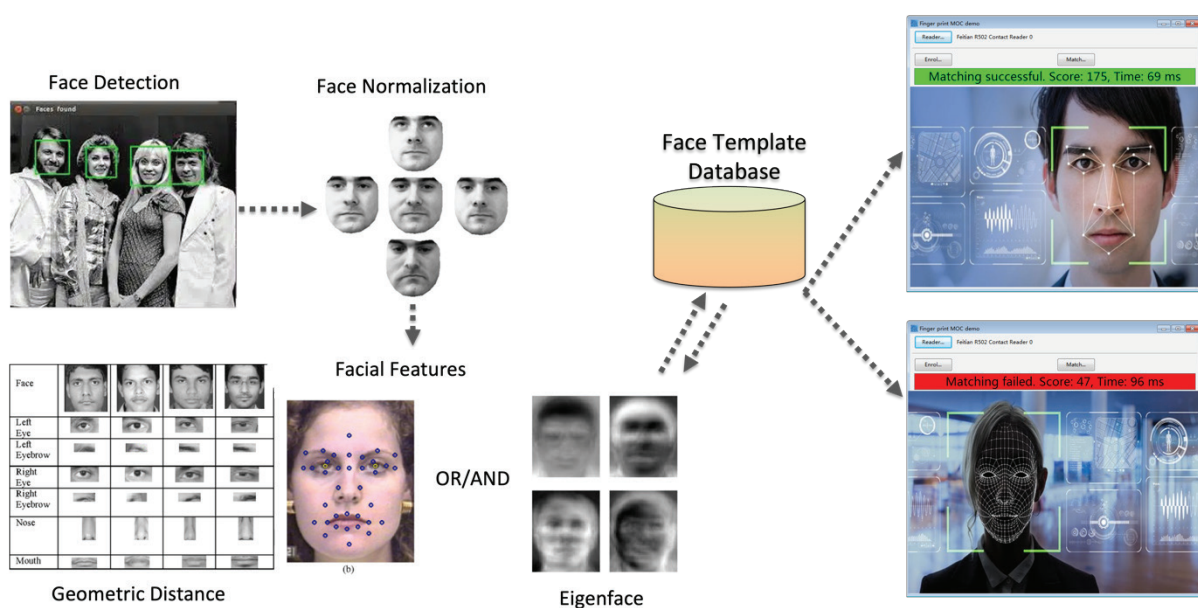


Figure 6: General Process Flow of Identifying the Face

d. Voice

Voice Biometrics deals with identification of a speaker from the characteristics of an individual's voice. So, it's often used when voice is the only available trait for identification. For example, a ransom case demanding money in kidnapping cases, forensic analyst will authenticate and identify the speaker through his voice. Figure 7 below shows the general process flow in identifying a speaker.

There are two approaches in voice recognition - text independent and text dependent.

Text independent - Analyst will provide a general topic of interest for the speaker to speak in a spontaneous and comfortable way.

Text dependent - Analyst will prepare a text or predetermined phrases for a smooth reading.

There are also two types of recognition related to voice: voice recognition and speech recognition. The objective of voice recognition is to recognize WHO is speaking, while speech recognition aims to understand and comprehend WHAT was spoken.

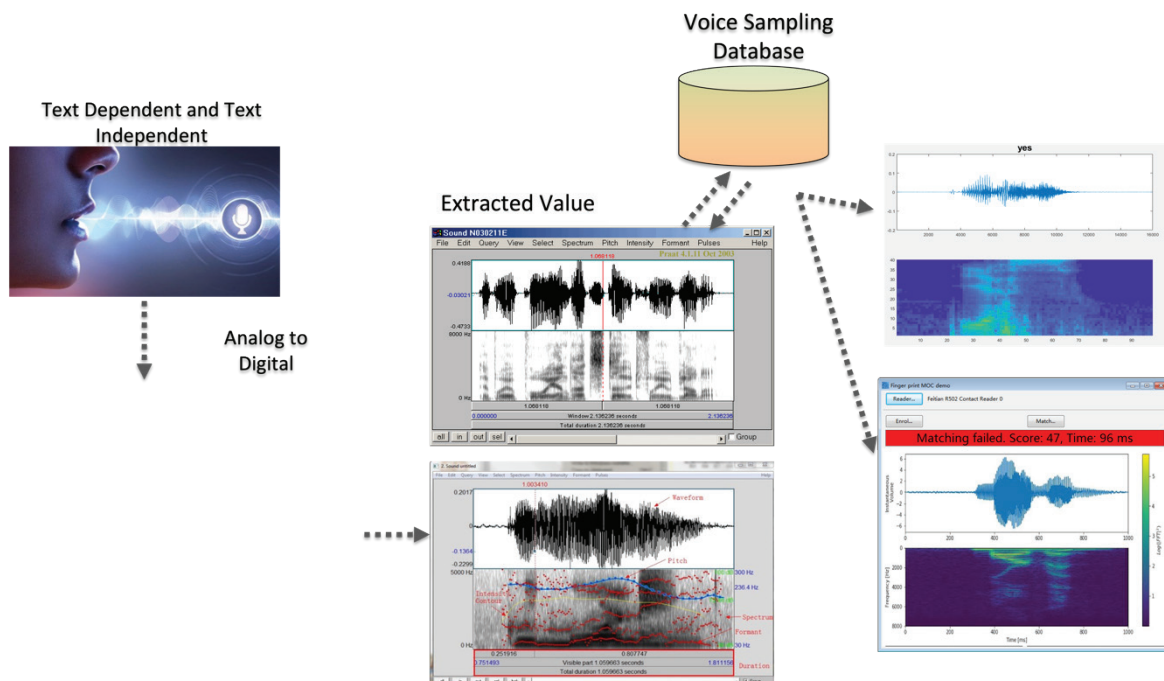


Figure 7: General Process Flow of Identifying the Voice

As illustrated, all biometrics will be matched with a database. We can conclude that the bigger a database, the more accurate results can be attained.

Bridging The Gap

There are at least five factors which differentiate Biometrics from Forensic as follows:

- Work Approaches** - The objective of forensics is to establish a timeline before and after an event. We are developing a time metrics whereby there will be proper evidence collection that needs to be reconstructed forensically to relate to the suspect's involvement. Meanwhile, biometrics' objective is to establish the individual presence during a crime.
- Evidence** - In forensic, we are searching for relevant evidence, while in biometric, it is more straightforward, as we already know the traits. For example, if there is a fingerprint, we know that is a type of trait to be collected from suspect.
- Real Time Recognition** - In forensics, the event has already occurred, so there is no real time factor, while in biometrics, we can set a rule at the sensor level to trigger any

abnormal pattern. So, we would know the timeline straightaway.

- d. Inconclusive Decision - In Forensic, there will always be inconclusive finding, and this is contingent on many relevant external factors that may impact the quality of evidence. While in biometric, we only focus on positive or negative match, and most of the time are aware of the false positive, false negative and vice versa.
- e. Quality - Forensic relies on a variety of devices to sufficiently construct a strong and reliable evidence to be used in court. In biometric, it relies on the specific identified biometric traits. For example, facial traits that can be demonstrated in any camera installed.

From the five factors highlighted, both technologies have their own processes in which when combined, can significantly improve the quality of evidence. In conclusion, it can be seen that the biometric technology should complement Forensic Identification in conducting investigation. However, not only must the technical aspects be emphasized, but people and processes must be strengthened as well.

References

1. <https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics>
2. <https://eab.org/expertise/wg/fbwg.html>
3. <https://www.nist.gov/forensic-science>
4. <https://www.nice.com/engage/blog/rta-understanding-the-types-of-biometrics-2513/>
5. Reference: *Biometrics in Forensic Identification: Applications and Challenges*,
6. Saini and Kapoor, J Forensic Med 2016 : *Biometrics Realistic Authentication*, www.tutorialspoint.com

Dawn Of A New Strain In Banking Trojan

By | Muhammad Nooraiman Noorashid, Fakhru Afq Abd Aziz, Muhammad Faridzul Sukarni Muhammad, Muhammad Iskandar Shah Abdul Aziz & Kamarul Baharin Khalid

Introduction

Money is the most powerful motivator for cybercriminals. Year after year, financially motivated criminals will go to any length to extract money and sensitive information from their victims. One of their methods is by using a banking trojan, a malware explicitly designed to extract sensitive information and data stored in the online banking systems. The usage of this trojan has increased throughout the years, and financial institutions are having difficulty tracking it due to new deployment techniques and constant evolution of methods that can bypass existing security detection. Many banks are experiencing difficulties because of these persistent threats. Moreover, the current prevention method is deemed ineffective against the cybercriminals' attacks. Financial institutions can only hope that their current system will be able to withstand any attacks without causing significant damage to the clients and customers who use their systems.

Even though all the trojan horses' malware share the same core or foundation, banking trojan has its unique signature, which distinguishes it from other trojan horse malware. Cybercriminals are no longer targeting financial institutions and their customer. They have grown to be more exclusive and sophisticated as they widen their interests to social media, communication platforms, and other digital platform fields. Most of their victims are users who are not from an Information Technology (IT) background or unsuspecting users who are often tricked into downloading the trojan without realizing the impact of their actions on their company or to their sensitive personal information. This malware is used to infiltrate numerous businesses and corporations. To avoid becoming a victim of cybercriminal, users need to be aware of which software or programs that are safe for their environment and avoid using unknown and questionable software.

A malicious trojan banking program runs in the background, whereby the user is unaware of its unauthorized processes. It could be a game, utility application, or even a messenger application. This type of malware is dangerous because it duplicates, or it looks similar to a financial institution's official banking application.

At first glance, the malware will appear as a legitimate software or a process compatible with the operating system during the installation phase. After obtaining permission, the malware will access all the computer files in search of vital information or steal credential information to assist the attacker in illegal transactions, identity theft, and money extraction from the user's account. Thus, downloading and installing applications from an unknown source software without proper verification can lead to severe crime-related problems.

To combat this type of cyber-attack, financial institutions must increase the security for their authentication method to ensure that their customers can safely complete a transaction without risking their confidential information from being exposed to a third party. Every action or task in our daily life today revolves around mobile devices, particularly online transactions. Financial institutions must safeguard all transactions made by their customers. As for the users, they must learn and be aware of banking trojan malware. This can help them determine which software is safe to use and also keep them from becoming a victim of banking trojan malware.

History of Banking Trojan

Customers took nearly two decades to warm up to the concept of Internet banking, which first appeared in the 1980s. With most banks enabling online banking by the year 2000, it wasn't long before attackers discovered ways to use banking trojan to exploit this new attack surface. Banking institutions quickly realised that they were an appealing target for attackers, so they hardened their security systems. As a result, cybercriminals quickly realised that it was difficult to attack banking institutions, so they shifted their focus to their customers instead. Stealing customer credentials seemed more feasible, thus the first banking trojan was created. Banking trojans primarily infiltrate users through spam, phishing, advertising, drive-by downloads, or social engineering. To deceive users, they masqueraded as official document attachments or interactive online games. The malware creator's attack scope,

technical skill, and focus have shifted since then. What began as a malware aimed primarily at the clients of financial institution has since spread to online advertising, digital analytics companies, financial technology companies, social networking sites, and communication platforms. Banking trojans are now spread widely on the Internet. All businesses, and not just the financial business, should take measures to safeguard themselves and their customers.

For more than 15 years, malware has been used for re-sending received SMS messages to attackers, including circulating those with a TAN code (Transaction Authentication Numbers). Some trojans leverage the USSD code (Unstructured Supplementary Service Data) also known as the quick codes to replicate a transaction with the phone's bank card. However, they were not full-fledged banking trojans as their capabilities were noticeably inferior to those of their desktop computer banking counterparts. The first full-fledged banking trojans for the Android mobile platforms were discovered about ten years ago, the first generation was the Android SpyEye banking trojan. This banking trojan was accompanied by the SpyEye malware for Windows due to the dual nature of the attack, attackers were able to bypass two factor authentication.

Malware on an infected Windows system can attempt web injection by putting a piece of malicious code into a page as soon as a user of the infected Windows system browses a banking site using the browser. The banking site's URL in the browser's address bar will be altered, and a connection will then be altered using HTTPS as the injection will be done on the client-side. The infection also alters the content of the web page. The trojan may embed some text into the banking site that states, for example, that the bank needs to change some procedures urgently due to many new cyber-attacks. The users will be tricked into downloading an additional application (about 30 KB in size) from the provided link and install it on a mobile phone. The 'software' is in fact a SpyEye mobile banking malware, of course. The trojan's principal function is to intercept all incoming SMS messages and transfer them to a cybercriminal-controlled server. SpyEye caused alarm among banking service users for several months until it was discovered in the databases of all major antivirus programs, after which, its activity progressively subsided.

The Rise of Android Banking Trojan

After some time, banking IT personnel mastered programming, and online banking applications gradually shifted from PCs to mobile phones. As a result of this change, malware developers' lives were made easier. They no longer had to waste their time infiltrating the Windows systems but instead, focused all their efforts in building mobile banking application trojans. After all, a smartphone with a banking application is like a walking wallet. Banking trojans, like other Android malware, spread by masquerading as legitimate applications. Of course, the developers do not publicize the software's malicious capability but will appear after some time or after a new update is downloaded.

A banking trojan will be deployed in the form of an application that purportedly to integrate multiple client programs from many prominent banks. Why install a bunch of different apps if users can download just one? There have also been reports of dangerous programs being embedded in legitimate banking software that had been previously updated by cybercriminals. These programs were spread through phishing emails that directed victims to bogus bank websites that looked identical to the official sites.

