

www.cybersecurity.my

eSecurity

The First Line of Digital Defense Begins with Knowledge

Vol 48 - (1/2020)



Overview Of Malaysia Digital Identity Initiative

Overview Of 5G Technology From The Perspective Of MyCERT

My Phone Has Been Hacked

"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 1965-1995



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
(726630-U)

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

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

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



WELCOME MESSAGE FROM THE CEO OF CYBERSECURITY MALAYSIA



Dear Readers,

I am pleased to present 27 interesting and informative articles in this first publication of e-Security Bulletin year 2020. We hope the highlighted articles reflect current issues in cyber security and technological landscape.

We are now experiencing one of the worst global pandemics of this century. The COVID-19 pandemic has had a massive impact in the world and has affected several countries to a standstill already. During these times, cyber security is of more importance, as the environment is conducive for cyber criminals to strike. The pandemic has created an enormous challenge for businesses worldwide to continue operating despite massive shutdowns of offices, public facilities, and schools. Employees have been forced to work remotely. Consequently, schools have resulted in closures, impacting almost 70% of the local student population. Hence, this has resulted in a dramatic increase of the internet users spending more time online. Due to the excessive time spent online, reports of cyber-criminal activities have risen. Effective cybersecurity is most pertinent during this crucial time and requires all parts of an organization, all individuals, and all groups, to work together as a team. Cybersecurity does not just affect a person, but everyone around them. And in the globally connected world we live in, that literally is everyone. Infected devices have a way of infecting other devices, and compromised systems can make everyone vulnerable.

While some of us might already get used to being at work 24-7, there are still some others who are tight to the usual working hours of 8am-5pm five days a week, as their work is considered as critical which relate to system, filing, customer service and others that require face-to-face communication. Working from home has opened multiple vectors for cyberattacks through the heightened dependency on personal devices and home networks; social engineering tactics are even more effective on a distracted and vulnerable workforce; critical business assets and functions are significantly more exposed to targeted cyberattacks; public sector services such as hospitals and healthcare services are under acute pressure and have been hit particularly hard by new types of ransomware at disrupting connectivity and denial-of-service attacks. On this note, be sure to check on the article entitled *"COVID-19 Theme Threats In Malaysia"* together with *"Overview of 5G Technology From The Perspective of MyCERT"* and the other articles in this edition for more ideas to stay safe while actively online.

As COVID-19 continues to alter our lifestyle, organizations and individuals must protect their sensitive data to digitally safeguard themselves. While some changes are likely to be temporary, others will have long-lasting effects. Think very carefully before clicking!

I would like to convey my utmost appreciation to all contributors for their nobility of sharing invaluable knowledge and for continuous support towards our goal of enhancing online safety.

Thank you and warmest regards.

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

EDITORIAL BOARD

Chief Editor

Ts. Dr. Zahri bin Yunos

Editor

Lt Col Mustaffa bin Ahmad (Retired) CJCISO

Internal Reviewers

1. Mohd Shamil bin Mohd Yusoff
2. Ramona Susanty binti Ab Hamid
3. Nur Arafah binti Atan
4. Jazannul Azriq bin Aripin

Designer & Illustrator

1. Zaihasrul bin Ariffin
2. Nurul Ain binti Zakariah

READERS' ENQUIRY

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

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

TABLE OF CONTENTS

1. Importance Of Inculcating A Continuous Learning Culture In Cyber Security	1
2. Industrial Control Systems Under Siege	4
3. Threat Modelling: Wise Or Waste?.....	6
4. Online Purchase Fraud: Challenges And Solutions	9
5. Overview Of Malaysia Digital Identity Initiative.....	14
6. Cyberstalking	17
7. The Conundrum Between Usability & Security For Smart Card with Multi Factor Authentication (MFA)	19
8. Behavioural Biometric.....	22
9. Overview Of 5G Technology From The Perspective Of MyCERT.....	25
10. Cryptocurrencies & Cybercrime	29
11. Forensics Face Recognition Technology – The Challenges.....	33
12. Deploying An Open Source Video Analytics In Cctv For Forensic Readiness.....	36
13. Cyber Insurance: A Panacea To Mitigate Business Risk?	41
14. Factors Influencing Exchange Rates.....	46
15. Protection Of Personal Data: Understand Your Rights As A Data Subject	50
16. “Has My Phone Been Hacked?” – Tips On Common Hardware Failure	53
17. Title Of The Article- COVID-19: Stay Safe On & Offline!	56
18. The Work From Home Checklist	60
19. Transformation To Modern Finance	61
20. Social Media For Awareness Program.....	64
21. Disruption, Obnoxious, Exploitation: Web Defacement Based On MyCERT Case Study.....	66
22. COVID-19 Theme Cyber Threats In Malaysia	69
23. BLOCKCHAIN: Beyond The Cryptocurrency	73
24. Web Application Firewall Detection And Fingerprinting Tools	77
25. Mitigating Terrorism On Social Networks.....	80
26. CyberSecurity : Crossword Puzzle.....	83
27. Senario Keselamatan Siber Sewaktu ‘Perintah Kawalan Pergerakan COVID-19’	84

Importance Of Inculcating A Continuous Learning Culture In Cyber Security

By | Zaleha binti Abd Rahim & Ts. Lt Col Sazali bin Sukardi (Rtd)

“Never stop learning, because life never stops teaching”

Introduction

Learning is a process of absorbing new information and applying the knowledge in a real-life situation. Creating a culture of learning in an organization is not easy especially when it concerns the attitude of learning. If an organization wants to remain competitive, it has to find various ways to inculcate a continuous learning culture. The organization needs to make employee learning a priority not only in policy but also commitment in time and financial resources.

The continuous learning culture requires adopting a new organizational learning mindset namely Didactics (being taught); Discovery (finding out for oneself); Discourse (interacting with others) and Doing (having experiences). Continuous learning is a process of learning new skills and knowledge on an on-going basis that will enable a person to up-skill and re-skill himself in order to perform effectively in the workplace. It is important for everyone to constantly acquire new knowledge and skills using either formal or informal approaches.

Digital Transformation And New Security Challenges

Digital transformation is becoming the largest driver for new technology investments and businesses. Market researcher IDC forecasted that global spending on digital transformation will reach \$1.18 trillion in 2019. Although digital transformation could be costly and risky for any organization, it is no longer a matter of choice. Digital transformation is critical for survival in a competitive era. In recent years, cyber-attacks have evolved to become more brazen and sophisticated. On this basis, cyber security needs to be catapulted to high priority. Organizations will be most vulnerable if they merely focus on technology and processes;

while failing to engage their workforce as part of their overarching security strategy. It is said that humans are the weakest link in cyber security. As such, cyber security personnel must keep abreast of the latest advanced technologies and also, be more proactive in acquiring new knowledge.

Continuous Learning Culture In Cyber Security

Most organizations embrace continuous learning to improve performance and innovation. This can also enhance employee satisfaction and retention as employees who actively engage with learning and training will attain job satisfaction. Employees are valuable contributors to the success of the organization.

There are several activities which organizations can create to support continuous learning:

1. On-the-Job Experience

The most effective way to learn is on-the-job experience because empirical knowledge acquired is well retained. No other learning method is as effective as on-the-job experience. Therefore, it is an organization's responsibility to provide job experiences and training opportunities to its employees that will enable them to attain real learning experiences. The more they are exposed to work, the more knowledge they will acquire. Regardless of success or failure, each employee will learn more as they progress.

2. Formal Training / Seminar / Conference

Formal training is an essential platform to learn and re-learn at a much faster rate. Employees will get to learn from experts in respective fields and follow their instructions and advice especially on technical courses. Formal training courses are normally very costly to organize. Therefore, employees should always grab the opportunity to update their knowledge through such courses.

3. Reading

Reading is the best way to learn. By reading and researching, employees will gain a deeper understanding of a topic. Therefore, fill your leisure time with reading. The more you read, the more you will learn and contribute to the betterment of the organization.

4. Sharing Knowledge

Knowledge-sharing is essential for a company to achieve success as it can facilitate decision-making capabilities, build learning organizations and stimulate innovation. Therefore, employees should be encouraged to share their knowledge.

The more you share, the more knowledge you gain. Sharing one's knowledge helps one to retain and remember the facts. If you have attended a training program outside the office, try to schedule a sharing session immediately thereafter so that the knowledge acquired can cascade through the organization and benefit everyone.

5. Attain Industry Knowledge

Employees should update their business process knowledge as well as industry knowledge.

6. Leadership Qualities

Leadership is not about being the best. Rather, it is about making everyone else better. Everyone is a leader in his/her own right. Employees need to believe in their own capabilities and have enough confidence in their knowledge levels.

7. Give recognition to learning

Do give recognition to individual learning, team learning and community learning. Praise individuals and groups which use learning as one of their success indicators. For example, once a project is completed, the project team is given an opportunity to present their project creatively. This will educate the rest of the organization on the skill sets, key achievements, and lesson learnt.

8. Make the artifacts of learning visible to employees and easy to access

A company's culture can be expressed through its artifacts. To promote a learning culture, it is important to ensure the organization places emphasis in creating state-of-the-art facilities for learning from conference and training rooms to library and e-learning tools.

9. Leaders as Role Model

When employees see that their supervisor is fully engaged and supportive of learning and development initiatives, it creates an atmosphere that promotes continuous learning. Sometimes employees may be hesitant to take time off from daily work for training due to difficulty in getting management approval. Therefore, it is important for leaders to become a role model.

10. Coaching and Mentoring

Mentoring is a great opportunity to refresh one's knowledge and skills while supervising someone. Mentoring need not necessarily be confined to technical knowledge. It could encompass providing guidance, direction, supervision and motivation. In addition, mentoring can give you a boost in confidence to enable you to be a good instructor.

11. Field Work

Field work provides an unparalleled opportunity to study the real world. It provides the opportunity to reinforce classroom-based learning and increases knowledge, skills and subject understanding.

12. Discussion with Peers

A peer discussion is an activity that encourages one to engage with others in reflection on learning and practice. Research shows that having another person's view can help reflect on your practice and reduce the potential for professional isolation.

Benefits of Continuous Learning

To innovate or establish a new process requires learning. Employees need to learn new knowledge or skills in order to expand their horizon and move higher up the value chain. When organizations do not support a continual process of learning, innovation does not happen, processes remain unchanged, and nothing new is ever accomplished. Practicing continuous learning delivers the following benefits for cyber security team:

- Protects the organization against evolving cyber threats
- Enables and empowers cyber teams to perform optimally and efficiently
- Inspires a collaborative culture

- Increases productivity and helps the organization to continually improve, achieve goals and attain new possibilities and capacities.
- Expands knowledge of current hacker methods and understand different ways to stop attacks
- Improves strategic decision making
- Stimulates cognitive activity, keeps teams actively engaged and passionate about what they do

An organization learns when its employees are continuously creating, organizing, storing, retrieving, interpreting, applying and sharing information. The information becomes knowledge and ultimately, wisdom for improving work environment, performance, work processes as well as achieving vision and mission of the organization.

When employees try something new, learn a new skill, or take on an unusual project, employers need to understand that they might not always be successful or even meet their expectations. Despite this set-back, employees need to know that supervisors are on their side. That kind of trust and understanding is essential for creating genuine employee engagement and a continuous learning environment.

When employees realize that their effort will be acknowledged regardless of the outcome, they tend to be more willing to try a new approach, voice their concern, or suggest a new idea. Similarly, they would not cling onto unproductive projects out of fear of failure.

Empowerment gives employees the freedom to make their own decisions, learn from their efforts, and assess the outcomes. This not only encourages career-long learning but promotes trust, team-building, and healthy communication. Therefore, organizations should remove barriers to learning and reward behaviors that facilitate learning such as risk-taking, action learning, constructive feedback and reflection.

Summary

It is not enough for cyber professionals to merely equip themselves with technical degrees and certifications. They should continuously seek new knowledge and learn new skills to stay ahead in the ever-evolving threat landscape so

cyber threats can be thwarted from inflicting any serious damage to an organization. Continuous learning will help up-skill and strengthen cyber security teams so they are always prepared to defend against rising cyber threats. Enhanced understanding, knowledge, skills and application of offensive and defensive strategies will improve an organization's security posture.

To sum up, instilling a culture that values and emphasizes continuous learning will ensure an organization does not easily fall victim to any future cyber-attacks.

References

1. <https://www.td.org/magazines/td-magazine/10-ways-to-build-a-culture-of-continuous-learning>
2. <https://criteriaforsuccess.com/build-a-sustainable-learning-culture-in-4-steps/>
3. <https://www.learningsolutionsmag.com/articles/1898/marc-my-words-ten-steps-to-building-a-learning-culture>
4. <https://www.panopto.com/blog/building-a-sustainable-learning-organization/>
5. <https://biv.com/article/2014/09/benefits-creating-organizational-learning-culture>
6. <https://blog.apruve.com/3-benefits-of-a-learning-culture-every-management-should-know>
7. <https://www.inc.com/entrepreneurs-organization/top-5-ways-a-learning-culture-impacts-bottom-line.html>
8. <https://www.infosecurity-magazine.com/blogs/continuous-learning-50/>
9. <https://www.valamis.com/hub/continuous-learning>
10. <https://www.information-age.com/digital-transformation-changes-security-needs-123478114/>

Industrial Control Systems Under Seige

By | Ahmad Hazazi bin Zakaria, Ummu Khosyatillah binti Muzakir, Mohd Faizal bin Sulong, Muhammad Syahmi Azri bin Zulkefle & Norhamadi bin Ja'afar

At the dawn of digitalisation and 4th industrial revolution, Industrial Control Systems (ICS) are 'facing' its own revolution. From a legacy system, ICS needs to integrate with modern and sophisticated digital technology to improve production capacity and meet market demand. ICS is increasingly being targeted as cyber-attackers take advantage of the Internet to target machines on organizations' industrial networks. With the rise in frequency and sophistication of today's cyber-attacks, companies are struggling to keep up with the onslaught. New threats and vulnerabilities are becoming the greatest risk and it needs to be well managed to ensure the most probable and damaging attacks are dealt with first.

The most significant vulnerability identified in ICS is unauthorised access to the physical system. Unauthorized access will compromise the ICS's availability and its ability to function properly. An internal attacker holds an advantage in privileged access to an industrial network. According to a research report by Positive Technology Security, 82% of cases were insider attacks which meant someone had authorized access and extensive knowledge of the corporate information system [1]. In this regard, an insider attack is the most feared. Once inside the system, an attacker could target any ICS components to perform malicious acts, resulting in severe consequences to the system [1]. Networks, hosts, services and ICS resources access control mechanisms are designed to regulate access and determine level of activities permitted. Only compartmentalization and access control can contain them.