Phishing SMS is another way for mobile banking trojans to proliferate. Phishing messages can be used in several ways, for example, when a user who has registered with one of the free classified listings sites receives a message offering to buy his product and because the victim is addressed by his name, the recipient's will be less suspicious. Malware writers have previously processed the site's userbase, extracting all sensitive information. After clicking on the shortened phishing link in the message, the potential victim will be directed to an intermediate page. After the attacker discovers that the user is using an Android based mobile device to access the site, the victim's cell phone service provider will be named. The customer will then be directed to a bogus page containing a MMS message in the style of the mobile service provider. The trojan download process begins after the user clicks on the fake MMS link.

Another way banking Trojans lure users is by requesting them to enable Accessibility Services mode, including some specific functions for those with disabilities. Trojan could also gain admin rights if it receives proper authorization

which can be gained by tricking the users to enable the application's permissions. Once access is allowed, trojans typically remain in the phone's memory until a mobile banking app is launched. When the trojan detects a banking application being launched, it will display a fake login and password form on top of the original app. The data that is entered will be instantly transferred to the attacker's server via SMS message.

The mobile banking trojan may contain HTML code for a several dozen pages, each with a unique design that mimics the most popular banks' application interfaces. Then, by intercepting the SMS with a one-time password the attackers could possibly gain full access to the bank account. In order to avoid arousing suspicion in the victim, incoming messages from banks are frequently disguised. If the trojan is unable to gain direct access to the bank account, it will then steal bank card information of the victim. In some cases, for example, disguised tabs will appear in order to request the victim to link their bank card to the Google Play account that is being used. As anti-fraud mechanisms are now widely used by security concerned business owners, it is now more difficult to buy anything with stolen card details, though it is still possible to pay for online toys or music on less prominent sites. Since the demographics of visitors to such websites are usually minors, site developers rarely bother to thoroughly check the payment information.

Banking Trojans Modus Operandi

The installation process begins when the victim clicks on the APK file sent via WhatsApp.

As shown in Figure 1, the victim will be prompted to allow installation from "Unknown Sources."

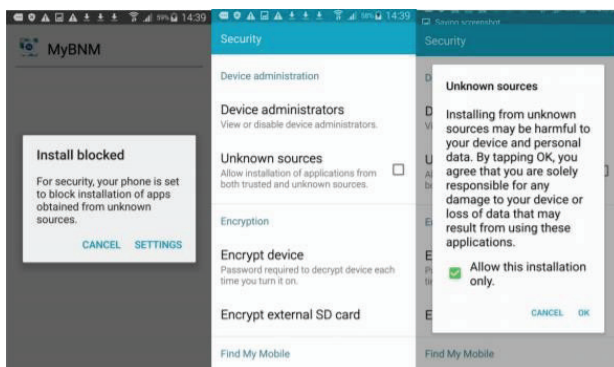


Figure 1: Installation Process

After enabling the "Unknown Sources," the victim's device will then proceed with the installation, as shown in Figure 2 below, with the victim's consent by clicking on the install button.

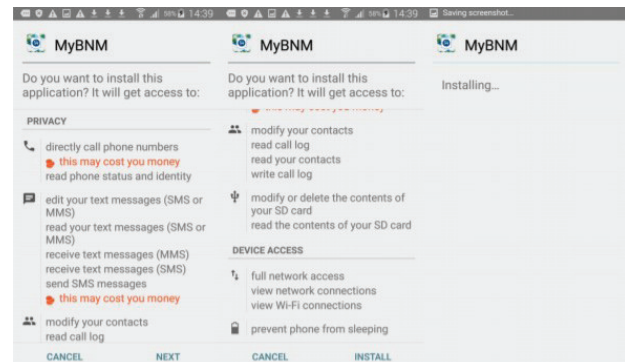


Figure 2: Access Request

The scammer's application is now successfully installed on the device. The victim will see the "MyBNM" icon on the home screen, as shown in Figure 3 below.

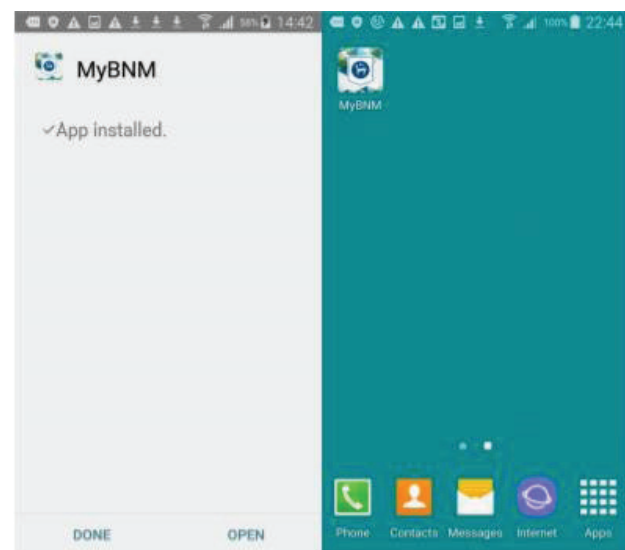


Figure 3: Success Installation

During installation, some victims will see a security pop-up screen stating that the application to be installed contains malware, as shown below. If the victim clicks "Install Anyway," the installation will proceed as shown in Figure 4 below.

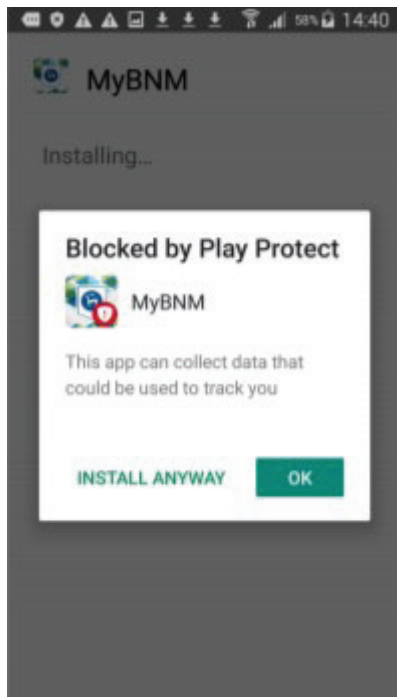


Figure 4: Security Block

When the victim launches the installed scammer app, he/she will be prompted to make the scammer app the default SMS application, as shown below. If the victim presses the "OK" button, the scammer application will continue and prompt the victim to enter a pin code. This pin code will be provided by the scammer via phone calls or text messages. As shown in Figure 5, no network activity occurs.

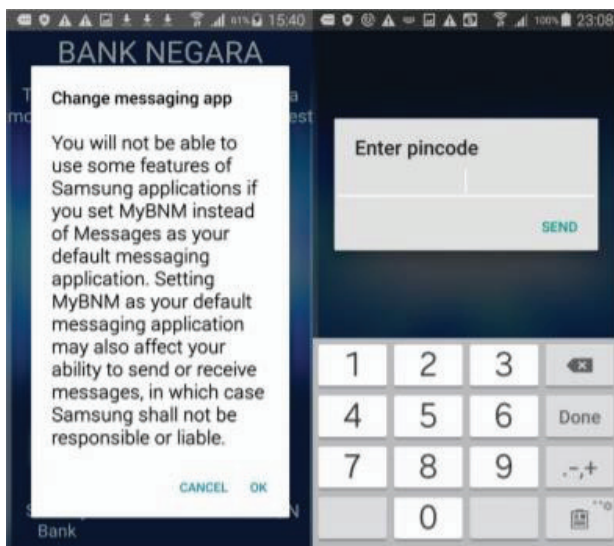


Figure 5: Application Start Interface

If the entered pin code has been validated, the scammer application will then display the main screen, as shown in Figure 6. The victim will be forced to choose the banking service of their choice and log in using their online banking credentials through the scammer application.

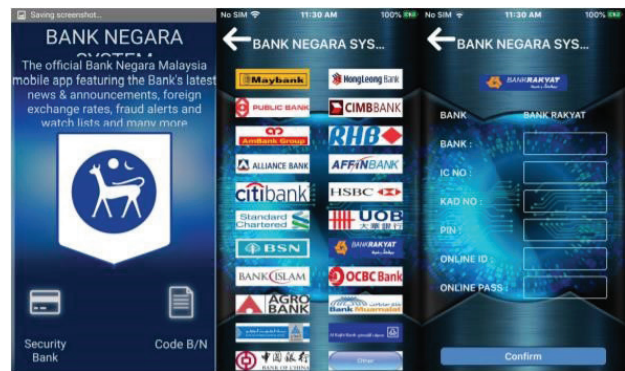


Figure 6: Application Main Interface

Best Practices to Protect Devices

The technology that you use can make you a target for malware and cyber-attack, especially if your devices are not secured properly. There are several ways to minimize the risk for your devices from being the target of malicious intents:

- Keep your phone's screen always locked. One potential threat is having your device stolen, which could provide the attacker with complete access to your personal information. When you enable a lock screen, you will be able to specify how long the phone can be idle before locking back. Make sure to choose the shortest time possible.

Some may find this inconvenient, but it will protect you by automatically activating the lock screen even if you forget to lock it yourself.

- Keep your mobile application updated to the latest software version to avoid vulnerabilities and exploitation.
- Set a secure password and, if possible, enable biometric authentication and two-factor authentication (2FA). This is a secondary method of verification that occurs after an attempt to use your password. 2FA uses another private account or something you physically have. Apple ID and Google accounts, both provide 2FA if your device is compromised by nefarious actors, so always enable it for added security. Biometrics such as fingerprints and face ID are also becoming increasingly popular.
- Maintain the most recent version of your device's operating system (OS) and applications. When it comes to protecting yourself from hackers, the first step is to always install software updates as soon as they become available: this is crucial for both

smartphones and computers. Yes, updating can be tedious and inconvenient, and it can sometimes result in annoying changes to the interface you are used to. Nonetheless, a large proportion of successful hacks exploit previously patched vulnerabilities; exposing yourself unnecessarily is foolish.

- e. Install antivirus software or scan on a regular basis with CyberSecurity Malaysia's Mobile Assessment Security Scanning Application (MASSA).
- f. Connect to secure Wi-Fi and use VPN when using public Wi-Fi. You run the risk of exposing sensitive data transmitted from your device if you visit unsecured websites using the public Wi-Fi. You are also more vulnerable to man-in-the-middle attacks and malware exposure. On the other hand, ensuring your Wi-Fi is secure also prevents unauthorized access to your network. Also, turning off Bluetooth and Wi-Fi when not in use is a great safety measure as well.
- g. Be cautious when downloading any application, documents, or other files. Install only applications from Google Play, Apple App Store, and Huawei APP Gallery. Do not open suspicious emails, messages, or links. If you receive a suspicious email informing that you have won something, do not open the email, or click on the link, as it will redirect you to a fake site in which the malware will be downloaded and installed on your phone. Thus, giving the hacker access to any data on your phone.
- h. Do not jailbreak or root your smartphone because jailbreaking your device disables much of its built-in security and exposes it to infections. While this gives you more control over your device, it also makes it vulnerable to attacks and malware. Aside from having the risk of malware or spyware, it also means that you will miss the security patches from the latest OS updates. Jailbreakers have a high chance of skipping the updates to keep the jailbreak functional which increases the risks of being hacked.
- i. Periodically check the permission of the apps in your device OS. Even if the apps on your phone seemed safe and straightforward when you installed them, subsequent updates could have turned them into something more sinister. Take two minutes to review all the apps on your smartphone and see which permissions they are using: on iOS and Android, you will find lots of relevant information under Settings > Privacy.
- j. If you have sensitive data on your mobile device, encrypt it and keep a backup of the data. Encrypting your data ensures that it remains secure even if it is infected by malware. If it is lost or stolen, your emails, contacts, financial information, and other information can be compromised. Most phones have encryption settings in the security menu that you can enable.

If assuming that every smartphone user follows all of the above recommendations, then one can reasonably expect the malware infection rates to drastically drop in the near future. Cyber-hygiene is as important as cyber-security because when people are properly educated on how to avoid non-conforming apps, websites, and software, the Internet will be safer.

Conclusion

Mobile malware is one of the most serious issues in mobile banking. Malicious applications are capable of stealing personal information, logins, and passwords in order to steal money and breach security systems. They can quickly infect a large number of devices due to the creative methods used to exploit the overall vulnerability of mobile operating systems. No one is immune to such attacks regardless of individuals or organizations. Dealing with sensitive data is therefore a significant challenge for mobile banking and other businesses. As the number of threats increases year after year, it is critical to remain on top of the problem by educating users about current threats and upgrading security software.

To summarise, mobile malware developer's interest in Android OS will continue to grow, with their efforts focused primarily on developing malicious programmes that target this specific platform. There has been an increase in the number of attacks that use vulnerabilities and exploits to gain root access to a smartphone.

References

1. Cybleinc. (2021, June 21). Banking trojan Variant spreading through Android app. Cyble. <https://blog.cyble.com/2021/06/17/banking-trojan-variant-spreading-through-android-app/>.
2. C. S. N. min, & Alicia Hope. May 24, 2021. (2021, May 21). Android malware Named TEABOT banking Trojan Targets Sixty banks in Germany, Spain, Italy, Belgium, and the Netherlands. CPO Magazine. <https://www.cpomagazine.com/cyber-security/android-malware-namedteabot-banking-trojan-targets-sixty-banks-in-germany-spain-italy-belgium-and-the-netherlands/>.
3. Palmer, D. (2021, June 1). This android trojan malware is using fake apps to infect smartphones, steal bank details. ZDNet. <https://www.zdnet.com/article/this-android-trojanmalware-is-using-fake-apps-to-infect-smartphones-steal-bank-details/>.
4. Mabuza, E. (2021, August 11). Android trojan hits more than 10,000 victims in 144 countries - and SA isn't spared. SowetanLIVE. <https://www.sowetanlive.co.za/news/south-africa/202108-11-android-trojan-hits-more-than-10000-victims-in-144-countries-and-sa-isnt-spared/>.
5. Panda Security. 8 Mobile Security Tips to Keep Your Device Safe. <https://www.pandasecurity.com/en/mediacenter/panda-security/mobile-security-tips/>, 2019 March 05, accessed on 25 August, 2021
6. Y. Magali, "10 security best practices for mobile device owners" <https://www.cdillc.com/10security-best-practices-mobile-device-owners/>, accessed on 25 August, 2021

Comparison Between Security Risk Management Models

By | Nur Athirah Abdullah & Norahana Salimin

Introduction

Risk management is necessary for each organization to make an effective business decision. It should help an organization identify, assess and treat risks which will contribute to building up the organization's risk management capability. Each country will have different regulations, policies, guidelines, or best practices documentation regarding risk management. Risk management for financial sectors (FIs) are extremely important to ensure business success and continuity in managing financial activities.

We shall take a look at three documents to compare its similarities and differences.

- a. Risk Management in Technology (RMiT) by Bank Negara Malaysia (BNM)
- b. Technology Risk Management Guidelines (TRMG) by the Monetary Authority of Singapore (MAS)
- c. ISO 31000:2018 Risk Management – Guidelines by International Organization for Standardization (ISO)

Comparison Of RMiT, TRMG And ISO 31000

No	Content Element/ Topic	RMiT	TRMG	ISO 31000
1	Scope of risk management	Requirements regarding FIs' management of technology risk	Risk management principles and best practice to guide FIs	Guidelines on managing risk faced by any organization
2	Type of document	Policy	Guideline	International standard
3	Target audience	Financial sectors (FIs) in Malaysia	Financial sectors (FIs) in Singapore	Anyone. Not industry specific
4	Issuer	Bank Negara Malaysia (BNM)	Monetary Authority of Singapore (MAS)	International Organization for Standardization (ISO)
5	Effective date or latest version	1 January 2020	June 2013	14 February 2018
6	Compulsory to follow	Yes for FIs in Malaysia	No. It is treated as industry best practices	No. It is on a voluntary basis for any organization
7	Roles and Responsibility	Yes	Yes	Yes
8	Applicable for Data Centres	Yes	Yes	Yes
9	Project management	Yes	Yes	Yes
10	Technology Risk Management Framework (TRMF)	Yes	Yes	No

No	Content Element/ Topic	RMIT	TRMG	ISO 31000
11	System development and acquisition	Yes	Yes	No
12	Software testing	Yes	Yes	No
13	Cryptographic functions	Yes	Yes	No
14	Network	Yes	Yes	No
15	Outsourcing or third-party provider	Yes	Yes	Yes
16	Cloud services	Yes	Yes	No
17	Access control	Yes	Yes	No
18	Patch management	Yes	Yes	No
19	Security of digital services	Yes	Yes	No
20	Cyber Risk Management (CRF)	Yes	No	No
21	Cybersecurity operational management	Yes	Yes	No
22	Distributed Denial of Service (DDoS)	Yes	Yes	No
23	Data Loss Prevention (DLP)	Yes	Yes	No
24	Security Operations Centre (SOC)	Yes	No	No
25	Cyber Emergency Response Team (CERT)	Yes	No	No
26	Technology audit	Yes	Yes	No
27	Vulnerability Assessment and Penetration Testing (VAPT)	Yes	Yes	No
28	Training and awareness	Yes	Yes	Yes
29	Regulatory process	Yes	No	No

Advantage And Disadvantage

Models	Advantage	Disadvantage
RMiT	<ul style="list-style-type: none"> The requirements or guidance are detailed so that practitioners can easily adapt and implement to their respective environment. Compulsory to be followed by FIs. Therefore, the usage of this document will be very high and impactful only to FIs but all relevant third parties which are servicing the FIs. Publicly available which encourages wider adoption. 	
TRMG	<ul style="list-style-type: none"> The requirements or guidance are detailed so that practitioners can easily adapt and implement in their respective environment. Publicly available which encourages wider adoption. 	<ul style="list-style-type: none"> These are merely recommended guidelines and best practices for organizations. Therefore, the usage of this document may not be very high.
ISO 31000	<ul style="list-style-type: none"> The guideline is a baseline guide that applies to all sectors. 	<ul style="list-style-type: none"> These are merely recommended guidelines and best practices for organizations. Therefore, the usage of this document may not be very high. The guidelines are not detailed. More for high level implementation. This guideline needs to be purchased directly from ISO. This reduces the likelihood that organizations will use this document due to cost.

Conclusion

All three documents have their own advantages and disadvantages. For FIs in Malaysia, they could not avoid complying with the RMiT while in Singapore TRMG is still deemed optional. For non-financial sectors, ISO 31000 is a sufficient baseline for implementing risk assessment.

References

- (BNM), B. N. (19 June, 2020). *Risk Management in Technology (RMiT)*. Retrieved from Bank Negara Malaysia: <https://www.bnm.gov.my/documents/20124/963937/Risk+Management+in+Technology+%28RMiT%29.pdf/810b088e-6f4f-aa35-b603-1208ace33619?t=1592866162078>
- Standard, B. (2018). *Risk management — Guidelines*. BS ISO 31000:2018, 1-26. Retrieved from <https://www.iso.org/standard/65694.html>
- Wei Yang, T. (30 March, 2017). *MAS Technology Risk Management Guidelines (TRMG)*. Retrieved from IT Security 001: <https://simpledu.wordpress.com/2017/03/30/mas-technology-risk-management-guidelines-trmg/>

Protection For Cyber-Bully Victims Under Malaysian Law

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

These days, a lot more people are relying on the Internet as the main method of communication. The Malaysian Communications and Multimedia Commission (MCMC) Internet Users Survey 2020 showed that the number of users rose by 1.3% to 88.7% of the population in 2020 compared to 87.4% in 2018. This survey also revealed that most of Internet users utilize the Internet for social purpose and the most frequent online activity is text communication with 98.1%, followed by social media at 93.3%.¹

Despite its positive impact, the Internet is also used as a tool to cyber-bully others. A case in point was a 20-year-old who was found dead at her family home in Penang after she allegedly fell victim to cyber-bullying over a Tik Tok video that she and her colleague did which drew negative criticism on Facebook as it went viral.²

Cyber-bullying is defined as “abuse/harassment by teasing or insulting a victim’s body shape, intellect, family background, dress sense, mother tongue, place of origin, attitude, race, caste, class, or even name calling using modern telecommunication networks such as mobile phones (SMS/MMS) and Internet (Chat rooms, emails, notice boards and groups)”.³ Cyber-bullying could be in the form of cellular or digital imaging messages, chat and discussion room messages, e-mail, instant messaging, pictures and photographs and unauthorized video, messaging on social gaming profiles and networking sites, such as Chatroulette, Formspring, Facebook and MySpace and on systems, such as Twitter and YouTube, and Web blogs, pages or polling sites to target the victims.⁴

Since cyber-bullying is becoming more rampant as a result of an increase in social communications sites, legal actions should be taken to protect the victims of cyber bully. At the moment, there are no specific prescribed law on cyber-bullying in Malaysia, but there are other laws to curb such cyber-bullying incidents. For instance, Section 233 of the Communications and Multimedia Act 1998 which renders it an offence for any individual to make or initiate the transmission of any obscene, indecent, false, menacing or offensive comment or communication with the intention to annoy, abuse, threaten or harass any individual. Subsection (2) of this section further provides that if a person knowingly by means of any network service or applications service provides obscene communication for commercial purposes to a person or permits a network service or applications service under the person’s control to be used for an activity as described in paragraph (a) of this section, he commits an offence. Subsection (3) to this section states that a person who commits an offence under this section shall, upon conviction, be liable to a fine not exceeding fifty thousand Malaysian Ringgit or imprisonment for a term not exceeding one year or both; and shall also be liable to a further fine of one thousand Malaysian Ringgit for every day during which the offence continues after conviction.

It is further observed that Section 114A of the Evidence Act 1950 (Act 56) also protects victims of cyber-bullying. Subsection (1) to this section provides that a person whose name, photograph or pseudonym appears on any publication depicting himself as the owner, host, administrator, editor or sub-editor, or who in any manner facilitates to publish or re-publish the publication is presumed to have published or re-published the contents of the publication unless the contrary is proved. Subsection (2) to the section states a person who is registered with a network service provider as a subscriber of a network service on which any publication originates from is presumed to be the person who published or re-published the publication unless the contrary is proved. Subsection (3) to this section further provides that any individual who has custody or control over any computer on which the publication originates from, is

¹ Internet Users Survey by Malaysian Communications and Multimedia Commission

² <https://www.thestar.com.my/news/nation/2020/05/22/cyberbullying-victim-leaves-suicide-note>

³ Cyber Bullying: Profile and Policy Guidelines. Tirunelveli: Department of Criminology and Criminal Justice, Manonmaniam Sundaranar University.

⁴ Nurul Mazrah Manshor, Salmah Roslim, Rohayati Hussin (January 2014). The Communication and Multimedia Act 1998: Adequacy of Protections to the Victims of Cyber Bullying in Malaysia. Universiti Teknologi MARA (UiTM), Malaysia

presumed to have published or re-published the content of the publication unless the contrary is proved.

In addition to the provisions under the Communications and Multimedia Act 1998 (Act 588) and Evidence Act 1950 (Act 56), regard may be given to the provisions of the Penal Code (Act 574) to determine whether an act of cyber-bullying constitutes an offence of criminal intimidation or otherwise.

Section 503 of the Penal Code, on the other hand, defines the offence of criminal intimidation. Under this section, to constitute criminal intimidation, a person must have threatened another individual that caused injury to the individual or damaged to the reputation or property; or anyone whom that person is interested. Such threat must have also been made with intent to cause alarm to that person or to cause the person to do any act which he is not legally bound to do as the means of avoiding the execution of such threat, or cause that person to omit to do any act in which that person is legally entitled to do as the means of avoiding the execution of such threat.

It is worthwhile to note that under Section 506 of the Penal Code, the punishment for criminal intimidation is more severe when the threat is to cause death or grievous hurt, or to cause destruction of any property by fire, or to cause an offence that is punishable with death or imprisonment, for a term which may extend to seven years, or to impute the unchastity to a woman.

Furthermore, Section 507 of the Penal Code provides for the offence of criminal intimidation by anonymous communication. If the criminal intimidation is communicated anonymously or under a false name or identity, this section provides for a further punishment in addition to the punishment provided for the offence of criminal intimidation under Section 506.

It can be concluded that the provisions of law as discussed above may well protect the victims from cyber-bully and to help them feel safer. Until a specific law on cyber-bully is being legislated, victims could rely on these laws to protect themselves from cyber-bullying incidents.

Challenges Of New Working Normal

By | Ida Rajemee Ramlee, Syafiq Anneisa Leng Abdullah, Wan Zariman Omar & Nurfaezah Hanis Halim

Overview

In 2020, the world had to grapple with the worst health crisis that infected many people. The latest data reveals that there have been more than 228 million confirmed cases with nearly 4.7 million deaths reported worldwide. Malaysia recorded more than 1.9 million confirmed cases with 19,827 death cases [1]. Globally, COVID-19 has not only caused havoc in public healthcare system among the societies but also resulted in major economic and social turmoil, forcing everyone to accept a new normal of wearing face masks, following the standard operating procedures (SOPs) and lockdowns, as the new way of life.

Although the implementation of Movement Control Order (MCO) has impacted the economy negatively, many companies adapted to the changes by introducing online meetings and flexible working arrangements among the workers to ensure continuity and sustainability of businesses. Various practices have been developed to ensure that this new working arrangement remains secure and safe. Despite the flexibility of working from home (WFH), it is not a one-size-fits-all as the various adaptability and readiness of companies to adopt this new working arrangement may lead to different challenges faced throughout the implementation. In addition, it is crucial to manage these challenges so that the productivity of workers will be maintained at an optimum level. For this purpose, we will look into WFH through three (3) components namely as (i) Process (ii) Technology and (iii) People.

i. Process

As WFH becomes the new normal, more organisations are opting for this arrangement even after the MCO has been lifted. Nevertheless, this shift can be supported with the right processes which should be clearly defined and communicated through the organisation's policies and procedures.

Ever since the pandemic, our working life have changed in many aspects which includes the working environment. The way services are being offered by organizations may need to be relooked alongside the adaption of relevant

technologies, working process, and revamping of standard schedule. For example, a remote working session can be conducted instead of going onsite. The element of flexible working hours, splitting a task, readiness, and safety of the remote working platforms such as teleconferencing or other more suitable remote desktop tools need to be considered.

Relevant policies and procedures which are adapted in the working process have to be reviewed to ensure its suitability, adequacy, and relevancy to adapt and address the new working norm. Amongst the policies related to WFH are Teleworking Policy, Use of Personal Device or Bring Your Own Device (BYO), Backup Policy, Password Policy, and other supporting procedures. These policies and procedures need to be adhered by all employees within the organisation.

Most importantly, the way of handling and dealing with classified operational data need to be clearly defined to employees in order to minimise the risk of data leakage and data security breach.

Proper information security controls need to be put in place while data is being transferred and to ensure the preservation of confidentiality, integrity and availability of data is observed. This can be achieved by managing access to the corporate data resources and usage of designated devices that have been installed with the most current security patches and updated virus definition. In addition, existing VPN capacity may also be expanded and corporate data to be encrypted based on classification level. These additional requirements should be incorporated in the revised processes for the viability during this new normal. This will also ensure that business and operational requirements are met, with productivity not being compromised.

ii. Technology

One of the biggest concerns when it comes to remote work from a corporation's perspective is ensuring the security of network connections. Many have found solace in ensuring the implementation of Virtual Private Network

(VPN) for all those who are required to work remotely as it is a secure connection over the Internet from a device to a network. This will ensure that data confidentiality is preserved and prevents unauthorized user access. However, the quality of VPNs installed is essential to allow employees access to the network with ease without disruption.