Patching is necessary for software and application to receive latest updates. This should be treated as the highest priority as it remediates vulnerabilities with the highest risk. According to a study published in CPO Magazine, 62% of operating systems in IoT and ICS networks were found not being updated, patched, or supported anymore [2]. However, patching software or application need to be tested under simulation. Any failures, misconfiguration or abnormal results observed during pre-patching testing can then be rectified. In ICS, patching application can be very difficult if security fixes change the way how ICS software interface with the application. Thus, resulting in unstable

system and a disrupted the system operation.

Remote servers to monitor and control ICS applications is widely used to administer ICS hosts. The user from remote servers is granted privilege access to operator screens. Even with privilege access controls in place, remote display protocols used in ICS have been found to accept connections from anywhere, clear text credential and poor encryption algorithm. Should the host server be compromised, the attacker will also gain access to the remote server. This will allow unauthorized change to graphical user interface as well as other ICS software functionality. Exploited connection from the attacker can occur in two scenarios; either from local area network (LAN) where the attacker must gain access or from outside of the ICS LAN which creates higher exposure to attacks.

Some factories and manufacturing plants use web application to access and display human machine interface (HMI) application. It enables a user to access HMI without going through central control. Unfortunately, web services developed for the ICS are vulnerable to cyber-attacks. Moreover, many companies are using insecure connections to upgrade and modernize their ICS and permit backdoor access thus allowing malicious parties to enter the ICS environment [3]. System architecture often use demilitarized zone (DMZ) to protect critical system and reduce network components exposure. However, vulnerabilities that exists in web server could potentially be exposed to an attack path. A poor session tracking, authentication, SQL injection and cross-site scripting vulnerabilities also cause unauthorized access to web servers and applications. One broken in, the attacker can impersonate user identity without proper authentication.

Denial of services, false code execution, data loss and security bypass are some of the possible consequences that may occur due to buffer overflow in ICS services. Programmable logic controller (PLC), HMI, Data Historian, Engineering workstation are all interconnected and thus, interact with each other. Thus, data collection from the field devices is crucial in ICS. Each reading from the field site measurement plays a very important role in determining the

outcome of process production. Buffer overflow is often the result of programmer oversight. Exploited code allows an attacker to create an interactive session in PLC program and send commands with the privileges of buffer overflow. Buffer overflow from remote code execution is also a common attack method to gain access to hosts. In ICS network application, buffer overflow vulnerabilities still exist and mitigation techniques is to reduce their exposure. [4].

The ICS vulnerabilities can be mitigated by compartmentalization in functionality, strong authentication, and limiting application and user permissions to only designated user. Implementation of user privileges may require an overhand in ICS components. Redundant functionality on ICS hosts needs to be removed to minimize unwarranted attacks. Proper documentation on ICS services, applications and networks architecture overview will help organization gain better insight into how ICS system should be maintained and managed.

References

1. <https://www.ptsecurity.com/ww-en/analytics/ics-vulnerabilities-2019/>
2. <https://www.cpomagazine.com/cyber-security/new-cyberx-report-details-ics-security-vulnerabilities/>
3. <https://www.paladion.net/blogs/biggest-threats-and-vulnerabilities-in-ics/scada-systems>
4. <https://fas.org/sgp/eprint/nstb.pdf>

Threat Modelling: Wise Or Waste?

By | Harmi Armira binti Mohamad Har & Farihan binti Ghazali

Cybersecurity is all about staying ahead of threats rather than managing them later. It is not enough to apply security technologies such as Intrusion Prevention/Detection System (IDS/IPS) and firewalls, the software itself needs to close risk gaps. So you need a secure software development process.

The misconception of secure development is that the security elements are applied towards the end of the lifecycle. For an example, penetration or security testing is conducted in the testing or maintenance phase only. However, the ideal concept of Secure Software Development Life Cycle (SSDLC) is implementing security elements in all phases, especially in early development.

In this article, we want to highlight the importance of implementing threat modelling activities. There are many software developers who may still overlook the most crucial step while implementing secure Software Development Life Cycle (SDLC) process. To ensure secure software development, alongside conducting risk management, one of the steps to secure SDLC is to perform a Threat Modelling assessment.

What is Threat Modelling?

Threat modelling is a method of optimizing software and network security by identifying security objectives, locating potential vulnerabilities and developing countermeasures to prevent or mitigate the effects of cyber-attacks against the system. The process involves rating the risks, according to the severity and the probability of occurrence. Details on how to initiate threat modelling will be in the next section. Threat modelling is usually conducted during the design phase of a software development lifecycle. Identifying, categorizing and ranking all potential threats and weaknesses while understanding the software's architecture is important. Threat modelling is widely considered as one of the best methods of improving the security of software.

How to create Threat Modelling?

Threat modelling is used to identify, analyze and mitigate the threats against an application. It allows a threat simulator to gain sufficient understanding on the basic structure of the system and helps build all possible scenarios that could go wrong in an application. Basically, threat modelling comprises four major phases as follows:

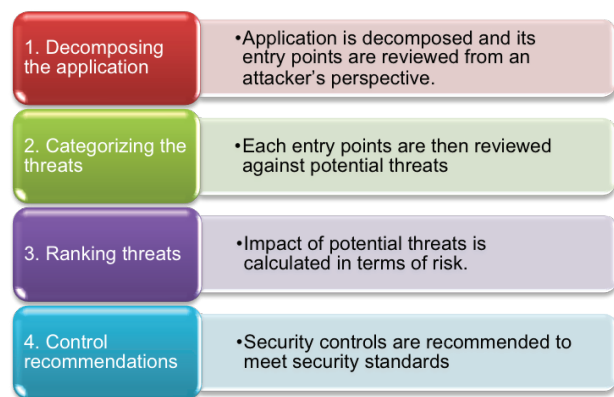


Figure 1: Four Major Phases for Threat Modelling

These major steps can be used as references to execute threat modelling. Moreover, there are also other ways of expressing the application, which can be used to categorize and identify the threats. Architecture representation, data flow diagrams (DFD), and attack/threat trees are methods to illustrate the decomposition of an application. It is important to use the right methodologies when conducting threat modelling activities. More commonly used methodologies include Microsoft Threat Modelling Process, Process for Attack Simulation and Threat Analysis (P.A.S.T.A) and Threat Library Approach.

Microsoft Threat Modelling Process is a step-by-step approach to threat modelling that focuses on identifying assets and architecture, decomposing the application, identifying and documenting the treats. P.A.S.T.A. methodology is a seven-step process applied to most application development methodologies which take into account compliance requirements, business impact analysis and dynamic approach to threat management, enumeration, and scoring. Threat Library Approach uses a pre-

defined set of common and prevalent threats for real-time decision-making analytics.

Aside from this methodology, there are also other techniques for threat enumeration and discovery which can be implemented. These techniques and lists can be used to categorize the threat in order to define the scope of threat modelling. STRIDE technique is one of the most popular techniques that can be used to enumerate and categorize threats. The “Top X Threats” (ex. OWASP’s top 10) list offers an

overview on attacks which were most prevalent based on statistics provided by practitioners.

After categorizing the threats, we proceed to the next phase which is ranking the threats. This phase is where the threats are prioritized based on the risk ratings. The most popular ranking systems are DREAD, CVSSv3, and Open Group Factor Analysis of Information Risk. For each application and scenario, different categories and ranking systems apply depending on the suitability.

An Example of Threat Modelling

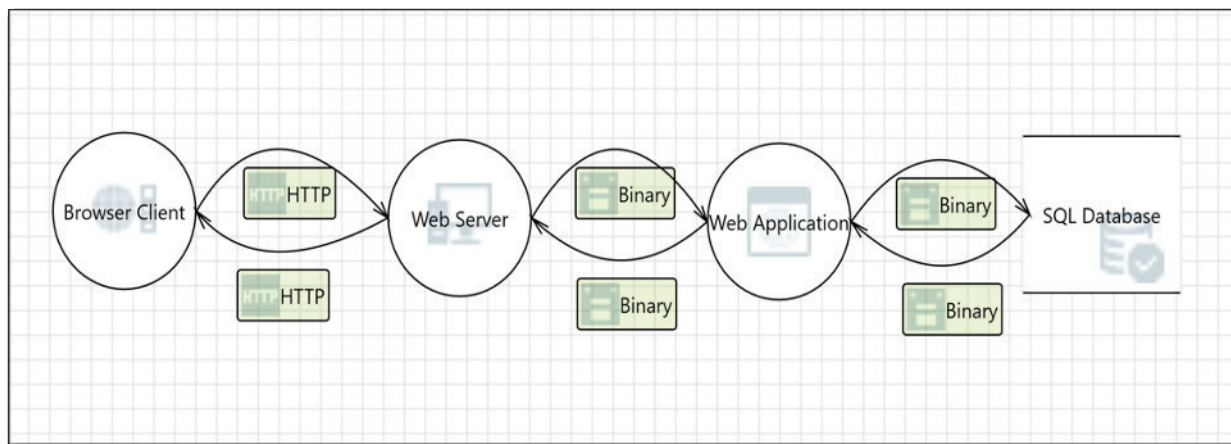


Figure 2: Data flow diagram of basic application

Figure 2 shows an example of a basic data flow diagram of an application. A basic architecture normally consists of five (5) main components: browser client, web server, web application, database, and data flow. The figure above was drawn using Microsoft Threat Tool. This tool helps to generate a set of reports that provides possible threat identified based on the diagram drawn. Microsoft Threat Modelling implements STRIDE methodology as an approach to analyze the diagram and generate all possible related threats. The table below shows an example of the threats identified based on the diagram in Figure 2.

Threat	Category
Interaction: Web Server → Web Application	
1. Web server memory tampered	T
2. Cross-site-scripting	T
3. Elevation using Impersonation	E
4. Weak authentication scheme	I
5. Replay attacks	T
6. Collision attacks	T

Interaction: Web Application → Web Server	
1. Cross-site-scripting	T
2. Elevation using Impersonation	E
3. Weak Authentication scheme	I
4. Replay attacks	T
5. Collision attacks	T
Interaction: Web Application → SQL Database	
1. Persisted cross-site-scripting	T
2. Cross-site-scripting	T
3. Spoofing of source data store SQL Database	S
4. Weak access control of resource	I
5. Risks from logging	T
Interaction: SQL Database → Web Application	
1. Potential excessive resource consumption for web application or SQL Database	D

2. Potential SQL Injection Vulnerability for SQL Database	T
3. Spoofing of destination data store SQL Database	S
4. Authorization bypass	I
5. Lower trusted subject updated	R
6. Risk for logging	T
7. Weak credential storage	I
8. Data logs from unknown source	R
9. Insufficient auditing	R
10. Potential weak protections for audit data	R
Interaction: Browser → Web Server	
1. Spoofing the browser external entity	S
2. Cross-site-scripting	T

Table 1: Possible threats identified using Microsoft Threat Modelling.

Acronym: S → Spoofing, T → Tampering, R → Repudiation, I → Information Disclosure, D → Denial of Service, E → Elevation of Privilege.

Conclusion

Performing threat modelling helps to identify potential threats against the application developed. Threat modelling can be performed throughout the entire development cycle phase, however the earlier the better. Once a set of possible threats is identified in the early phase of development, the programmer or developer must take note and try to avoid writing a code that will open up to the threat. Threat modelling not only identifies threat related to application design, but also can be used to recognize application loopholes and logic business error, which a security scanner often tends to overlook. Different methodologies used for threat modelling may yield a different set of threats. Each methodology has its own merits. It all depends on the threat we want to identify. Threat modelling requires time, knowledge, skills and resources, but it would come in useful at the end of a development life cycle.

This activity helps in minimizing the number of vulnerabilities and risks associated with an application. At the end of the day, it depends on the criticality and asset value of the application developed.

References

1. *Safe Code: Tactical Threat Modelling* (2017)
2. *Threat Modelling: Designing for Security*, Adam Shostack, ISBN 978-1-118-80999-0, 2014
3. *Microsoft Threat Modelling Tool: User Guide* (2016)
4. *Certified Secure Software Lifecycle Professional Textbook*
5. *Secure Web Application Defender Training Module (v1)*, Cyber Security Malaysia (CSM)
6. *Threat Modelling: 12 Available Method* URL: https://insights.sei.cmu.edu/sei_blog/2018/12/threat-modelling-12-available-methods.html

Online Purchase Fraud: Challenges And Solutions

By | Noor Azwa Azreen binti Abd Aziz & Nurfarhana Nasrulhaq binti Mohd Zulkifli

Background In The Asean Region

Southeast Asia is one of the most internet-addicted regions in the world. The top five internet-addicted Southeast Asian countries are the Philippines, they spend 10 hours 20 minutes (10:20) within 24 hours at the top of the list. Then, comes Thailand (10:02), Indonesia (09:11), Malaysia (08:05) and Singapore (07:02). In addition, it is reported that around 90% of Southeast Asia's internet users are smartphone users. Southeast Asia is experiencing rapid growth of Internet, digital, social media and mobile activity. With more than 370 million Internet users in January 2018 and double-digit growth in most segments and most countries of the region, the digital sector is booming and attracting a lot of interest (We Are Social).

According to Google and Temasek 2017 report, it is predicted that Southeast Asia's internet economy is to surpass \$50 billion, significantly exceeding earlier estimates in 2018. It is also predicted that an economy of four times that value by 2025. In 2018, the e-commerce industry has grown at over 100 percent year-on-year, and there are 120 million consumers who are buying online with the top 3 players which are Shopee, Tokopedia and Lazada now counting for 70 percent of this market.

Background In Malaysia

Malaysia has 28.7 million internet users in 2018 (87.4%). Malaysia also emerges fourth globally in mobile social penetration and the lead among Southeast Asian countries including Singapore which is in sixth place, followed by Thailand (eighth) and the Philippines (10th).

As a result of Malaysia's internet and mobile connectivity, Malaysia has high rates of e-commerce usage. Malaysia presents a unique opportunity for businesses as 75% of internet users spend their money via e-commerce, with 58% spending through mobile commerce platforms.

According to an online report export.gov on 19 August 2019, out of all the internet users

in Malaysia, 53.3% of them goes to online shopping websites or application. Malaysia boasts 15.3 million online shoppers (50 percent of the population) and 62 percent of mobile users their devices to shop online. With 19 million Malaysians using the Internet, we have the highest penetration of online shoppers supporting a business worth RM25bil and is expected to double by the year 2020.

A survey conducted by Shopee has also found that 85% of people who shop online are below 35 years old. The study also shows that 90% of those who shop online make their purchases at least once a month.

In addition, according to onlinefraudguide.com, Malaysia is considered as one of the high-risk countries for online fraud. The cases of online fraud in the country are becoming rampant, making up nearly 70% of complaints reported to the Malaysia Computer Emergency Response Team (MyCERT) so far this year. One of the reasons that online fraud keeps on increasing in the country is because Malaysian consumers lack the awareness or just plainly take it for granted and did not take any precautionary measures to prevent them from being the victims of online scam. Furthermore, the consumers also prioritize convenience rather than security and usually the security is put aside or ignored. Thus, there should be a balance between convenience and security amongst the consumers.

Cybercrime

As everyone is aware, the Internet and technology are like a double-edged sword where the widespread use of digital technology has also brought with it new challenges in the form of cyber threats. Cybercriminals will always find ways and also weak points in the network that can be taken advantage of.

The current cyber threat in Malaysia has been seen more complicated and attacks are coming from various locations. It is because the motivation for attacks comes from various aspects not limited to politics, sentiment and ideology, financial and personal gain.

Cybercrime is a fast-growing area of crime. With the advancement of technology, criminals are exploiting the anonymity, unregulated and borderless cyberspace and the speed of development of the internet and tools to commit a diverse range of criminal activities either physical or virtual, causing harm and threats to the victims.

Based on the statement from the Minister of Communication and Multimedia reported by The Star Online on 9 October 2018, the 4 most common types of cybercrime frauds are telecommunication fraud, financial fraud, 419 scams and fraud related to online purchases. In addition, based on fraud reported to CyberSecurity Malaysia through Malaysia Computer Emergency Response Team (MyCERT), fraud purchases are the top three cases that reported to them from January to August 2019. Some of the types of purchase fraud incidents reported are the foreign buyer scam, the upfront deposit scam, the rental/tenancy scam, the auction and merchandise scam, the overpayment scam, the vehicle syndicate scam and more.

Online Purchase Fraud

The fraud purchases online can be via social media (Facebook, Instagram, etc.), Instant Messaging (WhatsApp), purchasing apps (Carousell), websites (Mudah, Lelong, Lazada, etc.), forums and etc.

The common online fraud purchase report received by Cyber999 were mostly related to SCAM. It involved 2 types of scams and they are stated as follows:

1. The buyer didn't receive the purchased item where the payment has been made or the goods received are either less valuable than those advertised or significantly different from the original description. Any attempt to contact the seller would be of no use because the scammers will disappear immediately after they received the transferred money.
2. Seller didn't receive the payment, but the item has already been posted to the buyer.

There are some trends of online purchase fraud by CyberSecurity Malaysia and they are as follows:

1. Most of the offers made by online fraudsters are too good to be true such as the very cheap price for branded items or holiday packages.
2. Seller blocked buyers from communicating (in WhatsApp, Facebook, Instagram), respond with many excuses or disabled his/her account after buyers transferred money.
3. Fraud seller will request few payments for the purchased items for customs clearance, items must be bought in bundle (after first payment), etc.
4. The seller was contacted by a fraud buyer and saying that he/she had already transferred money with some amount which is higher than advertised. So the balance needs to be refunded to the buyer's other account.
5. A buyer transfers the money to a seller by using online banking and delays the scheduled payment by 2-4 days delay. Then, the buyer gives the receipt payment to the seller. After receiving the parcel, the buyer cancels the payment without the sellers' knowledge. In this sort of incident, the sellers rarely check and re-check whether the money transaction is successful.

CyberSecurity Malaysia received a general report of fraud purchases without the monetary lost value. Most of the reports received were from Malaysian victims. For international victims, CyberSecurity Malaysia advises them to report to their Law Enforcement Agency (LEA) and forward the report to the Malaysian Embassy in their country.

Based on the statement from Deputy Secretary-General (Policy) Minister of Communication and Multimedia, online purchase fraud in Malaysia recorded a loss of RM4.2 million for the first quarter of 2019 with is the second-highest cases after call fraud cases. This amount will keep increasing in the future if the relevant action is not taken.

Challenges In Tackling Online Purchase Fraud

Law Enforcement Agencies (LEA) faces many challenges in tracking and catching the perpetrators of online purchase fraud. This is

because these perpetrators most of the time use fake identities and fake profile pictures so that they are not easily caught.

Solutions To Tackle Online Purchase Fraud

There are techniques that can be deployed which allows malicious individuals to be tracked. It requires collaboration with other LEAs, government agencies, international partners and private corporations by using a blend of high-tech and low-tech tactics.

For example in the United States of America, the Federal Bureau of Investigation (FBI), the U.S. Postal Inspection Services, U.S. Customs Service, Internal Revenue Service-Criminal Investigative Division, and the United States Secret Service has developed a program that is called the "Operation Cyber Loss" to combat Internet fraud. The United States also created the Internet Fraud Complaint Center (IFCC) to help with the operation.

Meanwhile in Singapore, the public can provide scam-related information by calling the police hotline or submit the information online. In addition, scam-related advice and experience sharing is made available at www.scamalert.sg.

In Malaysia, the Malaysia Computer Emergency Response Team (MyCERT) normally will request the victim to lodge a police report and notify the respective bank as it is a standard process for fraud online purchase-related incidents. MyCERT will forward the matter to relevant authority bodies such as police to track down the suspects and report to the service provider of the medium used such as mudah.my to investigate the advertisement posted by the suspected buyer/seller.

Platform providers such as Shopee, Lazada, Zalora and e-Bay should also actively monitor and do a detailed background check on the seller that wants to sell their products through the platform providers rather than just simply request the sellers' e-mail address, phone number and also identity card number which can be manipulated, faked, stolen from other sellers or identity. Their system should be able to check and validate the details rather than simply accept and save the information given.

The victim is also advised to refer to Ministry of Domestic Trade and Consumer Affairs (KPDNHEP) to file the report as its involved with

fraud purchases. Internet users may also refer to the link <http://ccid.rmp.gov.my/semakmule/#> to verify the suspected bank accounts.

Netizens also should have a basic understanding of most of the internet frauds that are happening in Malaysia so that they do not fall into the traps of cyber criminals including the ones that are involved in online purchase fraud. Netizens should do some research and know the details of the sellers of the products that they are going to buy.

Many fraudulent cases on online shopping, the public can make a report to CyberSecurity Malaysia (CSM). CSM would assist any Fraud incident request case on a case basis. They would request additional information for further necessary action such as full email header, the related URLs link, screenshot, proof of payment and etc.

CSM would also notify the respective party for further investigation such as the web hosting, website owner/admin, or other relevant agency. The public can report to Cyber999 for any online fraud purchases. Cyber999 can be contacted via:

1. Online Form - https://www.mycert.org.my/online_form/index.html
2. Email - cyber99@cybersecurity.my
3. Telephone – Office Hours: 1-300-88-2999 (24 hours x 7 days)
 - (Emergency): +6019 - 266 5850 Calls to MyCERT
 - Cyber999 Hotline is monitored during the business hours (8:30 AM – 5:30 PM)
4. SMS 15888 using the following format:
 - CYBER999 REPORT (email)(complaint) to 15888
 - Each SMS will be charged at RM0.35 per message.
5. Fax: +603 - 8945 3442
6. Cyber999 Apps:
 - <https://itunes.apple.com/my/app/cyber999-mobile-application/id888552400?mt=8&ign-mpt=uo%3D4>
 - <https://play.google.com/store/apps/details?id=my.cyber999.mobile>

CyberSecurity Malaysia assists in taking down website involved in the fraud activities if it is hosted in Malaysia. They work with Law

Enforcement Agency(LEA) on technical aspects, to facilitate police investigation.

CyberSAFE under CyberSecurity Malaysia is providing awareness to public and Internet users the right way to buy/sell on Internet. This will help the public from being victim of fraud online activities.

Our priority now is to strengthen and effectively collaborate with other countries, agencies as well as higher learning institutions. This includes focusing on 3 main components that are;

1. People for skills, knowledge and talent.
2. Process for policy, strategy, SOP, international/recognize standards
3. Technology that can assist in cybersecurity-related matters such as minimizing vulnerabilities, depth analysis in digital forensics, malware analysis and data analytics.

CSM provides technical assistance to LEA to facilitate investigation and with International agencies, we work closely with the CERTs of the respective country where the fraud activity is conducted/originates by obtaining relevant information related to the fraud.

There is also a need to collaborate bilaterally, multilaterally, regionally and globally in cybersecurity-related areas. They can collaborate in information sharing, skills, best practices, practical legal and technical approached, capacity building and cybersecurity awareness and education.

If the parties had been a fraud in cross-border electronic commerce, they can:

1. Call the Ministry of Domestic Trade, Co-operatives and Consumerism (1800886800) or file the complaint at their website.
2. Call the Royal Malaysia Police department for Commercial Crime Investigation at 603-20319999 or 603-22663333 or visit their website.
3. Call Cyber999 Help Centre
4. Lodge a report to the respective online marketplace such as eBay, Amazon.com, Groupon, Mudah.my, Lelong, Zalora, Lazada, etc. and refer to their terms and conditions on how to conduct any hearing or dispute

Conclusion

The tools and methods of attack from cybercriminals are becoming complex and sophisticated. Moreover, with the increase of transactions via mobile devices, potentially the risks will be even higher. The cyber perpetrators are usually a step ahead of cyber security professionals. This will impact our economy and the safety of the users in the country. That is why cybersecurity professionals need to buck-up and gain more knowledge, skills and training on relevant cybersecurity matters to bridge the gap between cyber criminals and cybersecurity professionals.

Looking at those threats, the protection approach must be holistic. It should equip people with knowledge on how to properly use the internet, as well as process which helps people and technology to be able to communicate in a secure manner.

In terms of technology, we need to do the necessary steps to ensure the machines used are installed with required hardware and software for security to protect against cyber-attack. We also need to ensure that the hardware and software are updated with the latest patches and follow the update schedule.

Again, everyone within the ecosystem has a huge role to play to ensure that consumer education and awareness initiatives had to be designed and targeted to address specific modus operandi that is known to be prevalent or emerging. The info to be delivered should be simple, easy to understand and tailored to the diverse profile of online users.

References

1. <https://seasia.co/2019/02/01/ranked-world-s-most-internet-addicted-countries-based-on-internet-usage-index>
2. <https://www.cio.com/article/3322220/southeast-asia-s-internet-economy-to-reach-us-72-billion-by-end-of-2018.html>
3. <https://wearesocial.com/blog/2019/01/digital-2019-global-internet-use-accelerates>
4. <https://www.thestar.com.my/opinion/letters/2018/03/15/subtle-dangers-lurking-behind-online-transactions/>
5. <https://www.thesundaily.my/archive/85-people-who-shop-online-are-below-35-MUARCH545078>
6. <http://onlinefraudguide.com/risk-countries-fraud/>
7. <https://www.export.gov/article?id=Malaysia-E-Commerce>
8. https://www.kkmm.gov.my/index.php?option=com_content&view=article&id=14891:bernama-23-april-2019-kes-jenayah-siber-catat-kerugian-rm67-6-juta-tiga-bulan-pertama-tahun-ini&catid=118&Itemid=57-8&lang=en

Overview Of Malaysia Digital Identity Initiative

By | Farhan Arif bin Mohamad, Mohd Muslim bin Mohd Aruwa, Nur Iylia binti Ruslan, Mohd Alif Erfan bin Mohd Efendi & Ts. Ahmad Dahari bin Jarno

In the real world, the mechanism of proving the identity of an individual is straightforward. It is conducted using a dual verification system by comparing information against biometric parameters of a human. For example: a picture-based identity card compared to the human facial features or passport with fingerprint biometric parameters towards a human fingerprint.

When an individual shows up at a bank with an intention to open a bank account, or visits a car rental company to rent a car, these places will require the person to present his or her government-issued identity card, proof of address or any verification that might be required for the transaction. The organization usually requires the individual to be physically present at the premises for physical verification. However, this method of identification and verification process is irrelevant in the digital world. In the virtual environment, the respective organisation can seek an alternative method to verify individual, when they are not able to represent themselves physically for verification process based on information supplied by documentation. Thus, as the digital identity (known as Digital ID) emerge through the ecosystem, community and industries must anticipate the need to introduce new mechanisms and technology that are able to address limitations of the current physical verification system.

Keywords

Digital Identity (Digital ID) is a unique representation of an individual's identity in the cyberspace, which is used to enable access to digital services and carry out online transactions in a more secured manner through an authentication process.

National Digital Identity is a Verifiable Platform of Trust aimed at verifying the identity of an individual on the Internet or an individual's virtual identity in the cyber world. It is not intended to replace MyKad.

Digital Identity Verification Platform is used by government and private service sectors to verify

identities of individuals who accessed electronic services, perform transactions and digital signatures provided by them. [1]

Background

The Malaysian Government recently announced an initiative to implement the National Digital Identity (National Digital ID) that will enable Malaysians attain a higher level of confidence in embracing digital economy. The adoption of National Digital ID by the public will be voluntary and not compulsory.

The Ministry of Communications and Multimedia will spearhead this initiative, while a detailed study on the implementation model is expected to be carried out by the Malaysian Communications and Multimedia Commission (MCMC).

A comprehensive study was conducted in September 2019, for a period of nine (9) months. The aim of this study is to identify holistic approaches of the National Digital ID framework and the findings will be forwarded to the Government.

The recommendation is intended to develop appropriate implementation models that meet the needs of the people, businesses and the nation. It will also consider Malaysia's unique context including the existing MyKAD and private infrastructure, current factors, as well as identifying new policies. The study's primary focus includes local contextual analysis, implementation strategy, operating model, technology and enabling policies and related legislations. [2]

In addition, the National Digital ID will also enable the Government and entrepreneurs to innovate and offer digital services that will facilitate business processes using digital signatures. This will promote process improvements and create efficiency as the digital platform is expected to adopt interoperability standards, stronger security and trust for high value transaction through greater identity assurances.

Issues & Challenges

Currently, the government and private digital service providers are providing digital identity verification management systems to the clients independently which have resulted in several limitations and challenges:

1. The fragmented system and proprietary requirements may result in additional preparation and higher maintenance cost due to duplication and increase the cost of investment;
2. There is no standardization or any proven method at national level for the implementation of identity verification;
3. The disclosure of privacy and threat to safety of users' data; and
4. Inconvenience for users while accessing online services due to multiple password and online log ins. [1]

Objectives and Benefits of Implementing National Digital Identity for Internet Users

The objective for the implementation of the National Digital Identity is to support the Government's digital service efficiency and embrace the digitalization of our national economy. It is an important enabling platform in the provision of trusted digital services that is convenient, seamless, as well as time and cost saving.