WFH also means that any discussions, meetings, and training are required to be held virtually. The selection of the online meeting platforms should be user friendly, trusted, reliable and reputable in terms of security features. Nowadays, there are many online meeting platforms offered for instance Zoom, Google Meet, WebEx, Microsoft Teams, and many other applications on either free or paid licensed basis.

Due to the use of these various online meeting platforms, problems may arise on permission to record such meetings. This is because most online meeting platforms can be recorded without permission by any individual. Some content may have copyright properties and may not be owned by participants. It is the responsibility of the host to manage and control the environment on the online meeting platforms by giving prior consent and clear instructions to participants if the meeting could be recorded. In addition, for shared content a specified level of classification should be observed to maintain confidentiality. Therefore, the host should monitor the online meetings session closely and block unauthorized participants to protect against any data leakage.

With WFH, the type of data, classification level, location of data repository, and how the data is being stored determines the security controls that need to be implemented. In this context, the organization needs to specify a suitable mechanism to store and retrieve the data with proper access control. WFH introduces new risks, hence a thorough risk assessment needs to be conducted and suitable controls should be implemented to preserve confidentiality, integrity, and availability of information.

iii. People

Working from home has changed the working environment where employees are now expected to work longer hours.

This is due to distraction and challenges to meet the deliverable deadline. Employees are forced to a more intense work pace while working at home and in some cases causing greater stress. This may lengthen duration that the employees

are required to work from the typical eight-hour workday. Inability to address these issues may lead organizations to lose competent employees due to disengagement and burnout.

By not providing sufficient and proper support to employees, the attrition rate is bound to increase where loss of talent will surely result in intangible cost to the organization. Addressing these matters will require a good work attitude like self-discipline, self-motivation, and good time management. Priority should be given to the work output and meeting the deadlines instead of the length of hours worked. The management has to implement suitable action plans to ensure that employees are motivated; while maintaining their good work attitude at optimum level.

Conclusion

It can be concluded that there are many challenges faced by both organizations and employees while adopting to WFH. These challenges are no simple feat as there are many factors involving process, technology and people that need to be considered.

As WFH becomes the new normal, ensuring information security through preservation of confidentiality, integrity and availability is of paramount importance and therefore, a main challenge. This can be achieved through defining data classification information to avoid data leakage. Other relevant security controls that need to be implemented can be identified through continuous risk assessment.

Relevant processes need to be governed by suitable policies and procedures to serve as guidance to the employees. The technology that are being used should be free from known vulnerabilities and relevant security patches are updated for employees to perform their tasks seamlessly and more efficiently.

Last but not least, self-discipline is also equally important and employees need to comply with the relevant policies and procedures. With the right processes, technology support and good work attitude, working from home can further increase productivity and efficiency and thus, will be widely accepted as a new working norm.

Reference

1. <https://www.outbreak.my/ms/world>
2. *8 mobile security threats you should take seriously | CSO Online*
3. <https://www.nst.com.my/news/nation/2021/04/678941/study-wfh-may-remain-post-covid-19>
4. *Remote-working checklist: 10 top challenges you'll face during the giant work-from-home experiment | ZDNet*
5. *The 7 biggest remote work challenges (and how to overcome them) (zapier.com)*
6. *Top 5 security issues with working remotely in 2021 - Keap*

Online Proctoring

By | Nor Radziah Jusoh, Muhammad Nahwan, Sulhan Bin Muhammad & Ghani Ganesh

Before the Covid-19 pandemic hit our world, exams were typically conducted in school halls and exam centres using paper methods. Right after Covid-19, the world of examination transformed from the traditional way to an entirely new norm of Online Exam System.

An online exam system or also known as e-exam is one of the alternatives that is currently used by schools, higher learning institutions and adult learning centres. To conduct e-examinations, both students and educators will need a digital device that can support the online system such as mobile phones, tablets or computers that have access to Internet. A webcam and microphone are also required depending on the user's capability.

The exam taker can access exam questions using their designated user id and password. They will have their own individual screen with time display in order to keep track of time. If paper-based exam requires a set of exam question booklet and answer sheets, online exam system uses the screen to display the questions and the students can input the answer to the question directly into the system. Some online exam systems can inform the exam takers of their results on the spot.

During the pandemic, online exam system benefited the education sector when physical exam was unable to take place as usual. However, the big issue is how can educators monitor and prevent the exam takers from cheating?

Proctor

Proctoring or invigilating is defined as an act to monitor exam takers during exam to ensure that they do not cheat. How does proctoring work?

A proctor's role is to monitor tests and exams to ensure that the students are not cheating or manipulating their answers in any way. All exam takers will be briefed and given a set of guidelines or rules by the proctor. Proctors will ensure the exam starts and finishes on time. In addition, they are responsible for conducting and ensuring a fair examination. But how does

proctoring for the online exam system work?

Online proctoring refers to remote invigilation of an exam using online monitoring software and video streaming to increase accountability and ensure the integrity, credibility, and authenticity of the online exam and exam taker. This can be done by installing an online proctoring software that tracks the activity of the exam taker during the exam. Each and every detail will be recorded. In fact, AI (Artificial Intelligence) is used to analyse the activities of exam takers.

The remote proctoring software provides comprehensive support to proctors as it helps them maintain the integrity of online assessments. With the help of the software, the examiner can also validate the identity of the examinee.

Experience on online proctor exam taker

As it is, taking a test or an exam through the traditional method was hardly a pleasant experience. But sitting for an exam at home as a result of global lockdown is even more uncomfortable. According to an online research, thousands of students had taken their first online exam using "ProctorExam" and rated their overall experience '4 out of 5 stars'.

A proctored online exam is monitored by an examiner. The well-structured software will reduce the burden of the already stressed exam takers by providing a positive exam-taking experience.

As more opt for remote learning and online tests, the demand for online proctoring increases. There are several key benefits of using online proctoring and how this eases the burden of educators:

- Proctoring ensures that examinees take fair online tests.
- Proctoring software allows for modifications.
- Applicants can schedule online exams 24 hours a day, seven days a week.

- Comprehension into learner behaviour and patterns is provided by detailed reporting.

The benefits and features of proctored online exams stated above enable a fair testing environment for all applicants. By preventing and discouraging unethical behaviour, individuals are assured that their academic integrity is maintained and institutions' reputation will be safeguarded.

One of the most significant advantages of online proctoring is that it eliminates many of the scheduling issues connected with online tests. Students can better plan their online exams which works based on their busy schedules. Furthermore, they could use a combination of automated and live proctoring available 24 hours a day, seven days a week.

By recognising patterns and understanding how the participants interact with online examinations, proctoring solutions could provide the instructor with a wealth of information regarding their test-taking behaviour. This information can be utilised to future improve future online tests and increase education outcomes.

However, online proctoring has several drawbacks as well. Unlike live exams, students need to have access to suitable technological infrastructure, without which the option for online proctored exams may not work effectively. Naturally, this creates a division between those who have and those who do not have access to technological infrastructure. In addition, students with disabilities will require more guidance and support when taking online-proctored tests. There are also concerns on how the recorded footage will be reviewed and used by others. Because these concerns are unlikely to be solved soon, online proctoring can only be offered as an alternative to other choices. As such, online proctoring should not be reinforced as the only choice; rather it should be deployed in contexts and situations when it is considered the best solution.

Given these concerns and considerations, the following advice should be considered when implementing online proctoring as part of examination processes. Prepare the online examination using the recommended methods. As an example, a university-wide approved online examination approach would assist lecturers in facilitating online examinations in a consistent manner. This will help clarify the duties and obligations of the instructors and

students. Exam takers must be given sufficient information regarding the online proctoring and they should be made aware of it before the start of the examinations.

Reference

1. <https://examonline.in/what-is-online-exam>
2. <https://www.merittrac.com/guides/how-online-examination-works>
3. <https://examonline.in/how-do-online-proctored-exams-works>
4. <https://files.eric.ed.gov/fulltext/EJ1285031.pdf>
5. <https://www.webce.com/news/2020/07/14/how-online-exam-proctoring-and-remote-exams-work>

How Does People, Process & Technology Fit In To Mitigate Malware In A CSIRT Organization

By | Muhammad Nasim Abdul Aziz & Megat Muazzam Abdul Motalib

Introduction

Incident handling and response is a set of technical activities done to analyse, detect, defend against, and respond to particular incidents and assist complainants in solving their computer security incidents. Computer security incidents refers to any event that is considered a threat to management of information systems (JPCERT/CC, 2021) such as; cyber harassment, denial of service (DoS), network intrusion, cyber fraud, and malware attack. Malware attacks are specifically designed to infiltrate the software system stealthily which will lead to negative consequences such as information theft, threats

to the victim and damage to IT devices. To counteract these incidents, every organization needs a Computer Security Incident Response Team (CSIRT), to mitigate cybersecurity related problems.

According to Malware Incident Statistics Feeds from Malaysia Computer Emergency Response Team (MyCERT), there are prevalent malware activities through the years. The total amount of Malaysia Botnet Drones and malware infections by unique IPs over the past 10 years (2011 – 2020) are 16,186,579.00 and 14,426,750.00 respectively (MyCERT, 2021), as shown below in figure 1.

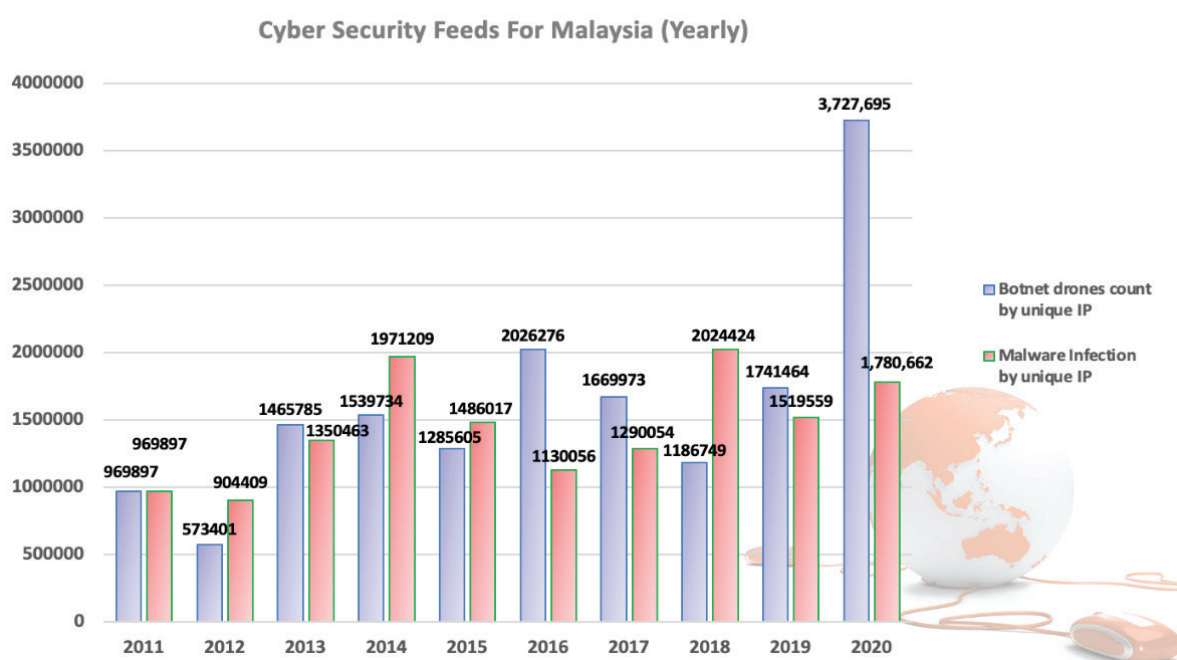


Figure 1: Malaysia Botnet Drones and Malware Infections (2011-2020)

From the statistics above, we can see that there has been a tremendous spike in Botnet Drones by unique IPs that happened in the year 2020. This is probably due to the pandemic that happened in the early 2020, that forced many business activities to go online and rely heavily on the Internet which presented a window of opportunity for cyber criminals to launch

malware attacks.

In The Star news report on 3rd June 2021, the Minister of Communications and Multimedia revealed that during January till May 2021, there was an increase in cybercrime in which 256 cases from the 5,000 reported cases were malicious code (Tariq, 2021).

CSIRT As A Security Organization To Mitigate Malware

CSIRT is a trusted point of reference that deals with computer security related incidents that are technical in nature. The main responsibility of CSIRT is to handle, prevent, and to mitigate incidents relating to computer security as well as assisting the organization in managing their cybersecurity risk.

There are three main services developed by CERT/CC that are traditionally used by many security organizations to handle, prevent and mitigate computer incidents as well as to assist the cyber community in managing their cybersecurity risk. The services are; Reactive Services, Proactive Services and Security Quality Management Services (ENISA, 2010) as shown below.

Proactive Services	Reactive Services	Quality Management Services
<div>1. Alerts, warnings and announcements</div> <div>2. Technology watch</div> <div>3. Security audit or assessment</div> <div>4. Cybersecurity information dissemination</div> <div>5. Cybersecurity monitoring (e.g. intrusion detection, network monitoring)</div> <div>6. Configuration and maintenance of security tools, applications and infrastructure</div> <div>7. Awareness and training programs related to handling cybersecurity incidents</div>	<div>1. Triage function</div> <div>• Incident handling - incident analysis, response on site, response support, response coordination</div> <div>• Handling vulnerabilities - vulnerability analysis, response, response coordination</div> <div>• Artefact handling - artefact analysis, response, response coordination</div>	<div>1. Risk analysis</div> <div>2. Business continuity and disaster recovery Planning</div> <div>3. Awareness building</div> <div>4. Education/training</div> <div>5. Information sharing with other teams in the organization</div>

Table 1 - CERT services of the incident management process adapted by CERT/CC

Based on Table 1 above, malware mitigation can be categorized under Proactive Services. Prevention and protection from malware infections need to be handled with proper planning by individuals that are involved. The process and technology to be used to mitigate the malware attacks and infections has to be properly planned as well. It is crucial to identity a proper plan and the right components to combat malware infection.