The implementation of the National Digital Identity (ID) will greatly benefit all stakeholders in our digital economy to conduct their business transactions in a secure and safe manner.

1. People/Users

- Experience stricter identity controls and guaranteed online data privacy
- Time and cost savings compared to counter transactions.
- Streamlined and consistent processes with easier access to government and business services.

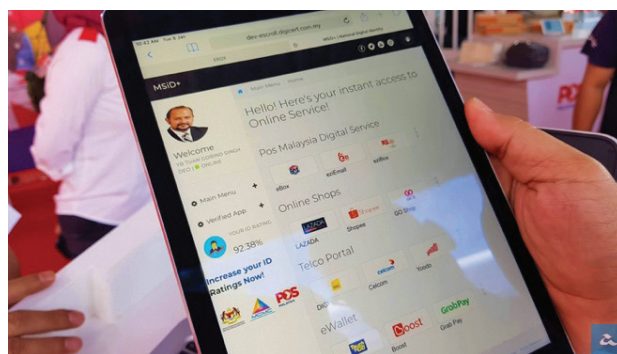
2. Government

- Stimulate and drive the nation towards digital transformation to elevate trust and enhance user's safety in online interactions.
- Improve efficiency and quality of online services for service delivery.

3. Online Service Provider

- Improves efficiency and saves cost in terms of user registration, developing and maintaining their digital identity verification systems.
- Encourage offers of new online services such as fintech, platform economy, apps economy and others.

Case Study: POS Malaysia Demonstrates Prototype of National Digital ID



POS Malaysia recently revealed its own electronic ID called MSiD+. Through this digital ID prototype, users simply need to register online and verify their identities over the counter at any post office and they will be able to enjoy various online services.

The MSiD+ prototype can be used to open new telecommunication accounts, renew driving license, access medical records, or even submit loan application. This new initiative will save consumers the trouble of queueing at post offices. Currently, the MSiD+ remains as a prototype under development. POS Malaysia plans to share its API with other government bodies to intensify integration and enhance user experience. [3]

The Ecosystem of Digital ID & Industry 4.0

As Digital ID accelerates e-commerce and digitalization in government sector and industries, this advanced technology is also being deployed in Industry 4.0.

Development of Digital ID is also driving new and more advanced technologies. Cloud computing will be deployed to develop a more secured online platform through the usage of good cybersecurity solutions. Service providers will also understand the flow of big data and other relevant pillars of Industry 4.0.

Most importantly, the implementation of digital credentials will also boost local industries as it allows them to further utilise the power of Industry 4.0. The overall digitalization process enables local industries to leverage on digital ID and realize the benefits of Industry 4.0.

Although there are several limitations in terms of cybersecurity as well as technologies, these limitations will eventually co-exist in the current IT ecosystem of the local community. The Digital ID initiative is able to reshape the lifestyle of local communities by improving interaction between systems and individuals, thus creating a better and more secure environment for the community. One example of how Digital ID has reshaped lifestyles is the usage of e-Wallets. This digital initiative has been able to reduce online fraud and the number of physical thefts as there is little or no longer the need to carry physical money while travelling.

Digital ID could also play an important role in cross-border controls. Immigration or Customs agency will be able to verify an individual through online databases using ID verification that is linked between countries. This can reduce the usage of passports as the main travelling document and significantly mitigate issues of fake passports, illegal immigrants or even fugitives.

Future Plans

The Digital ID initiative in Malaysia along with the rapid adoption of Industry 4.0 will soon become part of local digital lifestyle. Being a safer and trusted platform, Digital ID will be widely accepted by all users.

Digital ID is easy to adopt and should be embraced as an alternative for identification and verification across all industries. This technology enables people to accept and adopt digital lifestyle with trust. Adoption of Digital ID will certainly create a safer digital space, reduce physical threats and catalyse more innovation for the future.

References

1. *National Digital Identity (2017, July 05). Retrieved from MyGovernment: <https://www.malaysia.gov.my/portal/content/30592>*
2. *Malaysia plans to implement National Digital ID for Internet (2019, August 29) Users <https://www.malaysianwireless.com/2019/08/malaysia-national-digital-id>*
3. *Pos Malaysia Memperlihatkan Prototaip ID Digital Kebangsaan (2019, January 09) <https://amanz.my/2019190494/>*

Cyberstalking

By | Farhan Arif bin Mohamad, Ts. Ahmad Dahari bin Jarno, Shahrin bin Baharom & Muhammad Ashraff bin Ruzaidi

The Internet has revolutionized communications, to the extent it is now the most preferred medium of everyday communication. For most of us, it has greatly influenced our social lifestyles and changed the way we interact with each other. Social media sites allow users to interact and stay connected with their family, relatives, friends, or clients. It enables instant communication with anyone, anywhere, and anytime. Moreover, it helps users expand their social networks.

The emergence of social media and other interactive communication tools have created a world that is more open and connected, thus enabling people to share the most important part of their lives with families, friends and communities. However, there are dangers online and technology can be misused by abusers and stalkers to harass an individual. While social networking allows ease of communication, it may also lead to cyberstalking. Cyberstalking is a form of online harassment in which the perpetrator uses electronic communications to stalk a victim. In the beginning, it may involve sending repeated annoying and unwelcome messages. However, cyberstalking can go far beyond that, which involves threatening (in forms of emotional compromise) or malicious behaviors (leads to unhealthy intentions of threatening someone with harmful actions). While the vulnerabilities of the digital world should not cause paranoia, digital security basics needs to be taught to everyone for the benefit of modern civilization.

What is cyberstalking?

Cyberstalking is defined as online stalking. It involved the use of the Internet or other electronic means to harass or frighten a person or group. Common features of cyberstalking are:



Examples of Cyberstalking

- Making and posting fake or real sexual images of the victim or their loved ones.
- Creating malicious websites, fake social media profiles, and blogs about a victim with intent of compromising one's emotions, status, and well-being.
- Tracking their victims' every movement via GPS.
- Using the victim's social media account or email to stalk and contact others.
- Threatening the victim or their friends and family via emails.
- Releasing personal or fake information to discredit a victim online.
- Uploading personal information such as name, address, social security number or phone number on the Internet.
- Hacking into the victim's social media account to post offensive material and comments.
- Hacking and saving emails, text messages and social media posts and using them to harass or blackmail a victim. [1]

Where to report Cyberstalking?

First of all, if the victim is under 18 years old, he or she must first inform their parents or guardians whom they could trust. Tell them what is happening so they can support and help to stay safe. Victims also should consider changing their email addresses and any other account known to the stalker. Use privacy protection programs and email filtering to block stalkers.

If you are being cyberstalked by a certain individual, report this matter to the police immediately. Cyberstalking is a crime. The Police Department has a cybercriminal unit which handles cases related to cyberstalking. Remember to keep all evidences such as communication logs, online images or any messages so that authorities can track the identity of the stalker.

Victims must not meet the stalker face to face to solve the problem as this can be very dangerous. Therefore, do not act alone as this will cause more harm. Making an official police report is the first step in finding the Cyberstalker. The police will also provide security advice.

In addition, all evidence must be copied to an external disk, flash drive or CD ROM. Do not store it on your computer's hard drive. This is because some stalkers can try to access your computer either while you are online, or by using a virus or malware sent via email to erase all the evidence. [2]

Once all of the above is completed, it is important to contact Cyber999 of CyberSecurity Malaysia to report the matter.

How to avoid cyberstalking?



When it comes to cyberstalking, it is better to be proactive than reactive. Here are a few key pointers to protect against cyberstalking:

1. Abide by clear screen policy

If you are stepping away from the computer, please make sure to log out of computer programs. Lock computer or use a screen saver with a password to prevent others from accessing your computer. The same applies to your smartphone too.

2. Restrict physical access to personal devices

Cyberstalkers can use hardware and software devices to monitor their victims. Everyone must be careful about allowing physical access to a device such as laptops and smartphones. Therefore, do not simply lend personal devices to another person.

3. Private Calendars or itineraries

Delete or make private any online calendars

or itineraries. Such information could allow a cyberstalker to know where and when you are planning to be.

4. Practice good password management

Practice good password management for all online accounts particularly social media accounts. Create complex password that adhere to best practices such as minimum of eight (8) characters in length. The password must contain an uppercase letter, lowercase letter, digit, and special character. Never share the password with others and be sure to change your passwords frequently. Changing the password every six (6) months is strongly recommended. Also do not use the same password for all online accounts

5. Limit online sharing with those who are not in your friends circle

A wealth of information and personal data is frequently shown on social networks such as name, date of birth, workplace, home address and daily routine. Use the privacy settings to block or limit displaying personal information to avoid cyberstalking. [3]

Moving Forward

CyberStalking is a very dangerous trend as it comes with malicious intent. Victims of cyberstalking go through immense psychological strain which may affect their emotional and mental health. As such, it is imperative to educate our youths and adults about cyberstalking and their harmful consequences. Let's make the Internet a safer place for everyone!

References

1. *Cyber-Stalking is Increasing Each Year - Here's How to Protect Yourself* (2017, July 05). Retrieved from GlobalSign: <https://www.globalsign.com/en/blog/what-is-cyberstalking-and-how-to-prevent-it>
2. *Information Security Best Practice Series - Cyberstalking*. Retrieved from CyberSecurity: https://www.cybersecurity.my/data/content_files/11/573.pdf
3. *Cyberstalking: Help protects yourself against cyberstalking*. Retrieved from Norton: <https://us.norton.com/internetsecurity-how-to-how-to-protect-yourself-from-cyberstalkers.html>

The Conundrum Between Usability & Security For Smart Card with Multi Factor Authentication (MFA)

By | Nor Zarina binti Zamri & Noraziah Anini binti Mohd Rashid

Introduction

A smart card, also known as an Integrated Circuit Card (ICC), is a physical electronic authorization device that is used to provide access to resources, be it physically or virtually (e.g. website login page, etc.) [1]. These cards can be used and implemented for a variety of purposes, such as, in the form of a credit or debit card for financial functions, or a personal identification card [1]. Today, the usage of smart cards have multiplied in line with the needs and requirements of the current IT landscape. The smart card has a microprocessor or memory chip embedded that typically allows the card to store between 2,000 to 8,000 electronic bytes of data (equivalent to several pages of data) [2]. The information stored on the smart card's chip could be used to verify a cardholder's identity simply by allowing privileged access that the cardholder is entitled to, thus making its functions broader and not limited to bill payments or money withdrawals alone [3].

Smart cards were originally used as a telephone card for payment for French payphones. But today, the usage of smart cards has become more versatile and is applicable for various industrial sectors such as banking, healthcare, education, telecommunication, financial and etc. In the healthcare industry, the smart card has been used to verify a patient's identity for insurance claims. This will definitely speed up the overall application process for treatment, billing and prescriptions as personal details can now be promptly processed by accessing the data stored in the smartcard chip. In the financial and telco industries, these smart cards are also being used for payment authorization and registration of SIM cards for mobile phones [3].

However, treating smart cards as the only secured platform for securing data such as credentials etc., still leave users vulnerable to cybercrimes. To address this growing concern, smart cards are now paired with Multi Factor Authentication (MFA). MFA is an authentication step whereby users will only be granted access to

resources upon successful presentation of two or more proof of identity, such as, ownership, inherence or even knowledge [4].

Multi factor authentication



Figure 1: MFA Factors [5]

Figure 1 illustrates the three types of determinants, or factors, that are required to link an individual to a strong credential [5]:

1. **Ownership:** something you have - a smart card or a badge.
2. **Inherence:** something you are - a biometric trait, such as fingerprint or iris pattern.
3. **Knowledge:** something you know - password or your birthplace.

The specific evidence that an individual provides to support each factor (e.g. the card, the fingerprint, and the password) is called an authentication token. Smart cards developed with one or more authentication token promotes strong multifactor authentication that significantly strengthens access security.

Discussion

The option of developing an additional authentication factor to pair with a smart card is commonly debated on because of its usability (how easy it is for users to use the product) and security level. Different system implementation uses different authentication factors to increase the security level while still preserving the accepted usability for certain technologies. The

high level of security implementation without ease of use will lead people to regard security as bothersome.

In this article, we will discuss three types of Multi-Factor Authentication.

1. Password Authentication

Passwords are the most common authentication step for any web-based applications, systems-based applications and also the entire system. User generated passwords are easier to remember because it often relates to favourite activities such as fishing, sleeping or any predictable routine. It can also be the names of dear ones. These user generated passwords that are obviously easy to guess or crack is the primary cause of rising security concerns [6].

To ensure users set up complex password, the Password Policy in the password configuration requirement must be enforced. The objective of the said policy is mainly to avoid users from creating weak passwords. This Password Policy is defined as a set of rules to ensure passwords are strong and follow certain requirements. The rule of thumb for password creation should be as follows, but not limited to [6]:

- A minimum of 16 characters
- Complexity through usage of multiple characters
- Exclusive whereby it is only used for one account
- Short lived in which the password has an expiry date and needs to be updated regularly (e.g. 6 month)
- Difficult to guess

As for the pairing with smart cards, users would generally use their corporate's email access, where they would present the smart card together with the account's username and password.

With regards to Password Policy enforcement, most users find that it is quite burdensome to generate strong and complex passwords, as depicted in Figure 2. This leads to increasing use of simple unsecured passwords in the implementation thus ignoring the security impact.

Weak implementation of password authentication mechanisms may cause security flaw such as the password can be easily guessed. Since the password is set by the user himself, studies have

shown that users are more likely to provide easy to remember passwords, without being aware that weak passwords are vulnerable to hacking. If an attempt to guess a person's password is unsuccessful, hackers may find other available loopholes to break into an account [7].

The security flaws present in the Password Authentication has caused users to opt for a better authentication mechanism such as PIN Authentication and Biometric Authentication.

A substantial minority of online adults express password concerns

% of internet users who say they ever ...



Source: Survey conducted March 30-May 3 2016.
"Americans and Cybersecurity"

PEW RESEARCH CENTER

Figure 2: Password habits of Web users [8]

2. PIN Authentication

PIN is a numeric or alpha-numeric password which is used as an authentication token in accessing certain resources or system. Started in the year 1967, this form of authentication has been implemented for financial transactions involving the Automated Teller Machine (ATM) to authorize and dispense cash. Typically, users must key-in the correct PIN to verify any transaction [9].

Based on the international standard ISO 9546-1 PIN Management, an ATM PIN should be between four to twelve digits long. ISO encourages longer PINs as they are more secure. However, longer PINs might be harder to remember. Hence, the ISO recommended that users should not assign a PIN that is longer than six digits to promote better usability. Today, these six digit PINs are widely used across various platforms apart from ATM, such as the secure Type Allocation Code (TAC) code, mobile phone access code, building access door code etc. [10].

Since six digits PIN still does not guarantee better

security, but pairing the PIN authentication with a smart card might. However, as PIN is more or less similar to Password authentication, the risk of forgetting the PIN for ongoing transaction still exists.

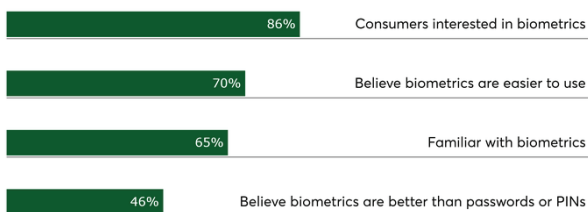
3. Biometric Authentication

Biometric authentication is another popular authentication mechanism, as depicted in Figure 3.

Biometric authentication is a security mechanism that relies on the unique biological trait of an individual to verify that the person's identity. For example, fingerprint, face, iris, vein, voice, retina and many more (biometric areas are also evolving on a daily basis), are called biometric modalities.

Consumers warm to biometrics

As passwords fade, users see the value in more advanced protection



Source: Visa, AYTM Market Research

Figure 3: The usage of biometric authentication mechanism[11]

Biometric modality (as mentioned in Figure 1), refers to a trait that a person inherits. This is something that this individual carries along all the time and can be accessed easily whenever needed, without the risk of forgetting.

For a better biometric security implementation, it is advised that this biometric template is stored within the smart card and live verification performed with the stored template. While promoting a better usability, the usage of biometric authentication also promotes better security.

Due to flexible factors, biometric has been paired with smart card usages. It is now used in sectors which require advance level of security such as custom verification at borders where users need to present their passport and biometric modalities (e.g. fingerprint recognition, face recognition etc.) for verification.

Also, in countries like Malaysia, the government has introduced fingerprint verification with the

national Identification Card (IC), called MyKAD. This card can be used for any transactions that requires the verification of a person's identity.

Conclusion

Despite all the security measures put in place, a combination of smart card authentication with MFA, a backup authentication method is still needed to complement the primary authentication method, in the event of any system failure or user's mishap. There are many authentication methods that can be used as backup such as captcha image verification, security questions, catchphrase, pattern drawing, phone call etc.

Nonetheless, authentication implementation must prioritize the balance between usability and security to ensure that the security level can be preserved while maintaining user's satisfaction. It is important to ensure a positive user experience.

References

1. <https://www.gemalto.com/companyinfo/smart-cards-basics>
2. <https://www.tech-faq.com/smart-card.html>
3. <https://www.securetechalliance.org/publications-strong-authentication-using-smart-card-technology-for-logical-access/>
4. <https://www.loginradius.com/blog/2019/06/what-is-multi-factor-authentication/>
5. <https://www.cyber.nj.gov/this-is-security/the-importance-of-multi-factor-authentication>
6. Inglesant, P. G., & Sasse, M. A. (2010). *The true cost of unusable password policies: Password use in the wild*. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*(pp. 383-392). New York: ACM.
7. <https://swoopnow.com/password-authentication/>
8. <https://www.pewresearch.org/internet/2017/01/26/2-password-management-and-mobile-security>
9. https://en.wikipedia.org/wiki/Personal_identification_number
10. https://en.wikipedia.org/wiki/ISO_9564
11. <https://www.paymentssource.com/opinion/cheap-and-simple-payment-tech-in-asia-opens-the-door-for-biometrics>

Behavioural Biometric

By | Indumathi D/O Vijayakumaran, Nur Iylia binti Ruslan, Mohd Muslim bin Mohd Aruwa, Farhan Arif bin Mohamad & Ts. Ahmad Dahari bin Jarno

Introduction

Behavioural biometric (BB) is an evolving technology that authenticates users based on specific patterns of behaviour.

This technique is able to recognize, capture, record, and/ or verify the identity of a person based on a specific set of defined pattern. BB works by uniquely identifying an individual through devices that has a 99 per cent accuracy rate that improves over time [1].

The focus of the BB recognition is on the method used in performing a specific activity rather than the output of that activity. Devices such as smart sensors or smart phones are used as a medium to capture data from authenticated users in order to study and analyse their pattern. This article provides an in-depth analysis on behavioural biometric that is set to enhance the future of human recognition with higher accuracy and feasibility in IT security.

Categories of Behavioural Biometric

According to Kim Smith, Content Marketing Manager of GoodFirms, researchers have categorised behavioural biometrics into five (5) categories as listed in diagram 1 below [2].

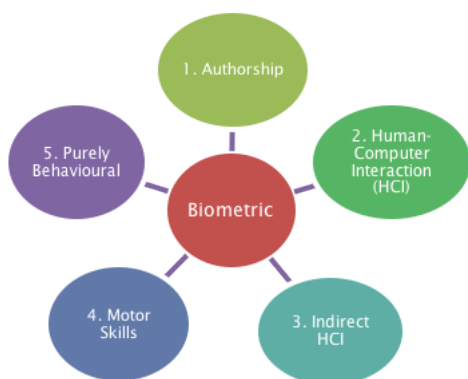


Diagram 1: Categories of Behavioural Biometric [2]

1. Authorship Based Biometric

The authorship pattern of a person on their text, paintings, and handwriting are used as baseline material to analyse and acquire the unique identity of a person. These traits are then used to train the biometric devices in capturing their identity based on the behavioural patterns. The details of the baseline material plays an important role in ensuring the parameters that are generated for the biometric devices are meeting certain levels of accuracy or also known as completeness, to be able to support the training of biometric devices while in the capturing process.

2. Human-Computer Interaction (HCI) Based Biometrics

An intelligent device is used in a computer to capture the style of an individual (e.g. certain movement or human reaction) that interacts with the computer system and helps in acquiring the required data. The key purpose is to uniquely identify a person based on their behavioural pattern.

3. Indirect HCI based Biometrics

This is an alternative method to indirectly capture the activities of an individual that interacts with the systems in the computer. The findings will then be used for behavioural analysis. Data is generally collected from an individual's activity that involve call logs, web surfing and a number of frequently used software. These data will help in studying their pattern of behaviour.

It is important to note that, this method is only used as a supporting parameter for HCI and it is not recommended as the main medium for data collection or as a main HCI method.

4. Motor Skills Based Biometrics

The muscle movements of an individual are captured to study their behavioural pattern. These movements are then used to identify and verify the original person to check the accuracy of detection.

5. Purely Behavioural Biometrics

The human skills, knowledge and strategies required to handle demanding tasks are collected in order to study behavioural traits. The process of identifying a person is then carried out using these collected data.

However, technology deployed under this method is still not able to identify in a seamless and perfect way. But improvement is certainly being made to address higher expectations for the implementation of a systematic and advanced biometric recognition system.

Common Types of Behavioural Biometrics

1. Keystroke

- The typing rhythm of a person.
- Timing of each keystroke on keyboards or adaptive keyboards, the pressure placed on each key etc.

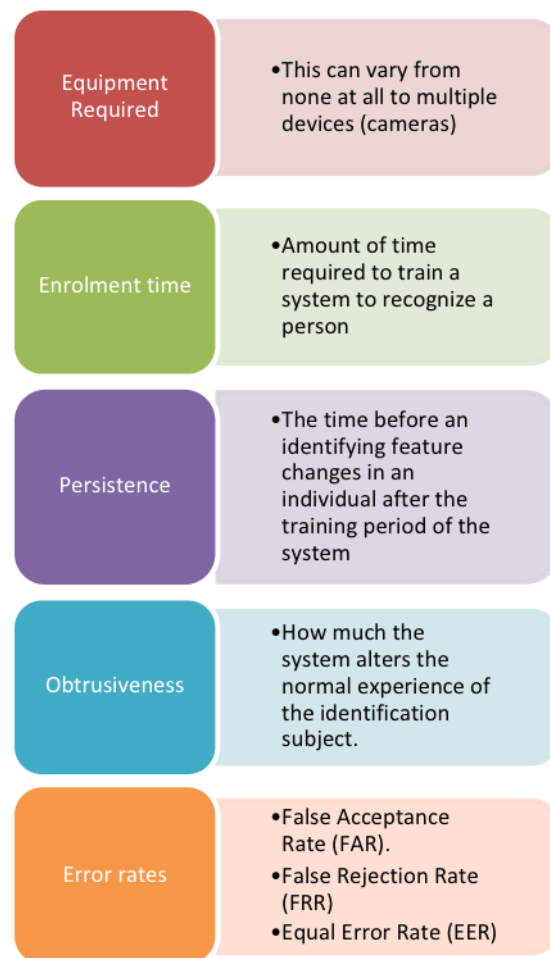
2. Signature

- Static (offline) – user places his signature on a paper; biometric system then recognizes the signature and analyses its shape
- Dynamic (online) – user places his signature on a specialized writing tablet that is connected to a computer

3. Voice

- Speaker identification method via voice recognition is one of the most advanced research on biometric technologies.
- Speaker identification process can be categorized according to the vocal tone of what is being spoken. The unique, regular variations in sound that occur as a user speaks has its own uniqueness in identifying a person.

Important Factors to Consider for a Successful Implementation of Behavioural Biometrics



Types of Attacks

- *Coercive Impersonation* – a type of attack in which the attacker physically forces a genuine user to identify himself to a system or removes the biometric (for example, a finger) from that person to be used as a key to gain access to certain resources [3].
- *Replay Attack* – recording a previously produced biometric such as taking picture of a face or recording a person's voice and submitting it to the biometric data collection unit [3].
- *Impersonation Attack* – an attack whereby the attacker can change his appearance to match a legitimate user. For example, using makeup to copy somebody's face or impersonating voices or forging a signature [3].

Conclusion

Biometric recognition solutions have evolved according to the needs and requirements set by the industry. The whole system today has become so complex that it is behaving more like human rather than a computing system. Programming a computing system to set human biometric parameters is akin to teaching a child to understand, communicate or interact with others.

By understanding the biometric characteristics and how it fits in perfectly as a security enforcement product, developers should design products that are complex and securely designed from the ground up. Most importantly, these products should convince users to trust biometric technology in protecting and securing operations from exploitations by cyber criminals.

References

1. Alex Rolfe, 2018. *Behavioural biometrics: How will it improve the consumer experience*, retrieved from <https://www.paymentscardsandmobile.com/behavioural-biometrics-how-will-it-improve-the-consumer-experience/>.
2. Erika Morphy, 2018. *What Are Behavioral Biometrics and How Do They Fit Into Marketing*, retrieved from <https://www.cmswire.com/customer-experience/what-are-behavioral-biometrics-and-how-do-they-fit-into-marketing/>.
3. Giles Hogben, ENISA Briefing: *Behavioural Biometrics*. Retrieved from https://www.enisa.europa.eu/publications/behavioural-biometrics/at_download/fullReport.

Overview Of 5G Technology From The Perspective Of MyCERT

By | Md Sahrom bin Abu & Muhammad Nasim bin Abdul Aziz

Introduction

Over the last few decades, the smartphone industry has seen exponential growth in its technology development and product utilization. Our daily routine has slowly shifted from face-to-face communication to virtual interaction via the Internet, supported by 3G and 4G technology.

However, there are inherent and existing network related problems such as lack of spectrum, high energy consumption, and intercell interference. These limitations have led to the development of the fifth-generation technology (5G) that takes mobile connectivity to a whole new level. This improvement brings enhanced upgrade in terms of speed, latency, and reliability. One of the greatest beneficiaries of low latency and high-speed networks is improved services in the healthcare and social care industry.

However, the leap of 5G on bandwidth, devices, coverage, and density can pose serious cyber threat to industries. Furthermore, security has always been an afterthought for new technologies. This article will delve into how this next-generation technology will alter the cyber threat landscape, forensic incident response and cybersecurity.

This article will first examine how Internet-of-Things (IoT) devices pose major threats in current and future network technology. We will then address how new technologies, such as network slicing and Artificial Intelligence (AI), can assist the cybersecurity field. Network slicing can help share resources amongst several different needs on a network. AI can assist cybersecurity experts in identifying bad network traffic on a connection, faster than before. Last but not least, recommendations on key areas for improvement and further research in 5G technology will be presented.

Evolution of Mobile Communication Technology

Telecommunication network has played a critical role in altering evolution of civilization and technology. Figure 1 illustrates the progress of mobile communication technology towards the current 5G network stage. The mobile communication system experienced significant technical leap every decade, while mobile communication services progress in cycles of approximately 20 years.

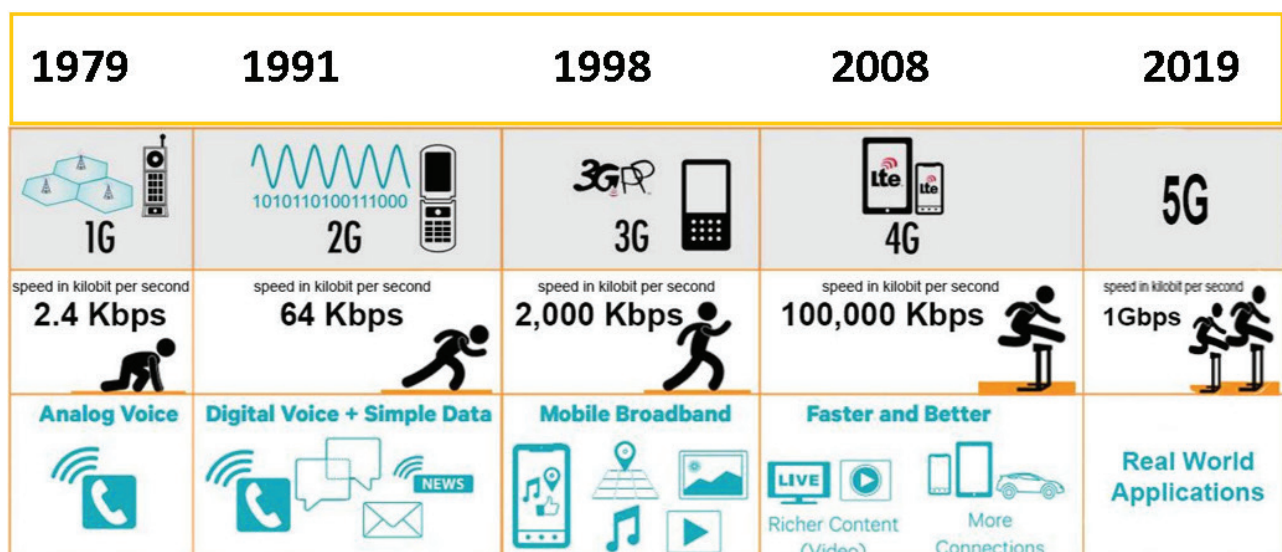


Figure 1: The Evolution of Mobile Communication Technology towards 5G Networks [1]

Since Nippon Telegraph and Telephone Public Corporation (NTT) launched the world's first cellular mobile communications service back in December 1979, known as First-generation (1G) technology, mobile communications technology has continued to grow at every decade and has evolved into new generation systems. From the first generation (1G) to the second generation (2G), voice calls were the main means of communication, while small bits of e-mail transmission was possible. However, when technology reached the third generation (3G), data communications such as "i-mode" and multimedia information such as photos, music, and video could be transmitted using mobile devices. By the fourth generation (4G) stage, high-speed communication technology exceeding 100,000 Kbps using the Long-Term Evolution (LTE) have emerged along a wide variety of multimedia communication services, thus driving the proliferation of smartphones.