People, Process & Technology As Components Of Mitigating Malware

Malware research service specializes in detecting, analysing, mitigating, eradicating and if possible, reversing the damage done by malware in the infected computer system. To accomplish this, an organization needs to hire specialized, trained personnel to resolve malware infections by following a specified set of process with the advanced technological equipment within a CSIRT organization.

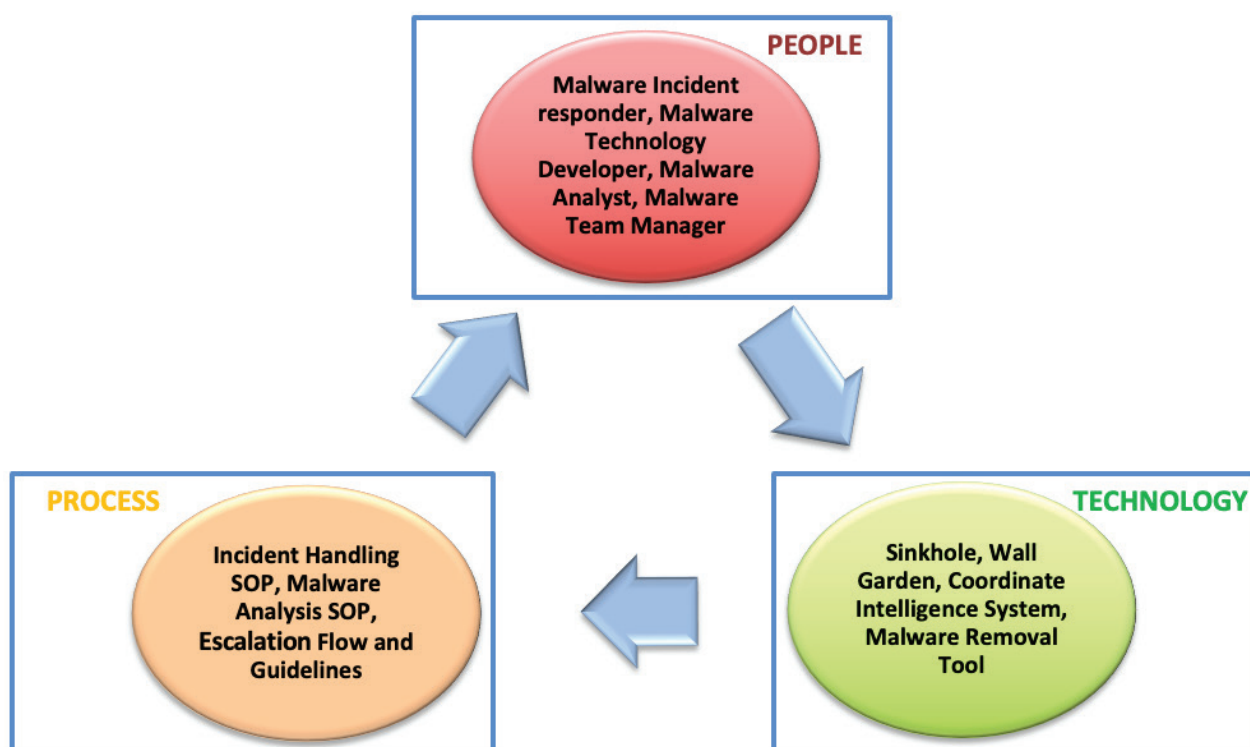
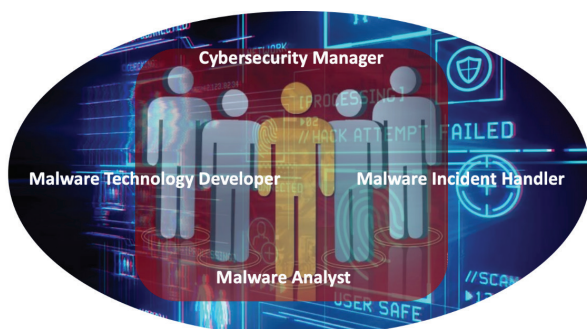


Figure 2: Fundamental Malware Mitigation Components

1. People as a Component in Mitigating Malware

In an organization, the groups and individuals within CSIRT typically comprise Malware Incident Responder, Malware Analyst, Malware Technology Developer and Malware Manager. These individuals are important when it comes to malware mitigation and cybersecurity in an organization.



Malware incident responder - Malware incident responder should be able to demonstrate an ability to respond to complainants as they are the first level responders. According to NIST, malware incident handlers should be able to identify characteristics of malware activities including how it infects and spreads (Souppaya and Scarfone, 2013). These responders would then use their tools to investigate, categorize

the malware and if required, further disseminate the information to relevant authorities. As a malware incident responder, they should be aware of the proper techniques and possess the ability to provide technical reports.

Malware analyst - Malware analysts need to recognize, research, and understand the various design of malware activities and the methods of infection. They need to utilize their knowledge in computer programming to acquire an understanding of malware activities and identify methods to defend similar attacks in the future. Malware analyst should be able to analyse these vulnerabilities and exploitations for which an attack is successful and share this information with other security organizations or individuals to prevent the specific malware infection from spreading.

Malware technology developer - A security software developer or malware technology developer are technologist who formulate computer programs with the intention of protecting computer systems and data in IT devices. They should be able to understand computer programming and cybersecurity concerns by analysing the malware source code in order to identify structures, functions, and vulnerabilities. In a CSIRT organization, a malware technology developer should be able

to perform reverse engineering and document the process of developing these programs. With comprehensive ability, malware technology developers should be able to develop technology and find solutions to mitigate malware.

Malware team manager - In a CSIRT establishment, malware team manager is an individual who manages the resources relating to malware research centre. They are responsible to monitor, manage, organize, and provide guidance to the malware team and resources under their control. Malware team manager should have an in depth understanding of malware threats and should be able to guide their team members on how to mitigate malware. They should be able to communicate with stakeholders and provide useful reports to their superiors in a timely manner. The ability to plan and provide necessary budget to allow an efficient operation of the malware research centre is vital to oversee the operation last long.

2. Process as a Component in Mitigating Malware

Having the right people alone is not sufficient in mitigating malware but having the proper process will support the successfulness of combating malware attack. The process of mitigating malware should allow the specialist to understand what and how it should be done. This process should consist of basic understanding of incident handling SOP, Malware analysis SOP, Escalation flow and the guidelines in handling malware artifacts.

Incident handling process generally consist six phases (Andress, 2014) which are Preparation,

Detection, Containment, Eradication, Remediation and Reporting. Malware specialist will need to abide and understand this process to control the spread of malware infection. They should be able to detect and categorize the type of malware infection by using technical tools that are available to them. The knowledge and proper way to document malware activities is crucial as it will further allow other security specialist to perform malware analysis. Proper guidelines in handling the malware is important to deter it from spreading. As malware is a rising concern in every aspect of the mitigation stages, the escalation flow should be adhered to mitigate the infection. This would not only assist in deterring the spread of malware internally, but also provides useful information to other security organization within the whole cyber environment.

3. Technology as a Component in Mitigating Malware

In order to be effective, malware mitigation technology should be developed by CSIRT. As a security organization that specializes in handling incidents including malware threats, it is important that proactive measures are developed. These measures can be in the form of a collaborative initiative with other specialist or with any concerned security organizations.

CSIRT should also participate in malware Working Groups such as Tsubame WG, M3AAWG and other malware related cooperation to develop malware mitigation systems that would allow effective countermeasures in preventing malware attacks.



Figure 3: How CMERP Protects

Source: <https://www.cmerp.my/index.htm>

CMERP(Coordinated Malware Eradication and Remediation Platform) is an example of technology development collaboration by CyberSecurity Malaysia and Universiti Teknikal Malaysia Melaka (CyberSecurity Malaysia, 2019). Launched in 2019, the goal is to detect suspicious communications through multiple supported protocols, redirects malicious network traffic using sink hole technique and avoid data breach within a network. CMERP then quarantines the infectious machine through a wall garden approach, and finally remediates the computer system with advanced malware removal tools to restore the computer.

Conclusion

Malware mitigation can be resolved with a combination of three fundamental components of People, Process and Technology. Establishing a CSIRT to mitigate malware attacks can be achieved through hiring suitable people, following a proper process, and utilizing an internally developed technological malware mitigation system. This will offer an effective malware mitigation service as all these three components would activate according to CSIRT's intention and objective. It is important that proper recognition be given by stakeholders, within the Computer Security Incident Response Team to these three vital components in mitigating malware.

Bibliography

1. Andress, J. (2014) *The Basics of Information Security. Second Edi.*
2. CyberSecurity Malaysia (2019) *CyberSecurity Malaysia Introduces New Malware Detection & Alert System To Strengthen Data Protection & Cyber Security In Malaysia.* https://www.cybersecurity.my/en/media_centre/media_releases/2019/main/detail/2695/index.html.
3. ENISA, E. N. and information S. A. (2010) *Good Practice Guide for Incident Management.* www.enisa.europa.eu.
4. JPCERT/CC (2021) JPCERT/CC. <https://www.jpcert.or.jp/english/>.
5. MyCERT (2021) *Malaysia Botnet Drones and Malware Infection 2021, MyCERT Incident Statistics.* www.mycert.org.my.
6. Souppaya, M. and Scarfone, K. (2013) *Guide to Malware Incident Prevention and Handling for Desktops and Laptops.* doi: 10.6028/NIST.SP.800-83r1.
7. Tariq, Q. (2021) *Saifuddin: More cybercrime reported during pandemic, TheStar.* <https://www.thestar.com.my/tech/tech-news/2021/06/03/saifuddin-more-cybercrime-reported-during-pandemic>.

Etika Belajar Secara Dalam Talian

By | Nur Haslailly Mohd Nasir & Alifa Ilyana Chong Abdullah

Pandemik Covid-19 yang mengancam seluruh dunia pada hari ini secara tidak langsung telah mempengaruhi sistem pembelajaran mahupun kuliah. Para pelajar terpaksa melazimi pembelajaran jarak jauh secara dalam talian menggunakan medium Internet dengan pelbagai aplikasi pembelajaran seperti Google Classroom, Google Meet, Zoom dan sebagainya.

Sekiranya belajar secara bersemuka ada etikanya yang perlu para pelajar ikuti dalam ruang lingkup bilik darjah, demikian jugalah ketika belajar secara dalam talian. Kamus Dewan Edisi Keempat mentakrifkan 'etika' sebagai prinsip moral (atau akhlak) atau nilai akhlak yang menjadi pegangan individu atau sesuatu kumpulan (persatuan, pekerjaan dan lain-lain). Jika berbicara tentang etika belajar secara dalam talian, ia merangkumi akhlak, nilai dan norma yang berlaku ketika proses pembelajaran tersebut.

Menuntut ilmu dalam Islam sangat menitikberatkan etika belajar. Adab yang baik harus diamalkan untuk meraih keberkatan ilmu yang dipelajari. Imam Malik RA pernah mengungkapkan: *"Pelajarilah adab sebelum mempelajari sesuatu ilmu."*

Berikut adalah 11 cadangan etika belajar secara dalam talian yang boleh diamalkan oleh para pelajar:

1. MEMBETULKAN NIAT BELAJAR

Meluruskan niat menuntut ilmu hanya untuk mendapatkan keredaan Allah Taala.

2. BERSIAP SEDIA UNTUK KELAS

Menyiapkan semua keperluan sebelum kelas bermula. Pautan kelas dan agenda untuk pembelajaran kebiasaannya dikongsikan oleh guru lebih awal. Jadi, sertailah kelas dalam talian dengan keadaan bersedia bersama alatan, buku teks atau apa saja bahan akademik lain yang diperlukan. Bersiap awal boleh memastikan pelajar mempunyai cukup masa untuk bersedia di hadapan kamera telefon mahupun komputer riba untuk pembelajaran.

3. HADIR AWAL KE KELAS

Disiplin untuk menghadiri kelas dalam talian

mengikut masa yang ditetapkan sama seperti kelas bersemuka. Sebaiknya masuklah 5 minit sebelum kelas bermula. Jangan biarkan guru dan rakan sekelas menunggu lama untuk memulakan kelas. Ia merugikan masa semua pihak.

4. BERPAKAIAN SOPAN DAN PATUH SYARIAH

Pakailah pakaian yang sopan dan patuh syariah bagi yang beragama Islam sebelum kamera dipasang untuk menjaga maruah diri pelajar. Hal ini perlu bagi mengelakkan pihak yang tidak bertanggungjawab mengambil kesempatan jika pelajar berpakaian tidak senonoh sepanjang kelas berlangsung. Malah, ia juga boleh mengundang suasana tidak selesa kepada pelajar lain mahupun guru.

5. GUNAKAN RUANGAN PERIBADI YANG SELAMAT DAN SESUAI

Pilihlah lokasi pembelajaran yang selamat dan sesuai semasa mengikuti kelas dalam talian. Gangguan bunyi bising serta keadaan tirai latar termasuk orang yang lalu-lalang di belakang kita dalam keadaan mencolok mata boleh mengganggu perhatian rakan sekelas. Kita juga perlu menjaga privasi keluarga daripada dipamerkan kepada khalayak secara tidak sengaja kerana boleh mengundang aib di kemudian hari.