By early 2019, South Korea became the first nation to introduce 5G technology. 5G is reportedly as being 100 times faster than the top speeds under 4G technology (Halpern, 2019). This technology holds great promises in unleashing groundbreaking digital services that will benefit consumers and industries over the next decade. The "Third Wave" initiated by 5G is expected to gain traction and expand through 5G evolution.

The new generation wireless technology will not only bring forth a change in speeds but also network architecture. Key attributes such as system performance, enhanced network services and operational efficiency form the basis why 5G networks were designed and developed [2]. As a result of changes in network architecture, cyber security risks will also increase.

Cyber threat in 5G

The superior connectivity enabled by 5G is poised to transform every industry from banking to healthcare. Mission critical networks powered by 5G could provide future services that connects humans and machines through highly efficient, ultra-low latency and broadband infrastructure [3]. 5G offers innovative possibilities in healthcare innovation such as remote surgeries, telemedicine and even remote vital sign monitoring that could save lives.

Are critical infrastructure industries such as energy and healthcare industries prepared to deal with the impact of cyber threats as a result

of 5G deployments? Are they able to protect their mobile networks and business operation? Do these industries have adequate security reference documents ready to help detect and prevent cyber-attacks? These are among the questions that need to be answered by organizations which are utilizing 5G networks.

In spite of advancements in 5G technology, security remains an afterthought for many. Cyber threats pose significant risks to businesses and industries that merely emphasize bandwidth, devices, coverage, and density without preparing themselves with 5G-specific security policies and user guidelines. Major security challenges related to 5G is privacy and personal data. Millions of user device information are collected by application developers around the world, which opens the opportunity for threat actors to try and steal users' private data. Geolocation information also present additional risks to device users as cyber criminals could detect the whereabouts of their victims.

5G will also boost technology in forensic incident response and cybersecurity. AI integration into system defenses such as IDS is one such technology that will flourish in 5G networks. A study by Lorenzo Fernandez Maimo et al., showed that AI integration with an IDS could increase the speed at which data is processed [4]. However, Aarti Bokar of IBM argued that AI which is programmed to make biased decisions can also make mistakes. These lapses could occur during coding while the data is being fed to the AI for processing [5]. There will be massive amounts of data in 5G networks, thus making it impossible for human experts to perform real-time detection. Further research into how to narrow these biases that current AI systems have can help to improve decision making when dealing with threats.

At present, 'Internet of Things' (IoT) devices are already vulnerable to cyber threats and they will continue remain so, even in the 5G era. Its limited built-in control mechanism makes it very difficult to give these devices proper security protocols to protect against external threats. IBM is expecting the number of IoT devices to reach close to 50 billion worldwide by the year 2020. The vast number of IoT devices entering the market over the next few years may pose a new threat in cyber security. Modern IoT malware and attacks, such as botnet scanning, would drain the CPU and memory of the IoT devices during an attack, causing substantial service response delay for time-sensitive applications, lower device stability and increase device reboot risks. This directly impacts availability of

legitimate services that are running on the IoT devices.

Malicious programs could run extraneous processes on a battery powered IoT device in order to drain battery capability, thereby shortening life expectancy of the device. For example, a simple malicious program that alters the sleeping cycles of battery powered cellular IoT devices dramatically depletes the battery power of such devices. Botnets are worrisome as its denial of service (DoS) attacks do not only affect their intended targets, but also impact the overall network services availability. Such was the case of Mirai malware which gained notoriety in 2016 [6]. It used massive denial of service attacks and caused several costly network outages. Botnets are also getting increasingly automated and sophisticated. These botnets have been targeting a broad array of IoT devices such as wireless cameras, CCTV, routers, and digital video recorders until late 2019. New variants have since emerged since March 2020 that were found to target Zyxel network-attached storage devices.

Although the above examples on cyber threats and attacks are prevalent in 4G networks, critical industries planning to adopt 5G networks must be prepared to deal with a larger scale of cyber threats and attacks as businesses and industries start to utilize IoT and ultra-reliable low-latency IoT extensively.

The benefits of 5G technology in cybersecurity and incident response

The future of cybersecurity within 5G network is not bleak. There are benefits in the next-generation technology for cybersecurity and digital forensic incident response (DFIR).

New 5G network architecture can generate new security protocols on user privacy, identity management, and threat detection. Threat detection will also benefit from artificial intelligence (AI). AI will strengthen threat detection as the increase in 5G networks speed would enable faster processing of vital information on abnormalities of human user and prevent an attack from occurring. This will especially be useful when dealing with remote networks inside a larger company. The increased speed will allow AI to receive the data more quickly, process it and report any anomalies [7] to the security management.

Another benefit that 5G will enable in future cybersecurity endeavor is Network Slicing. The concept of network slicing is to allow several virtual networks to run on a single physical network infrastructure. This enables businesses with differing needs such as maintaining a highly reliable server yet requiring low latency and high speed, to work off a single network [8]. Network slicing can be very beneficial for collecting data for forensic cases. This characteristic of 5G can help ensure the integrity of data being copied as evidence and increase the speed at which it is being collected [9]. Network slicing helps to enhance overall network architecture capabilities as the logical network components are separated from the physical network resources.

Conclusion and Recommendation

5G technology will be a quantum leap over its predecessors but like any other new technology, it presents new challenges. In particular, 5G is set to drastically alter the threat landscape.

The number of IoT devices is expected to grow exponentially throughout the world with the introduction of 5G [7]. Unfortunately, the surge in devices will also give rise to more vulnerabilities and this makes it harder for cyber-attacks to be prevented. Additionally, there are concerns on how IoT devices will adapt to network slicing, a major facet of 5G networks[9]. This lack of adaptation to a 5G feature which was supposed to improve performance can leave IoT devices more vulnerable.

IoT devices will continue to be a concern and securing these devices should be made a top priority for cybersecurity experts. Lack in hardware power and security measures will prevent them from counter attacks, thus leaving vulnerabilities in networks for attackers to exploit [10]. IoT devices should be standardized in terms of hardware and software to make security and forensics simpler. The security protocols and encryption on IoT devices need to be as hardened as possible as they remain the main target for attack.

One recommendation is for the cybersecurity community to continue investing resources to prevent known major attacks. Keeping these attacks from infiltrating 5G can help slow down attackers until a new attack method is developed. Researching methods of preventing these attacks or forensically tracing them back

to their origin and sharing this information to all organizations can be helpful. Solidifying against these known attacks will ensure a stable start to 5G until newer attacks discovered, and then the focus can shift to those attacks.

Another recommendation is to continue investing resources in crowdsourcing programs and encouraging the cybersecurity community to be more open about sharing their experiences in dealing with cyber-attacks. Crowdsourcing programs like MISIP are open forums to discuss and deliberate on cyber-attack trends which can be very beneficial for defense and forensic purposes [9]. Although employees may hesitate to reveal confidential information about their company or organization, perhaps we need to find an alternative to overcome that. If the cybersecurity community could be more open about sharing cyber-attack details, it may help beef up security for the 5G networks.

References

1. M. Irfan Baba, N. Nafees, I. Manzoor, K. A. Naik, and S. Ahmed, "Evolution of Mobile Wireless Communication Systems from 1G to 5G : A Comparative Analysis," *NCRACIT) Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.* © 2018 *IJSRCSEIT*, vol. 1, no. 4, pp. 1-08, 2018.
2. M. A. Sotelo Monge, J. Maestre Vidal, and L. J. García Villalba, "Reasoning and Knowledge Acquisition Framework for 5G Network Analytics," *Sensors (Basel)*, vol. 17, no. 10, 2017.
3. M. Condoluci, F. Sardis, and T. Mahmoodi, "Softwarization and virtualization in 5G networks for smart cities," *Lect. Notes Inst. Comput. Sci. Soc. Telecommun. Eng. LNICST*, vol. 169, no. October, pp. 179-186, 2016.
4. L. Fernandez Maimo, A. L. Perales Gomez, F. J. Garcia Clemente, M. Gil Perez, and G. Martinez Perez, "A Self-Adaptive Deep Learning-Based System for Anomaly Detection in 5G Networks," *IEEE Access*, vol. 6, pp. 7700-7712, 2018.
5. S. R. Choudhury and B. Lim, "A.I. has a bias problem and that can be a big challenge in cybersecurity," 2019. [Online]. Available: <https://www.cnbc.com/2019/07/17/ai-has-a-bias-problem-that-can-be-a-big-challenge-in-cybersecurity.html>. [Accessed: 18-May-2020].
6. M. Antonakakis et al., "Understanding the Mirai Botnet," *Proc. 26th USENIX Secur. Symp.*, pp. 1093-1110, 2017.
7. CPO, "5G and the Future of Cybersecurity," 2019. [Online]. Available: <https://www.cpomagazine.com/cyber-security/5g-and-the-future-of-cybersecurity/>. [Accessed: 18-May-2020].
8. S. Zhang, "An Overview of Network Slicing for 5G," *IEEE Wirel. Commun.*, vol. 26, no. 3, pp. 111-117, 2019.
9. A. Nieto, "An Overview of Proactive Forensic Solutions and its Applicability to 5G," *IEEE 5G World Forum, 5GWF 2018 - Conf. Proc.*, pp. 191-196, 2018.
10. J. Pan and Z. Yang, "Cybersecurity challenges and opportunities in the new 'edge computing + iot' world," *SDN-NFVSec 2018 - Proc. 2018 ACM Int. Work. Secur. Softw. Defin. Networks Netw. Funct. Virtualization, Co-located with CODASPY 2018*, vol. 2018-Janua, no. February, pp. 29-32, 2018.

Cryptocurrencies & Cybercrime

By | Sarah Khadijah binti Taylor, Mohd Sharizuan bin Mohd Omar, Muhammad Nooraiman bin Noorashid & Muhammad Faridzul bin Sukarni

What is cryptocurrency?

Many people have heard about Bitcoin, but did you know that Bitcoin is a type of cryptocurrency? Monero, Litecoin and Ripple are also different types of cryptocurrency, which have increasingly gained popularity among users.

So what is cryptocurrency? It is a digital token that allows user to transfer money without having to use banks. It was first introduced by Satoshi Nakamoto in 2009 with Bitcoin as the first cryptocurrency in the world. A statistic tracked by Coin Market Cap shows that Bitcoin, the most popular cryptocurrency to date, has reached to \$200 billion of market cap in just a short of time span[1]. This means that cryptocurrency has been generally accepted and trusted by global financial users.

How does it works?

To conduct a bitcoin transaction, user first need to install crypto wallet in his digital device such as smartphone or laptop. This crypto wallet is available as an apps which can easily be downloaded from wallet providers available online. Once a wallet is installed, user can now buy bitcoins using fiat currency from digital exchanges such as coinbase.com and bitcoin.org.

For example, John would like to send 1 bitcoin to Sally. First John and Sally both need to have a crypto wallet. To transfer his bitcoin to Sally, John needs to have Sally's wallet's public address. Next, he will transfer the bitcoin by using the apps that he downloaded.

The transaction will be posted online as a 'block', and this block will be broadcast to every participating party in the network. Those in the network will then approve the transaction, and then the block will be added to the blockchain. Next, Sally will then receive the bitcoin.

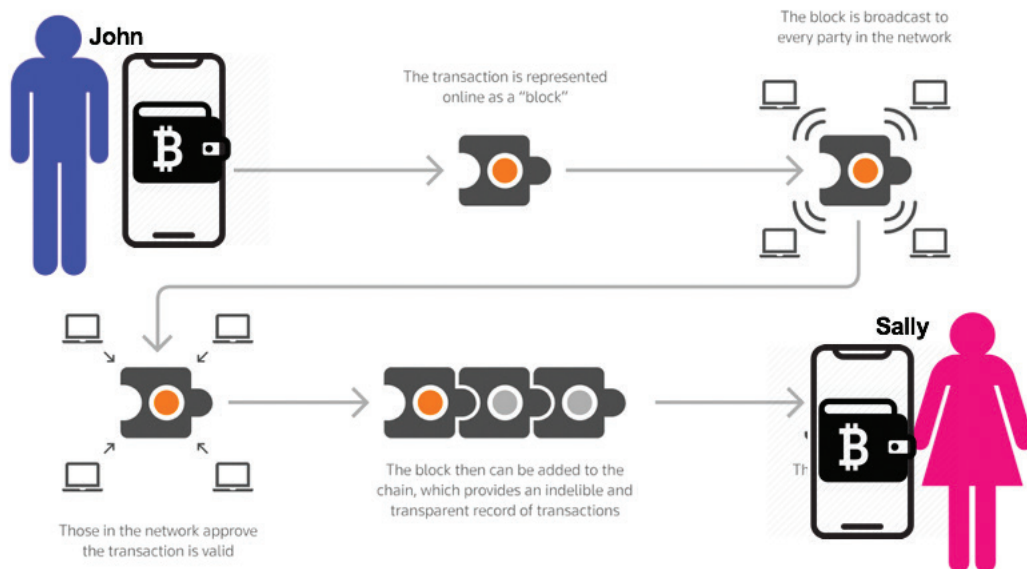


Figure 1. Process of transferring a cryptocurrency from one person to another

All transactions are recorded in a so-called online ledger, or better known as blockchain. Traditional financial system tracks transactions in a ledger which is held by banks. The blockchain, on the other hand, has no central authority. Instead it uses peer-to-peer computers to store the ledger. These peer-to-peer computers can be any device such as computers or smartphones that is connected to a particular cryptocurrency network.