6. GUNA IDENTITI DIRI YANG SEBENAR

Gunalah nama yang melambangkan identiti diri pelajar yang sebenar bagi memudahkan proses pembelajaran dan komunikasi antara pelajar dengan guru. Jangan mencuri atau menggunakan identiti orang lain khususnya bagi tujuan ataupun dengan niat yang tidak baik. Jangan sesekali berkongsi maklumat peribadi anda dengan orang lain secara sewenang-wenangnya.

7. TUTUP MIKROFON

Mikrofon perlu sentiasa ditutup bagi memberi laluan kepada guru untuk mengajar. Buka mikrofon hanya ketika proses soal jawab atau apabila diminta oleh guru. Hormati guru ketika mereka menyampaikan ilmu dan hormati rakan pelajar lain ketika mereka mengemukakan soalan ataupun memberikan jawapan. Jangan menyampuk! Ia sangat tidak sopan.

8. HIDUPKAN KAMERA

Hidupkan kamera sebagai bukti kehadiran dan tanda fokus semasa pembelajaran sedang berlangsung sebagaimana diminta oleh guru. Etika ini menjadi lebih penting ketika berlangsungnya peperiksaan ataupun kuiz dalam talian bagi mengelakkan penipuan identiti dan juga aktiviti meniru dalam peperiksaan. Jika kita menggunakan medium pembelajaran seperti 'Google Meet' atau 'Zoom', ada pilihan untuk menghidupkan/mematikan kamera. Sebaiknya guru dan pelajar/peserta kelas dalam talian menetapkan agar kamera sentiasa dalam keadaan terpasang jika tiada sebarang kerosakan pada peranti kamera.

9. MEMBERIKAN TUMPUAN SEMASA KELAS BERLANGSUNG

Tumpukan minda serta deria penglihatan dan deria pendengaran (melainkan orang kelainan upaya) semasa kelas berlangsung. Elakkan makan, minum, berbual, mengacau rakan lain dalam kelas, bermain permainan dalam talian, menonton YouTube, membaca komik, berbaring-barang, bermain-main mahupun melakukan apa-apa aktiviti yang boleh mengganggu rakan sekelas ketika kelas sedang berlangsung. Ia boleh mempengaruhi emosi pelajar lain dan juga guru yang sedang mengajar.

10. BERI MAKLUM BALAS SEWAJARNYA

Apabila diminta oleh guru untuk memberikan maklum balas, berikan respons mengikut format yang diminta seperti menggunakan ruangan 'chat box' atau gunakan isyarat tangan. Sebagai contoh, berikan respons isyarat tangan ketika guru mengambil kehadiran dan ketika guru meminta pengesahan sama ada faham ataupun sebaliknya tentang subjek yang diajar. Pelajar tidak seharusnya berlumba-lumba untuk bercakap sehingga menyebabkan keadaan kelas dalam talian menjadi riuh-rendah dan sukar dikawal.

11. SOPAN SANTUN KETIKA BERKOMUNIKASI

Berbicaralah dengan sopan sepanjang kelas berlangsung. Hormati guru dan juga rakan sekelas. Elakkan daripada menggunakan bahasa yang bersifat negatif atau perkataan yang kesat. Jangan menghina atau mengaibkan rakan melalui lisan mahupun tulisan ketika berada di kelas dalam talian. Berilah pujian atas kreativiti, idea dan komitmen kerja rakan sekelas yang lain. Bertolak ansur antara satu dengan lain dan beri peluang kepada semua rakan sekelas untuk terlibat dalam pembelajaran. Mohon izin daripada guru untuk sebarang urusan yang memerlukan anda keluar dari kelas dalam talian

sama ada keluar terus atas sebab kecemasan dan urusan yang tidak dapat dielakkan, mahupun keluar sebentar bagi tujuan seperti pergi ke tandas atau menutup siren penggera keselamatan. Jangan lupa untuk berterima kasih kepada guru atas kebenaran keluar yang diberikan serta ilmu yang dicurahkan, dan ucapkan terima kasih juga kepada rakan sekelas atas perkongsian pengetahuan.

Belajarlah dengan seronok. Tetapi ingat, bilik darjah dalam talian adalah untuk pembelajaran. Semua pelajar dan pengajar sedang melalui proses beradaptasi dengan pembelajaran dalam talian. Sebahagiannya dapat menyesuaikan diri dengan pantas, manakala sebahagian yang lain masih merangkak-rangkak untuk belajar dan bereksperimentasi mengguna pakai kaedah pembelajaran cara baharu ini. Barangkali masing-masing terkesan dengan pandemik ini. Boleh jadi juga ada halangan masing-masing yang tidak mudah untuk ditangani ataupun diselesaikan.

Kesabaran adalah kunci utama! Bersabarlah dengan rakan sebaya dan juga dengan para guru. Belajarlah untuk menghormati dan menerima kelebihan serta kelemahan dan kekurangan antara satu dengan lain agar kedua-dua pihak mendapat keberkatan dalam menuntut ilmu. Mari kita amalkan 11 etika belajar secara dalam talian dan bekerjasama untuk menjadikan pengalaman pembelajaran dalam talian kita positif!

Rujukan

1. *Etiquette Rules for Online Learning* (<https://resources.finalsite.net/images/v1584555915/jbhorg/agup242sjxqkfwsggj73/EtiquetteRulesforonlinelearning.pdf>)
2. *Google Classroom Rules and Expectations* (<https://www.aacps.org/cms/lib/MD02215556/Centricity/Domain/1755/Google%20Classroom%20Rules%20and%20Expectations.pdf>)
3. *Etiquette in the Virtual Classroom* (<https://www.miamioh.edu/regionals/eccoe/news/2020/09/etiquette-virtual-classroom.html>)

Tip Keselamatan Siber: Bekerja Dari Rumah@WFH

By | Noor Asyikin Zulkifli & Azatulsheera Mohd Azman



TIP KESELAMATAN SIBER:

Lindungi maklumat anda ketika bekerja di rumah!

BEKERJA DARI RUMAH@WFH

Salinan data & maklumat

Buat salinan data dan maklumat sekurang-kurangnya seminggu sekali atau 2 minggu sekali, bergantung kepada dasar sesebuah organisasi.



Simpan peralatan/peranti di tempat yang sesuai

Peralatan/peranti daripada organisasi seperti komputer riba, telefon bimbit dan tablet disimpan di tempat yang selamat supaya tidak boleh diakses oleh orang yang tidak sepatutnya.



Kunci pintu rumah

Pastikan rumah hanya boleh dimasuki oleh ahli rumah sahaja. Jangan biarkan rumah anda terdedah kepada orang luar kerana ia akan membolehkan mereka melihat aset di dalam rumah seperti komputer riba, dokumen sulit, mahupun peralatan rumah lain seperti TV dan sebagainya.



Mengatur kawalan keselamatan

Setkan kawalan keselamatan pada komputer riba atau peranti anda dengan kata kunci. Pastikan kata kunci ini tidak dikongsi dengan ahli rumah yang lain terutama sekali jika peralatan tersebut mengandungi maklumat sulit organisasi.

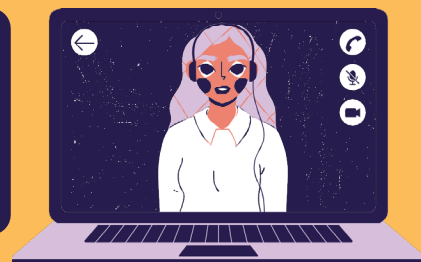


Ruang bekerja bersih, teratur & tersusun

Dapat mengelakkan dokumen daripada hilang, terbang, dan terkoyak. Jangan biarkan dokumen sulit terdedah di atas meja. Pastikan ia disimpan di tempat yang sesuai agar tidak mudah dicapai dan tidak dapat diakses oleh orang lain.

Apabila seluruh dunia dilanda Pandemik Covid 19, ia membiasakan kita untuk bekerja di rumah. Sudah semestinya kita akan berhadapan dengan pelbagai ancaman yang menyebabkan diri kita terdedah kepada risiko kehilangan atau kebocoran maklumat.

Jadi, bagi mengelakkan perkara ini daripada berlaku, 5 tip ini diharap dapat membantu sekurang-kurangnya meminimumkan kebocoran maklumat dan ancaman yang lain.



By: Noor Asyikin Zulkifli & Azatulsheera Mohd Azman

Bagaimana Hendak Bermula: Panduan Kerjaya Profesional Keselamatan Siber

By | Hamidun bin Katemin

Pendahuluan

Malaysia kini sedang dalam fasa pelaksanaan inisiatif Rangka Tindakan Ekonomi Digital Malaysia (MyDIGITAL) apabila perniagaan dan masyarakat memanfaatkan perkhidmatan digital dalam pelbagai urusan seperti e-dagang tanpa mengabaikan aspek keselamatan, perlindungan data dan kerahsiaan. Walau bagaimanapun, perkembangan penguasaan ekonomi digital di Malaysia telah menjadikan ancaman keselamatan siber semakin meningkat dengan bertambahnya penajaan, pertukaran dan penggunaan data oleh pengguna. Justeru itu dalam pelaksanaan MyDIGITAL ini, keselamatan siber telah dikenal pasti sebagai salah satu komponen penting dalam menangani ancaman siber dan juga dalam pembangunan ekosistem digital masa hadapan yang menjurus dan memanfaatkan teknologi kecerdasan buatan dan data raya.

Pelancaran MyDIGITAL ini telah menjadikan kerjaya dalam bidang keselamatan siber kini semakin berkembang dan menunjukkan potensi yang besar selari dengan sasaran utama MyDIGITAL, iaitu mewujudkan 500,000 peluang pekerjaan baharu berpendapatan tinggi. Walau bagaimanapun, kadar penawaran tenaga kerja profesional keselamatan siber terlatih dan berkemahiran masih kurang berbanding dengan permintaan industri. Malaysia kini berdepan dengan senario kekurangan pekerja berpengetahuan dalam bidang keselamatan siber dan bilangan pekerja sedia ada masih belum mencukupi dengan melihat kepada jumlah pengguna Internet yang tinggi.

Justeru itu, rebutlah peluang ini. Jadilah seorang pakar keselamatan siber. Kerjaya dalam bidang keselamatan siber memberikan peluang pendapatan yang lumayan dan amat diperlukan oleh pelbagai organisasi seperti perbankan, perkilangan, perniagaan, sektor kerajaan dan sebagainya pada ketika ini.

Jadi, bagaimanakah anda dapat melengkapkan diri untuk menceburi pekerjaan dalam bidang keselamatan siber yang semakin berkembang ini?

Perkara asas ini perlu dimiliki bagi anda yang ingin berjaya dalam kerjaya berkaitan dengan bidang keselamatan siber:

a. Kelayakan Akademik

Bagi anda yang ingin menceburi bidang keselamatan siber ini, anda amat digalakkan supaya memiliki kelulusan akademik. Keperluan akademik berbeza mengikut tahap dan jawatan. Dengan kelulusan akademik juga anda boleh menjawat jawatan yang lebih tinggi seperti Ketua Pegawai Keselamatan Maklumat.

Diploma

Terdapat beberapa jawatan seperti Pentadbir Rangkaian memerlukan sekurang-kurangnya diploma dalam sains komputer atau disiplin yang berkaitan di samping pengalaman kerja.

Ijazah Sarjana Muda

Kebanyakan jawatan di peringkat pertengahan seperti Penganalisis Keselamatan Rangkaian atau Penganalisis Forensik Digital memerlukan kelulusan akademik peringkat ijazah sarjana muda dalam sains komputer, teknologi maklumat atau disiplin yang berkaitan.

Ijazah Sarjana Lanjutan

Kebanyakan jawatan peringkat pengurusan dan tertinggi atau pakar seperti Ketua Pegawai Teknologi atau Ketua Pegawai Keselamatan Maklumat memerlukan sekurang-kurangnya Ijazah Sarjana Lanjutan atau Kedoktoran.

Persoalan:

Perluakah Saya Mempunyai Kelulusan Akademik?

Jawapan mudah:

Tidak semestinya. Hal ini adalah kerana industri keselamatan siber juga diterajui oleh ramai orang yang tidak mempunyai pendidikan tinggi, atau lulusan universiti. Perkara yang perlu adalah bekerja keras dan berusaha untuk diterima dalam komuniti keselamatan siber. Ia boleh dilakukan melalui pelbagai cara seperti penyertaan dalam pelbagai persidangan atau seminar sebagai pembentang kertas kerja, menyertai dan menyumbang dalam pelbagai projek keselamatan siber dan penyelidikan.

112

Usaha inilah yang dilakukan oleh kebanyakan mereka yang berjaya dalam bidang keselamatan siber dan patut dicontohi oleh mereka yang ingin menceburi kerjaya ini.

b. Minat yang Mendalam

Anda tidak perlu risau sekiranya tidak mempunyai kelayakan akademik. Minat yang mendalam terhadap bidang keselamatan siber juga membolehkan anda menceburi bidang ini. Tetapi, bagaimana hendak bermula? Perkara yang perlu dan boleh anda lakukan adalah mendalami ilmu seperti mempelajari asas pengkodan, pentadbiran pengoperasian sistem tertentu seperti Linux atau Windows, penyelenggaraan aplikasi seperti pelayan web atau pelayan DNS dan mempelajari cara rangkaian berfungsi, termasuk cara komputer dan peranti berkomunikasi dengan trafik rangkaian.