Technically, cryptocurrency combines peer-to-peer network, cryptography and gaming theory to operate. It uses peer-to-peer network to transfer the digital token (namely Bitcoin). Cryptography is used to secure the transactions from sender to receiver. Gaming theory, or better known as consensus mechanism, is used to validate the transactions. For example, in Proof-of-Work consensus mechanism, the peers on the network will compete with each other to validate a transaction and compete to create a new block by solving a mathematical puzzle. A reward in form of cryptocurrency is given to the winner. These peers are known as miner by the cryptocurrency community.

Why cryptocurrency?

There are many reasons users find it attractive to use a cryptocurrency. The following points help to explain the reasons:

1. Anonymity to its user

To send and receive a Bitcoin, a user does not have to give his real identity, instead he can use his pseudo name. This pseudo name is represented by strings of characters or a QR code, as shown in Figure 1 below. This means that transactions cannot be tracked to anybody, unlike traditional banks.

2. No authority or intermediaries

The traditional financial system relies on banks and central authorities monitoring all transactions. With cryptocurrency, the transactions do not go through a central authority or intermediaries. Cryptocurrency utilizes peer-to-peer network and cryptography to secure and validate each transaction made by user.

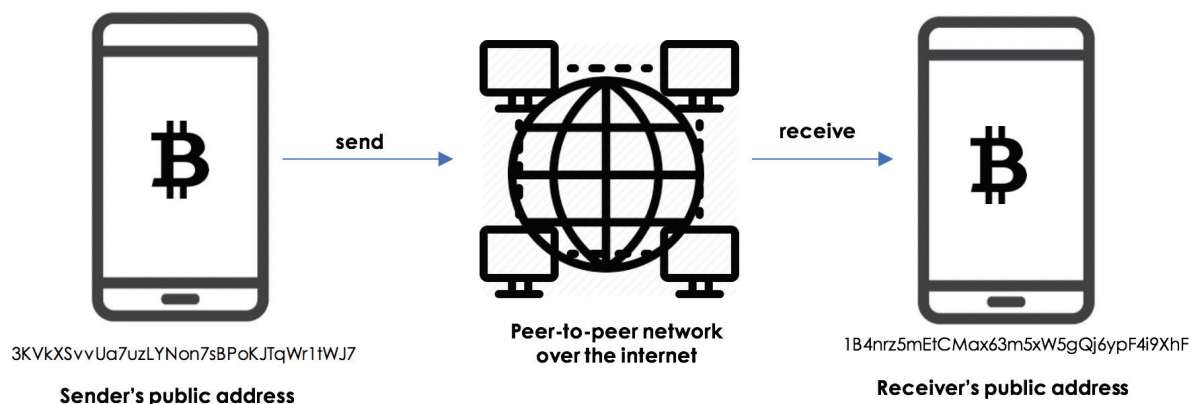


Figure 2. Cryptocurrency transaction model

3. A transparent and immutable transaction

All transaction records are posted on the so-called online ledger. This ledger, or technically known as blockchain, is published online and everybody can view it anytime, anywhere. Transaction of bitcoin, for example, can be viewed at www.blockchain.com, as shown in Figure 2. This provides a transparent transaction, where anyone can see and verify each of his transaction. These transactions are immutable - meaning it cannot be modified or withdrawn once the transaction is recorded in the ledger.

4. Providing alternative for individual underserved by banks

In fact, cryptocurrency provides a viable financial solution for individuals underserved by banks. People living in rural areas are now able to participate in the digital economy by using cryptocurrency. High value of transactions can also be transferred cross border with ease, a feature which is limited by the banks.

BLOCKCHAIN				
Products Data Explorer				
Login Sign Up				
Blocks	Hash	Time	Amount (BTC)	Amount (USD)
Transactions	53413ec53d2b00066f417829bb9b5b55e7ff664781068143c74aea9446d27...	18:02 PM	0.11934488 BTC	\$1,282.51
Average Fee	ef5b20ebe621338623b633aa4fba390c3ecf916534871377149cb98b8cf5ee...	18:02 PM	38.67843891 BTC	\$415,647.79
Average Value	50e76144c1493ff1b6d5dbe7703ac1414c4bc851014e170e542c779c093c68...	18:02 PM	0.04800214 BTC	\$515.84
Difficulty	9e629fca0e46b5b4b9229febbdabff3f535c22a0ff47a60d3fc4b51ed56ebd3e	18:02 PM	1.02457569 BTC	\$11,010.34
Hashrate	711b1db8d2d2f422dad9bab175dae55a213d675ac8a1c5bd3c955c6ae33898...	18:02 PM	54.75575200 BTC	\$588,418.45
Mempool	d8094bbda0e9d61aed0db7c02274b72c7410db44228145c2338742381331...	18:02 PM	0.29724060 BTC	\$3,194.22
Price	6cf242c8c74fac1e0d398d37f218c04214ef444656528bcfdc81a5d0055d9775	18:02 PM	0.01285796 BTC	\$138.17
Tx per day	1671432a45e8240ef1bd2291dd71f949b30776b41dca3018eb84a07e9549da...	18:02 PM	0.00009838 BTC	\$1.06
Unconfirmed	5aa911081382177abc48482c0d9bef291d367c0daa59bd65ce2ce8691aa5ce...	18:02 PM	0.17380892 BTC	\$1,867.79

Figure 3. Bitcoin transactions that can be viewed at www.blockchain.com

Cryptocurrency and Cyber Criminals

The rise of the cryptocurrencies has inevitably led to the growth of cybercrimes. The anonymous nature of these transactions has opened up a new venue for cybercriminals to leave no trace of any money trail. Cybercrimes connected to cryptocurrency occurs at worldwide scale. The high currency value loss, which has reached billions of dollars, puzzles everyone, including the cyber forensics investigators.

According to news reports, crime cases related to cryptocurrencies are happening around the world. In Thailand, for example, a 48-year old man has been arrested for cryptocurrency exchange fraud amounting to US\$16.32 million[2]. In South Korea, local authority claimed that North Korean hackers had stolen US\$2 billion worth in cryptocurrencies to fund its weapon development program[3]. Meanwhile in Japan, cybercriminals have stolen US\$32 million in a case related to Tokyo cryptocurrency exchange[4]. In United Kingdom, British investors lost US\$34.38 million to cryptocurrency scams in 2018[5]. Singapore, another country that actively supports the use of cryptocurrency, has seen its exchange Bittrue being hacked for US\$4.2 million in user assets [6].

Polis DiRaja Malaysia (PDRM) have reported that loss to cryptocurrencies cases in 2018 alone have amounting to USD55.25 million, and this figure have increased since then. This figure is quite surprising and thus, reflects the popular usage of cryptocurrencies among Malaysians.

While cryptocurrencies such as bitcoin highlights innovativeness in payment systems, the entire ecosystem has been a frequent target

of financially motivated criminals. Nevertheless Malaysian regulatory such as Securities Commission has taken steps to counter measure the criminal activity by providing guidelines and awareness to the public. Latest news, under the Securities Commission Order, all digital assets exchanges (including those who offer Bitcoin) must be registered under the commission. This is to ensure that customers' right are protected and governed under the Malaysia jurisdiction.

Conclusion

Some industry analysts predict that cryptocurrencies will eventually replace fiat currency in the near future. It has been recognized as legal currency by many developed countries such as South Korea, USA and Japan. But despite all its glory, many cybercriminals have manipulated this technology to their own benefit. Total reported loss of cryptocurrencies has reached billions (in US\$). Hence cyber forensics investigators around the world need to level up their skill, tools and guidelines to combat this incoming high-tech crime.

Acknowledgement

Authors would like to acknowledge Nur Syahirah Azhar and Khairunnajihah Suhud, attachment students from Universiti Teknologi MARA (UiTM) for their contributions in this article.

References

1. *Top 100 Cryptocurrencies by Market Capitalization*, CoinMarketCap. [Online] Available: <https://coinmarketcap.com/>; accessed 27-June- 2019.
2. *'Cryptocurrency Wizard' was arrested in B500million fraud case*, The Bangkok Post. [Online] Available: <https://www.bangkokpost.com/thailand/general/1743409/cryptocurrency-wizard-arrested-in-b500m-fraud-case>; Sept 2019.
3. *North Korean hackers reportedly stole \$2 billion from banks and cryptocurrencies to build Kim Jong Un's nuclear weapons*, Business Insider. [Online] Available: <https://www.businessinsider.my/north-korean-hackers-stole-2-billion-to-fund-weapons-program-2019-8/?r=US&IR=T>; Aug 2019.
4. *Hackers snatch \$32m from Japan cryptocurrency exchange Bitpoint*, Asia Nikkei. [Online] Available: <https://asia.nikkei.com/Spotlight/Bitcoin-evolution/Hackers-snatch-32m-from-Japan-cryptocurrency-exchange-Bitpoint>; July 2019.
5. *Bullish Brits lost \$34M to cryptocurrency scams last year*, The Next Web. [Online] Available: <https://thenextweb.com/hardfork/2019/05/21/uk-cryptocurrency-scams-34m/>; May 2019.
6. *Singapore Exchange Bittrue Hacked for Over \$4 Million in Crypto*, Coindesk. [Online] Available: <https://www.coindesk.com/singapore-exchange-bittrue-hacked-for-over-4-million-in-crypto>; June 2019.

Forensics Face Recognition Technology – The Challenges

By | Nazri bin Ahmad Zamani, Nur Afifah binti Mohd Saupi, Yasmin binti Jeffry, Muhamad Zuhairi bin Abdullah & Mohammad Hazim bin Zahri

Introduction

Face Recognition Technology (FRT) is an essential forensic tool that attest the identity of a person in a recorded video or photo at the time of a crime. The system is useful to verify if the person in the video is the suspect investigated, especially when no other witnesses could be found, or the witnesses accounts are not sufficiently strong. In the current wave of Deep Learning, FRT is becoming more accurate and robust against many factors concerning poor video quality.

There are still a lot of public misconceptions about the usage of Face Recognition Technology (FRT) in crime investigation and litigations. First and foremost, FRT is not a flawless solution. All algorithms used for matching comes with their own precision tolerance and margin of error. Therefore, there are possibilities that a match could be False Positive or *False Negative* instead of *True Positive* or *True Negative*. This leads to inconclusive matching results. Such ambiguity has yet to be resolved for almost three decades and is still being debated till today, especially in forensics application of FRT. Addressing this flaw require more than just enhancing matching algorithms. In fact, the overall solution requires a much more holistic approach. As such, the issues faced by forensics FRT need to be studied more closely.

The Forensics Frt Issues

One of the most common issues with highly inconclusive matching results in forensics FRT has to do with the quality of video evidence. The source of a video evidence can be any digital device such as CCTV recorder, a digital camera, or a smart phone.

CCTV is used to perform surveillance recordings, and it is one of the most common digital devices that provide digital evidence for the purpose of forensic analysis. However, the quality of these CCTV recordings are often poor due to several

factors, such as environment, type of camera, configuration and position of the camera. Last but not least, common issues of face attributes (pose, orientation, occlusions, and age) also come into play. Figure 1 shows the video quality factors.

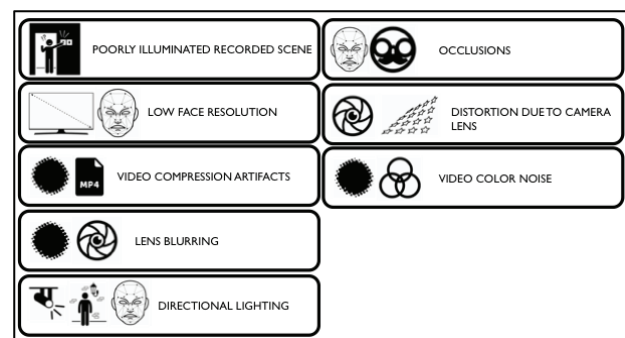


Figure 1. The factors that contributes to the inconclusiveness matching of the FRT

These are the common factors that the Digital Forensics Department of CyberSecurity Malaysia observed in many cases concerning video evidence. These factors contribute to many inconclusive matchings in the face identification analysis.

Poorly Illuminated Recorded Scene

Poorly illuminated recorded scene is one of the major issues that affects face identification precision. In this case, the face of a person of interest was recorded in a dark setting within a space and inside the camera's FOV (Field of View). This issue could be coupled with directional lighting and blurring, in which case, made the results even worse.

Directional lighting/illumination

Directional lighting on a face creates two conditions – the *shadow* and the *albedo*. The fusion of these two will further create more conditions – the *umbra* and *penumbra*. The umbra refers to the total blackness of the shadow and the latter refers to the state that is

in between of the two extremes. Extreme forms of shadows and albedos impact forensics FRT as both conditions attenuate the complexion quality of face features. Bad face features quality will consequently affect the accuracy of FRT. Although the latest Deep Learning approach to FRT seems promising, it is still ineffective if the dataset utilizes for training does not include directional illumination as part of data augmentation strategy. Figure 2 shows the effect of directional lighting on a face.

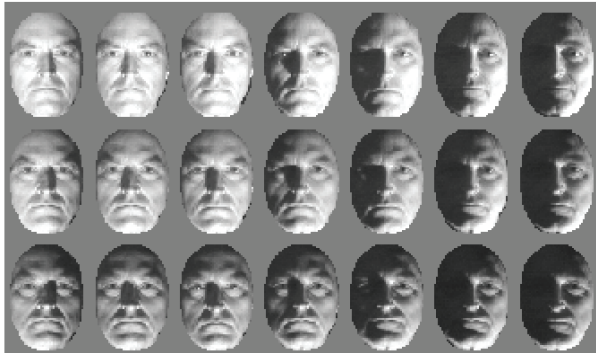


Figure 2. The effect of directional lighting on a face

Low Face Resolution

The face resolution inside a video evidence will determine whether the use of FRT is suitable. As a rule of thumb, face resolution that is lower than 100x100 pixel should be rejected in any forensics lab SoP decision tree. More attention must be given to the video that is coming from CCTV DVR as optical noises and video compression artifacts from this kind of machine could be difficult to deal with. Exception should be given if the quality of the face features within this condition are good; then resizing algorithms especially AI based Super-Resolution is highly recommended as enhancement.

Video Compression Artifacts

Video compression is a double-edge sword especially for a surveillance video. Video compression enables videos recorded to be space-sufficiently stored and play-backed if required. But while compression addresses the limited storage space inside the hard drive, the quality of the video stored is compromised. The setting has distorted the quality of a video stored to a level where the facial features in the video can hardly be identified.