Untuk membangkitkan keterujaan dan menaikkan semangat, anda juga boleh membuat pelaburan dengan membina sebuah makmal ringkas sendiri di rumah untuk merasai pengalaman sebenar dalam menangani ancaman siber. Bina sistem mudah dengan pelbagai sistem operasi pada komputer anda, kemudian buat simulasi ancaman siber. Fahami segala tindakan yang diambil sama ada di pihak penggodam atau penghalang serangan.

c. Pensijilan Profesional

Selain keperluan akademik, anda juga amat digalakkan untuk memiliki pensijilan profesional. Hal ini adalah kerana peluang pekerjaan dalam bidang keselamatan siber juga berdasarkan dan amat menitikberatkan keperluan pensijilan profesional. Pensijilan profesional dapat meningkatkan peluang pekerjaan dan penentuan gaji anda, meningkatkan serta mengukuhkan pengetahuan anda dalam konsep dan amalan keselamatan, seterusnya mendapatkan perspektif yang lebih luas tentang keselamatan maklumat.

Pensijilan profesional ini boleh didapati daripada pelbagai organisasi pensijilan yang diiktiraf seperti CyberSecurity Malaysia melalui Program Pensijilan Profesional Keselamatan Siber Global ACE (www.globalace.org). Program ini menawarkan pelbagai pensijilan profesional berdasarkan domain pengkhususan keselamatan siber seperti Pengamal Blok Rantai IoT, Pengamal Undang-undang Siber, Penganalisis Forensik Siber, Pengurus Risiko Keselamatan Siber, Juruaudit Keselamatan Awan (Cloud), Penganalisis Keselamatan

Data, Pengendalian Insiden dan Keselamatan Rangkaian, Penganalisis SOC, Penguji Penembusan dan Pengamal Aplikasi Selamat.

Program Pensijilan Global ACE ini menawarkan pensijilan berdasarkan Pengetahuan, Kemahiran & Sikap (Knowledge, Skill & Attitude atau KSA) yang diperlukan oleh setiap profesional keselamatan siber berdasarkan domain mereka. Maklumat lanjut berhubung dengan KSA setiap domain boleh didapati melalui pautan <https://globalace.org/ksa/about-ksa>.

Pensijilan profesional seperti yang dikeluarkan oleh Program Global ACE ini berupaya meningkatkan pengetahuan dan kemahiran anda tentang keselamatan siber. Perkara yang perlu anda lakukan untuk mendapatkan pensijilan profesional adalah dengan menetapkan terlebih dahulu domain pengkhususan keselamatan siber yang boleh meningkatkan dan memantapkan kompetensi, seterusnya meningkatkan kebolehpasaran anda. Kemudian, pilih organisasi pensijilan yang menawarkan pensijilan yang anda mahukan. Jika tidak pasti, cari mentor atau rakan yang boleh membantu anda membuat keputusan berdasarkan minat anda.

d. Pengalaman.

Majikan lebih cenderung mengambil pekerja yang mempunyai pengalaman dalam bidang keselamatan siber selain kelayakan akademik. Pengalaman ini amat ditekankan oleh majikan kerana kepakaran mereka boleh terus diterapkan dalam projek yang sedang dilaksanakan. Pengalaman yang berkaitan ini akan terus diterapkan atau diaplikasikan dan ia merupakan salah satu kriteria utama dalam pengambilan pekerja. Kebanyakan majikan tidak mempunyai peruntukan yang besar untuk latihan dan pembangunan kakitangan. Mereka lebih gemar dan menyukai individu yang mempunyai pengalaman yang berkaitan.

Beberapa Panduan Lain:

Bina Hubungan Anda dengan Pakar Keselamatan Siber

- Sentiasa libatkan diri anda dengan seminar, persidangan, konvensyen atau kumpulan kerja keselamatan siber kerana ia menyediakan platform untuk berhubung dan bertemu dengan ramai pakar keselamatan siber, bertukar-tukar idea dan seterusnya meningkatkan atau membangunkan kerjaya anda.

- Pembelajaran yang terbaik, murah dan mudah adalah belajar daripada mereka yang pakar dengan menjadikan mereka sebagai mentor dan sumber rujukan untuk menyelesaikan permasalahan atau pembangunan kerjaya.
- Sentiasa ikuti perkembangan pakar keselamatan siber melalui akaun media sosial mereka. Sentiasa juga mencari maklumat atau mengikuti perkembangan terkini melalui pembacaan menerusi pelbagai media seperti jurnal, majalah, blog atau laman web.

Penutup

Jangan jadikan latar belakang anda sebagai penghalang untuk terus mendalami bidang keselamatan siber. Di samping keperluan utama, iaitu kelayakan akademik dan pensijilan profesional, perkara yang penting juga adalah minat dan keinginan anda untuk terus belajar dan meningkatkan serta memantapkan kompetensi diri. Apabila kemahiran anda mula meningkat dan mantap, dekati atau bertemulah dengan mereka yang pakar dan percayalah bahawa peluang anda untuk menceburi kerjaya ini akan lebih cerah.

Rujukan:

1. <https://prebiu.com/2021/07/13/yayasan-peneraju-komited-lahirkan-ramai-profesional-dalam-bidang-keselamatan-siber/>
2. Program Kolaborasi Cybersecurity Malaysia – Inisiatif Kerjasama Awam-Swasta Kukuhkan Pembangunan Industri Keselamatan Siber Di Malaysia. https://www.cybersecurity.my/data/content_files/44/1936.pdf
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. Kerjaya dalam Keselamatan Siber. Pusat Keselamatan Rangkaian SKMM. <http://snsk.skmm.gov.my>
8. Cybersecurity Career Guide: Advancing Your Career at Any Stage. https://careersincybersecurity.com/wpcontent/uploads/2017/10/Cybersecurity_Ebook_small.pdf

Unsur Keselamatan Siber Dalam Dasar Keselamatan Negara 2021-2025

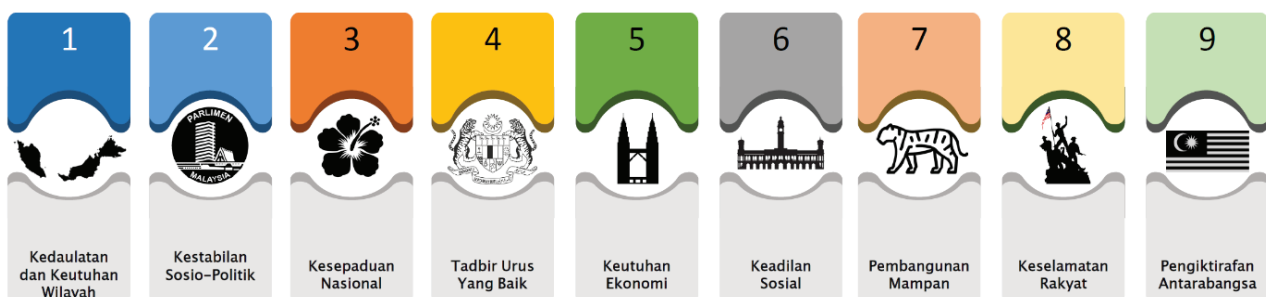
By | Marziation Omar & Nadia Salwa Mohamad

Keselamatan negara ditakrifkan sebagai ketiadaan sebarang ancaman seperti keganasan, peperangan mahupun pengintipan terhadap nilai yang diperolehi¹. Bagi sebuah negara yang berdaulat, falsafah Keselamatan Negara bermaksud usaha berterusan secara menyeluruh demi memastikan Malaysia terus kekal sebagai negara yang berdaulat, aman dan sejahtera. Aman dan sejahtera pula bermaksud tiadanya ancaman yang mengakibatkan kehilangan nyawa dan gangguan terhadap perihai kehidupan rakyat negara ini.

Kerajaan telah menggariskan Dasar Keselamatan Negara 2021-2025 (DKN 2021-2025) sebagai panduan utama bagi Kementerian dan Agensi setiap peringkat pentadbiran termasuk Persekutuan, Negeri dan Daerah dalam pendekatan tadbir urus keselamatan negara secara menyeluruh. DKN ini juga menyatakan komitmen dan langkah strategik kerajaan bagi menjamin kemandirian Malaysia sebagai negara merdeka dan berdaulat berasaskan demokrasi berparlimen dan Raja berperlembagaan. Dengan

mempertahankan Nilai Teras Negara melalui DKN ini, negara berupaya menghadapi ancaman keselamatan yang sentiasa berkembang dan berubah mengikut aliran terkini. Model lima (5) domain keselamatan telah mengurangkan tumpuan terhadap persekitaran fizikal (darat, udara, air) dan memberikan penekanan yang lebih kepada “alam maya”, dan antara ancaman yang dikenal pasti membabitkan keselamatan siber yang mampu memberikan kesan dan impak besar kepada kesejahteraan negara.

Terdapat sembilan Nilai Teras Keselamatan Negara yang diterapkan dalam DKN ini. Nilai Teras Keselamatan Negara yang pertama ialah Kedaulatan dan Keutuhan Wilayah. Malaysia perlu melindungi dan mempertahankan kedaulatan dan keutuhan wilayah daripada ancaman dalam dan luar negara. Kewujudan Persekutuan Malaysia seperti yang termaktub dalam Perlembagaan Persekutuan yang merangkumi semua negeri di Malaysia dan Wilayah Persekutuan hendaklah dipelihara dan dikekalkan.



Kedaulatan Malaysia merangkumi perairan laut wilayah dan hak berdaulat ke atas zon maritim Malaysia serta domain siber Malaysia.

Unsur keselamatan siber yang perlu dilihat dalam melindungi kedaulatan negara termasuk kesiapsiagaan bagi menghadapi peperangan siber, kesediaan dan kesungguhan oleh angkatan pertahanan dalam berdepan dengan ancaman domain siber dan elektromagnetik serta pertahanan siber aktif.

Nilai Teras Keselamatan Negara yang kedua ialah Kestabilan Sosiopolitik. Pada era globalisasi ini,

kestabilan sosiopolitik adalah satu perkara yang amat penting dalam usaha untuk mewujudkan suasana aman dan harmoni dalam kalangan rakyat Malaysia. Kerajaan dan rakyat harus bertanggungjawab dan bekerjasama dalam memastikan keamanan dan kestabilan negara tanpa mengira fahaman politik, agama, etnik, asal-usul dan status sosial.

Dari sudut keselamatan siber dan teknologi, keperluan pertahanan melibatkan pemantauan terhadap isu di media sosial yang mampu menimbulkan kekacauan seperti buli siber yang mensasar kepada kerajaan, parti politik,

organisasi dan individu; pencegahan penyebaran berita palsu dan penerapan kepentingan pembudayaan dalam setiap individu bagi mencapai ruang siber yang sihat dan selamat.

Nilai Teras Keselamatan Negara yang ketiga pula ialah Kesepaduan Nasional. Sebagaimana yang kita sedia maklum, Malaysia merupakan sebuah negara yang mempunyai kepelbagaian kaum, etnik, budaya dan agama. Kesepaduan nasional akan dapat dicapai sekiranya rakyat Malaysia saling memahami, bertoleransi, menerima kepelbagaian antara satu dengan lain dan memahami kontrak sosial yang menjadi tunjang kesepaduan rakyat Malaysia serta menghormati hak asasi manusia berteraskan Perlembagaan Persekutuan.

Sudut keselamatan siber bagi teras ini termasuk pengukuhan terhadap budaya digital Malaysia, pemantauan yang perlu mengambil kira naratif dan naratif balas melalui media sosial dalam cubaan untuk melencongkan pemikiran rakyat kepada ideologi baharu dan tingkah laku negatif yang fanatik kepada satu-satu pegangan tanpa mengira pandangan orang lain sehingga mengakibatkan pertengkaran, dan juga peneguhan minda dan patriotisme komuniti alam siber.

Nilai Teras Keselamatan Negara yang keempat, iaitu Tadbir Urus yang Baik juga merupakan teras penting keselamatan negara. Perkara ini melibatkan sektor kerajaan dan juga swasta. Sesebuah negara yang mempunyai tadbir urus yang baik boleh melaksanakan dasar yang digubal, menguruskan sumber negara dengan cekap dan berkesan, mendapat pengiktirafan antarabangsa dan memenuhi harapan rakyat.

Selain itu, tadbir urus yang baik juga merangkumi sifat integriti yang tinggi, jujur, amanah, adil, saksama, telus, bertanggungjawab dan sebagainya.

Bagi teras ini, kepentingan keselamatan siber mengambil kira penekanan terhadap pengurusan terbaik dalam teknologi data raya, perkhidmatan digital keseluruhan kerajaan dan pelan tindakan transformasi yang dilaksanakan serta tadbir urus dan pengurusan berkesan domain siber itu sendiri.

Seterusnya, Nilai Teras Keselamatan Negara yang kelima ialah Keutuhan Ekonomi. Sesebuah negara yang mempunyai ekonomi yang utuh dan berdaya tahan akan dapat menghadapi ancaman berkaitan ekonomi sama ada dalam atau luar negara. Pengukuhan ekonomi dan penambahbaikan keadaan sosial adalah

antara faktor yang menyumbang kepada pengukuhan tahap keselamatan negara.

Bagi teras ini, keselamatan siber menitikberatkan perlindungan sewajarnya terhadap infrastruktur maklumat penting, pengurusan ekosistem ekonomi digital Malaysia dan ancaman manipulasi teknologi digital yang perlu sentiasa diawasi.

Keadilan Sosial pula merupakan Nilai Teras Keselamatan Negara yang keenam. Perlindungan hak asasi manusia bagi setiap rakyat Malaysia adalah selaras dengan peruntukan Perlembagaan Persekutuan dan undang-undang antarabangsa yang diterima pakai oleh Malaysia. Perkara ini selaras dengan Perlembagaan Persekutuan dengan mengambil kira taraf kemajuan sosioekonomi kaum yang berbeza.

Keselamatan siber dilihat dari sudut merapatkan jurang digital antara semua peringkat rakyat sebaik mungkin, 4IR, impak sosial, budaya, identiti dan jati diri Malaysia serta memperkukuh rangka kerja perundangan dan penguatkuasaan dari semasa ke semasa.

Seterusnya, Nilai Teras Keselamatan Negara yang ketujuh ialah Pembangunan Mampan. Pembangunan mampan ialah pembangunan yang memenuhi keperluan semasa dan masa hadapan bagi mencapai keseimbangan pembangunan ekonomi, sosial, demografi dan alam sekitar. Pembangunan yang mampan juga merangkumi aspek pembudayaan mentaliti dan kaedah pengadaptasian teknologi yang cekap.

Dalam hal ini, keselamatan siber perlu sentiasa diberikan penekanan dalam pengetahuan tentang teknologi pemusnah, pengurusan akses digital dan juga pembangunan Kesedaran, Keupayaan dan Pendidikan Keselamatan Siber.

Nilai Teras Keselamatan Negara yang kelapan ialah Keselamatan Rakyat. Kerajaan perlu melindungi dan menjamin kesejahteraan, kebajikan dan hak rakyat Malaysia di bawah Perlembagaan Persekutuan.

Interaksi sosial dalam talian tanpa had telah menimbulkan masalah yang serius termasuk penggunaan identiti palsu dalam talian.

Keselamatan siber dilihat dari sudut keupayaan untuk mengurangkan jenayah siber, pengurusan keselamatan terhadap data secara menyeluruh dan memperkukuh rangka kerja perundangan dan penguatkuasaan.

Nilai Teras Keselamatan Negara yang kesembilan dan terakhir ialah Pengiktirafan Antarabangsa. Strategi diplomasi dua hala dan pelbagai hala yang dirangka secara menyeluruh, disokong oleh pelaksanaan dasar hubungan luar yang konsisten telah mewujudkan imej positif di peringkat antarabangsa sekaligus menjamin pengiktirafan berterusan terhadap kedaulatan dan kepentingan negara.

Kolaborasi dan integrasi komuniti keselamatan siber di persada antarabangsa perlu diperkasakan, termasuk perundangan siber rentas sempadan dan memperkukuh kerjasama global dalam keselamatan siber.

Akhir sekali, kepentingan keselamatan siber perlu diberikan perhatian memandangkan rakyat Malaysia telah mengalami kerugian berjumlah kira-kira RM2.23 bilion berpunca daripada penipuan jenayah dalam talian sejak tahun 2017 seperti yang dilaporkan oleh PDRM. Kesediaan organisasi bagi menghadapi ancaman keselamatan siber pula masih berada pada tahap rendah seperti yang dilaporkan oleh Trend Micro melalui Laporan Indeks Risiko Siber (Cyber Risk Index – CRI) baru-baru ini.

Kebergantungan terhadap domain keselamatan siber dalam kesemua teras yang disebutkan adalah sangat penting di samping keberkesanan program yang komprehensif dan rangka kerja yang dinamik pada tahap optimum untuk memastikan perlindungan terhadap rakyat dan infrastruktur penting negara.

Rujukan

1. Maisarah Sheikh Rahim; 13 Julai 2021, 6:59 pm; <https://www.utusan.com.my/terkini/2021/07/dkn-2021-2025-strategi-tangani-ancaman-covid-19/>
2. <https://www.malaysia.gov.my/portal/category/298?language=my>
3. Nor idayu Bosro; 13 Julai 2021, 7:54 pm; <https://www.kosmo.com.my/2021/07/13/dkn-2021-2025-strategi-tangani-ancaman-covid-19/>
4. Hafidzul Hilmi Mohd NoorJulai; 12, 2021 @ 1:17pm ; <https://www.hmetro.com.my/mutakhir/2021/07/729645/mkn-kenal-pasti-66-ancaman-baharu-keselamatan-negara>
5. <https://asset.mkn.gov.my/web/wp-content/uploads/sites/3/2019/08/DASAR-KESELAMATAN-NEGARA-2021-2025.pdf>
6. <https://securityandleadership.com/testicsl-paper-1-tactics-of-strategy-and-strategy-of-tactics-adapting-to-complex-competition-and-warfare/>
7. <https://www.nst.com.my/news/crime-courts/2021/07/708911/malaysians-suffered-rm223-billion-losses-cyber-crime-frauds>
8. <https://www.theborneopost.com/2021/08/29/cyber-security-preparedness-still-low-in-malaysia/>
9. Arnold Wolfers; 1952; "National Security" as an Ambiguous Symbol; *Political Science Quarterly*, Vol. 67, No. 4 (Dec., 1952)

Langkah Berbelanja Dengan Selamat Secara Dalam Talian

By | Nur Arafah binti Atan

Pendahuluan

Membeli-belah dalam talian kini menjadi sebahagian daripada kehidupan kita, malah perkara ini telah membuka lembaran baharu dalam sektor perniagaan di negara kita. Pelbagai manfaat dapat dinikmati daripada industri perniagaan dalam talian, namun perkara yang membimbangkan ialah kemunculan kes penipuan siber yang melibatkan produk tiruan, transaksi bayaran atau kualiti sesuatu produk.

Latar Belakang

Pandemik Covid-19 telah mengubah gaya hidup masyarakat dan mewujudkan budaya berbelanja. Sebelum tercetusnya pandemik Covid-19, kebiasaan perbelanjaan masyarakat adalah secara konvensional (luar talian), iaitu dengan mengunjungi pusat beli-belah, pasar raya, pasar basah dan sebagainya. Meskipun berbelanja secara dalam talian telah bermula sebelum era pandemik Covid-19, namun pada masa itu, ia tertumpu hanya kepada barangan perlu sahaja. Apabila bermula sahaja pandemik Covid-19, pembelian dalam talian secara perlahan-lahan telah membentuk kebiasaan baharu dalam kehidupan masyarakat.

Berbelanja secara dalam talian memudahkan pengguna membeli sesuatu barangan tanpa perlu pergi ke kedai secara fizikal. Hal ini bermakna anda tidak perlu lagi memandu, meletakkan kenderaan dan beratur untuk membuat pembayaran di kaunter. Malah, kesemua barangan yang dibeli secara dalam talian akan terus dihantar ke lokasi pilihan anda dalam tempoh masa yang ditetapkan.

Namun begitu, masih terdapat beberapa isu yang timbul terutamanya dari segi keselamatan. Pasti anda pernah mendengar kes penipuan seperti barangan tidak sampai kepada pengguna dan wang tidak dikembalikan kepada pembeli. Insiden ini sebenarnya dapat dicegah sekiranya anda mahir dengan selok-belok pembelian barangan dalam talian serta mengamalkan kaedah pembelian yang betul.

Panduan Berbelanja dengan Selamat secara Dalam Talian

1. Kenal Pasti Identiti dan Butiran tentang Syarikat/Peniaga

Sebelum melakukan apa-apa transaksi dalam talian, identiti peniaga perlu dikenal pasti terlebih dahulu. Seseorang pembeli harus memastikan bahawa mereka sedang berurusan dengan peniaga yang dikenali. Walau bagaimanapun, untuk menentukan identiti peniaga dalam talian yang kurang dikenali ramai, pembeli harus mendapatkan nama, nombor pendaftaran syarikat, butiran perhubungan seperti e-mel, alamat pos dan nombor telefon serta petunjuk yang jelas tentang lokasi peniaga tersebut.

2. Dapatkan Maklumat tentang Reputasi (Ulasan) Syarikat/Peniaga

Selepas mengenal pasti identiti peniaga, pembeli harus memastikan syarikat tersebut mempunyai reputasi yang baik dalam kalangan pembeli dalam talian. Justeru, anda harus membaca ulasan pembeli yang pernah berurusan dengan peniaga berkenaan untuk mengetahui kelebihan serta kelemahan semasa melakukan urusan jual beli dengan peniaga tersebut. Perlu diingatkan bahawa peniaga yang mempunyai tahap penilaian yang tinggi tidak semestinya menjual barangan yang tulen. Penilaian yang baik mungkin disebabkan oleh masa penghantaran yang cepat dan tahap pembungkusan yang berkualiti. Layanan dan cara penghantaran mesej yang baik juga dapat meningkatkan tahap penilaian seseorang penjual selain kualiti barangan yang dijual. Anda perlu pastikan yang anda berpuas hati dengan kesemua aspek penilaian yang diberikan kepada peniaga.

3. Menggunakan Platform & Laman Sesawang yang Sah dan Selamat Semasa Melakukan Pembayaran Dalam Talian

Pelbagai platform jualan dalam talian disajikan kepada pembeli yang menempatkan sejumlah kedai maya yang menarik. Pelaksanaan sistem yang baik pada sesebuah platform adalah penting untuk menjadikan urusan jual beli lebih selamat dan dapat menyediakan khidmat pengurusan wang yang lebih baik, selain mengelakkan isu penipuan.

Pada masa kini, terdapat beberapa platform jualan dalam talian yang menyediakan e-dompet untuk menguruskan transaksi antara pembeli dengan penjual. Ia dianggap sebagai orang tengah dalam sesuatu transaksi kerana mereka 'memegang' wang pengguna sebelum ia diserahkan kepada penjual. Apabila seseorang pembeli menerima barangan yang dibeli dan berpuas hati dengan barangan tersebut, barulah wang tersebut diserahkan kepada penjual.

Anda juga perlu memastikan bahawa butiran kad kredit dan akaun bank diproses menggunakan rangkaian yang selamat. Sambungan enkripsi selamat yang sering digunakan ialah Lapisan Soket Selamat (SSL) atau kata kunci OTP bagi transaksi akaun bank. Selain itu, semasa berurusan secara dalam talian, pastikan anda menggunakan rangkaian yang selamat dan elakkan daripada berkongsi peralatan komunikasi. Anda juga dinasihatkan untuk tidak melakukan pembelian dengan menggunakan sambungan Wi-Fi percuma seperti di kafe atau tempat awam. Sambungan Wi-Fi di tempat awam lebih berisiko kerana sesiapa sahaja yang berada di lokasi sama boleh memantau maklumat yang anda masukkan seperti maklumat perbankan atau kad kredit anda.

4. Membuat Rekod Pembelian/Transaksi

Butiran seperti masa, tarikh, nombor resit dan pengesahan pesanan perlu direkodkan oleh pembeli sebagai satu bentuk bukti pembelian. Semak penyata perbankan anda dan pastikan tiada bayaran ganjil yang dicaj pada akaun anda. Semakan transaksi perbankan secara kerap dapat membantu anda mengesan sekiranya anda telah menjadi mangsa penipuan dan anda boleh mengambil tindakan segera untuk menyelesaikan kes penipuan tersebut.

5. Ambil Perhatian tentang Dasar Kedai seperti Waranti atau Dasar Pemulangan Barang/Bayaran Balik

Selepas menemui barangan yang ingin dibeli, pastikan anda membaca dasar yang digariskan oleh penjual tersebut. Pastikan anda mengetahui tempoh dan jenis waranti yang ditawarkan. Anda juga boleh bertanya kepada penjual tersebut tentang dasar pemulangan barang atau bayaran balik sekiranya barangan tersebut tidak memenuhi spesifikasi yang dijanjikan setelah barang yang dibeli itu diterima.

6. Buat Aduan Sekiranya Barangan yang Dibeli Tidak Memenuhi Kriteria dan Tidak Sampai ke Tangan Anda

Sekiranya barangan yang dibeli tidak diterima dalam tempoh yang ditetapkan, anda boleh membuat aduan terus kepada pihak yang

menguruskan platform tersebut. Kebiasaannya, mereka akan membayar balik wang dengan memulangkannya ke dalam akaun pembeli sekiranya pihak penjual tidak dapat menghantar barangan yang dibeli atau barangan yang dihantar tidak memenuhi spesifikasi yang diiklankan. Aduan seperti ini membolehkan pihak pengurusan mengenal pasti penjual yang bermasalah daripada terus memperdaya pengguna. Mereka akan memadam akaun penjual ini dengan serta-merta sekiranya terdapat kes penipuan.

Sekiranya transaksi dibuat melalui laman sesawang rasmi pihak penjual atau anda melihat laman sesawang yang dirasakan ganjil, anda boleh melaporkannya kepada pihak berkuasa. Anda boleh menghantar laporan kepada Kementerian Perdagangan Dalam Negeri dan Hal Ehwal Pengguna (KPDNKK).

Rumusan

Membeli barangan secara dalam talian sememangnya menyeronokkan sekiranya anda mengetahui perkara yang perlu dipertimbangkan ketika membuat pembelian. Ia memerlukan penelitian dan sedikit kajian bagi mengelakkan anda tertipu dengan barangan yang ditawarkan. Anda juga boleh membuat penjimatan melalui pembelian dalam talian, antaranya dengan memanfaatkan kod baucar, mod pembayaran berdiskaun, atau perkhidmatan ganjaran tunai. Semoga anda mendapat input yang berguna menerusi artikel ini dan lebih bijak berbelanja secara dalam talian.

Rujukan

1. *Empat cara paling selamat membeli-belah atas talian* <https://www.astroawani.com/berita-teknologi/4-cara-paling-selamat-membelibelah-atas-talian-74751>
2. *Tips Supaya Tidak Tertipu Apabila Membeli Secara Online* <https://www.comparehero.my/money-tips/articles/tips-membeli-secara-online>
3. *Tips Membeli Barangan Di Kedai Atas Talian – Ketahui Cara-Cara Untuk Menjadikan Pembelian Lebih Jimat & Selamat* <https://amanz.my/2019199078/>

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

www.cybersecurity.my

 @cybersecuritymy

 CyberSecurityMalaysia

 cybersecurity_malaysia

 CyberSecurityMy

© CyberSecurity Malaysia 2021 – All Rights Reserved



MINISTRY OF COMMUNICATIONS
AND MULTIMEDIA MALAYSIA



ISSN 1985-1995