Figure 3. The reality of video compression effect on face information inside a surveillance video evidence

As shown in Figure 3, the face information inside a surveillance video evidence is layered with compression artifact, (in which it appeared blockish and segmented). Furthermore, the color accuracy of the face is also compromised due to the setting. This compromises FRT accuracy in identification.

Video Color Noise

Video color noise is correlated to video compression. As mentioned, the problem stems from the video compression configurations of a DVR. Figure 4 demonstrates such flaw.

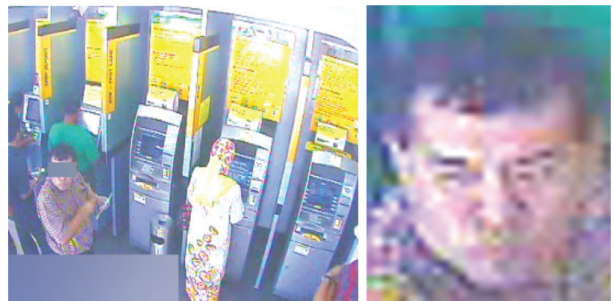


Figure 4. The colour noise plus compression artefact observed in a video evidence

Lens Blurring

Lens blurring could occur due to the camera configuration. The blurring can compromise face information quality especially if the video comes from the CCTV surveillance system. For other video recording system which provide better imaging solutions, blurring can easily be fixed via image processing.

Distortion Due to Camera Lens

Lens distortion is another common observed quality issue in any video or imaging system. Lens distortion causes a geometrical damage to

face features. The distortion can be mitigated via image processing technique. The problem with this approach is that it requires a forensic analyst to set distortion parameters. For an analyst to configure the parameter based on his or her judgement of what the original state of the face is somewhat arbitrary. Therefore, to use a badly distorted face during acquisition for forensic FRT is not strongly recommended.

Occlusions

Occlusions (for example beard, face tattoo, eye-glasses, hats, hijab, etc.) is another common problem faced by any FRT. This form of issue is irreversible by any means of imaging or AI method. Most samples with occlusions are rejected for FRT unless it is being used for other analysis such as object matching.

The Effects On Frt Performance

The effects of the aforementioned issues on a forensics FRT can be varied. As written by Shroff in his paper title, "Facenet: A unified embedding for face recognition and clustering.", the effect of JPEG quality vs accuracy rate is clear. He found out that better quality JPEGs produced higher accuracy results on its FaceNet system performance. As shown in Figure 5, the left table shows the effect on the validation rate with varying JPEG quality. The right table shows how the image size in pixels affect the validation rate.

jpeg q	val-rate	#pixels	val-rate
10	67.3%	1,600	37.8%
20	81.4%	6,400	79.5%
30	83.9%	14,400	84.5%
50	85.5%	25,600	85.7%
70	86.1%	65,536	86.4%
90	86.5%		

Figure 5. The effects of compression and face image resolution on FaceNet accuracy.

FaceNet is a FRT open-source powered with Deep Learning method. The system has been tested on thousands of individuals' face images. Many of the test results presented in this paper are consistent with real-life experience in forensics FRT. The performance drop is observed in deteriorating quality whether it is due to image resolution, video or image compression related issues, camera issues or occlusions. According

to Schroff and Maëlig [2] the solution to the problems is to add such conditions to the training set. This strategy should be taken into the new FRT enrolment procedures, where the issues are included as part of data augmentation effort instead of being ignored.

Conclusion

Each FRT method has its own limitation and breaking points in stress tests. The best approach to improve forensics FRT is to include qualitative factors into the data augmentation strategy of the face training data.

References

1. Schroff F, Kalenichenko D, Philbin J. Facenet: A unified embedding for face recognition and clustering. In *Proceedings of the IEEE conference on computer vision and pattern recognition 2015* (pp. 815-823).
2. Maëlig Jacquet, Christophe Champod, *Automated face recognition in forensic science: Review and perspectives, Forensic Science International, Volume 307, 2020.*

Deploying An Open Source Video Analytics In Cctv For Forensic Readiness

By | Mohammad Zaharudin bin Ahmad Darus, Nur Afifah binti Mohd Saupi, Muhamad Zuhairi bin Abdullah, Muhammad Umar bin Shahbuddin & Mohd Shahrulazam bin Samsudin

Introduction

In this current era, surveillance camera such as closed-circuit television (CCTV) plays a key role in helping to defeat crimes. Almost 51% of CCTVs are used to assist crime investigation and act as the eyes of Law Enforcement Agencies (LEA) but there are flaws in the current surveillance camera's hardware and software. Today's software is limited by hardware, but it doesn't mean it's impossible to create better software to match with the current hardware. There are still ways to create software that can help solve today's issues.

More specifically, with the help of open source, everyone has the ability to create their own system. What's an open source? It is a concept of freely distributed software and universal access to an application's source code. Open source was first proposed by a group of talented people who had no political agenda or similar situations where one can monopolizes as needed.

We would like to give a brief walkthrough to those who may want to deploy CCTV equipped with video analytics by only using open source. The following are some ideologies and practices that can help guide how to build it and can be improvised. This isn't the absolute version for the present time due to lack of technology. Hardware limitation may be overcome with the software quality.

What is a Forensic Readiness and Video Analytics?

Before we delve deeper into the technical aspects, we would like to explain the definition of forensic readiness before proceeding to product creation.

Back to the question: What is Forensic Readiness? Based on the Forensic Readiness Guidelines (NICS.2011), forensic readiness is the ability to preserve, collect, protect and analyze digital evidence so that it can be a great help in legal matters. It is also defined as the ability of an

organization to maximize its potential to use digital evidence, while minimizing the cost of investigation.

In this article, we will discuss how to deploy video analytics such as face recognition from open source for CCTV application. Figure 1 below shows the main process of digital forensics which digital forensics analyst uses.



Figure 1: Digital forensics process

To the second part of the question: What is Video Analytics? Video analytics is the ability to analyze the video through the detection and determination of occurring events. This capability is supported by a wide variety of domains such as smoke detection, safety detector, retail, transport, etc. This plays a critical role as the people who monitor the camera cannot watch the live feed all the time.

Video analytics will focus on the frame which may be suspicious and will notify the owner if anything happens. Different people may have differing levels of focus or different ideas of suspicious activity. Video analytics can be used for motion detection, facial recognition, license plate reading, etc.

What is an OpenCV?



Open Source Computer Vision (OpenCV) is a library equipped with programming language and the ability to help build a programmable

software. The library is a cross-platform meaning that one platform can access or access the other platforms. OpenCV supports multiple frameworks like TensorFlow, Torch/PyTorch and Caffe.

The library is equipped with more than 2,500 optimized algorithms, including both classic and up-to-date algorithms, to ensure that the algorithms can still support future uses. By implementing this algorithm, facial detection and recognition, movement detector, human action classification, object movement, and extraction of 3D models can be produced as the result of the algorithm.

Since OpenCV holds most of the facial recognition algorithm compared to the other libraries, OpenCV-free systems are considered less comprehensive since they lack the algorithm that OpenCV provides.

More than 47,000 within the community regularly use and update the library, therefore contribute to the development of OpenCV. Not only is the library popular among communities, but the larger group of researchers and the

government are also leaning towards OpenCV usage.

Detection in Facial Recognition

There are three stages in facial recognition where it can be considered as a complete functional system that can assist in forensics investigation, which are detection, recognition and finally, tracking.

Detection of the facial recognition is the ability to detect object or subject at a distance that does not compromise its ability to discern objects. For facial recognition, the detection capability relies heavily on hardware such as the camera and the computer running the program. Based on the distance-testing test, each camera produces different results. It depends on the type of camera.

To detect an object or a subject, there must be between 5% to 15% facial features just to detect and higher features point to do identify or even verify. The following diagram shows the Open Source's classes for face/object detection

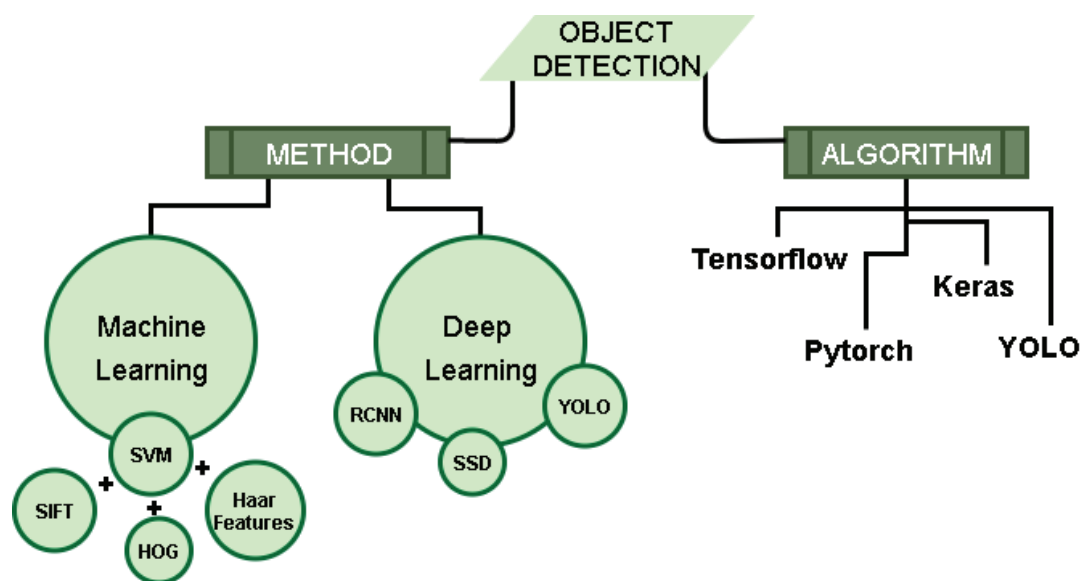


Figure 2: Open Source's classes for face/object detection

Recognition in Facial Recognition

Recognition plays a critical role in helping to identify an object or a subject because of its ability to compare the stored image and the live feed image in a short period of time. This can be considered technology within a technology where it is capable of identifying or verifying a subject on the basis of a digital image or a video.

The comparison is made by analyzing the patterns of textures and shapes of the object or the subject. In order to ensure that the system is able to identify or verify, the facial features point of recognition should be more than 25%. The higher the rating or recognition points, the higher the possibility of verification is true, and no change has been made in advance. The following diagram shows the generic flow of identifying person's face.

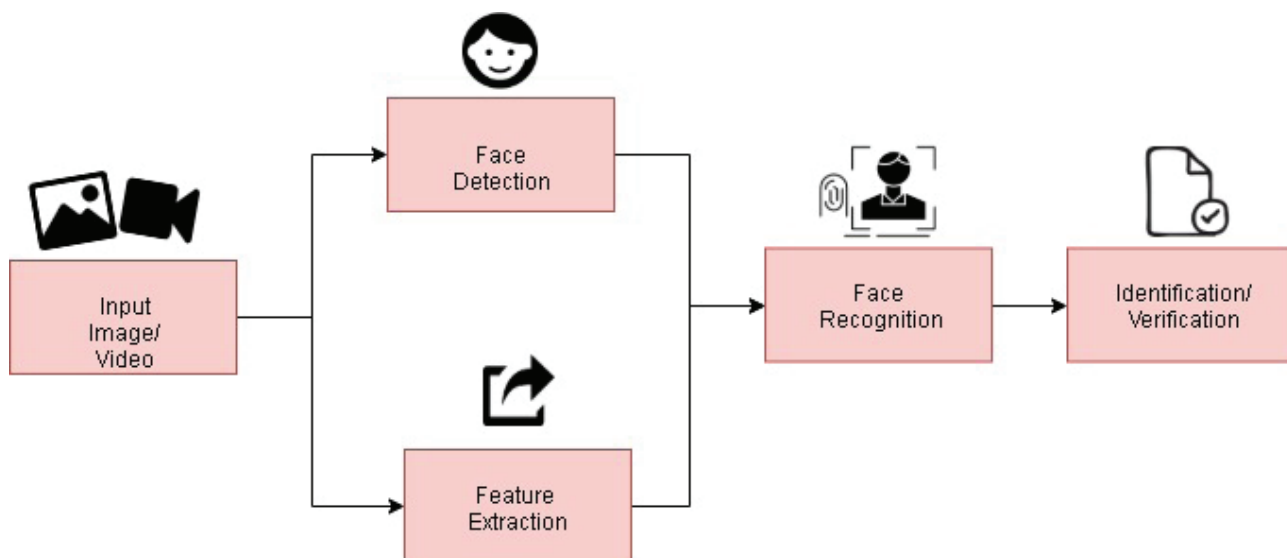


Figure 3: Generic flow of identifying person's face

Near Real-Time Object/Subject Tracking

Tracking is the last stage of facial recognition. After detection and recognition by means of video, the path or movement of the object or subject is recorded for future reference. In tracking, the previous frame is used as a referenced frame. Then, compare it to the current frame. By using Euclidean distance formula, if the distance between two objects is within the threshold, this is the same object. In special cases, tracking plays a major role, such as when a suspect fled from the crime scene, by using tracking, the system able to track down the path taken, and where the Law Enforcement Agencies (LEA) needs to search for a suspect. This can narrow down the investigation and reduce the time for the analysis.

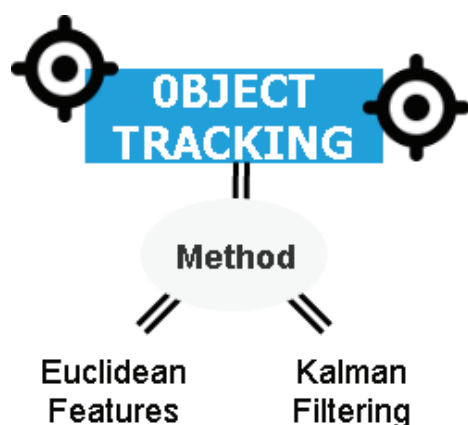


Figure 4: Method of object tracking

You Only Look Once (YOLO)

YOLO is a system for detecting objects in real time which is quite fast and precise compared to other detectors of the same type. They apply the model to an image at multiple location and scales. YOLO split the image into grid cells 13x13. Each of the cells is capable of predicting five bounding boxes. Whichever regions have high scoring are considered as being detected.

Confidence score will be executed to predict how much the bounding boxes encloses to the object the image will be divided into regions, and then the bounding boxes will be weighted to the predicted probabilities. YOLO can be a crucial help for the LEA in detecting which vehicle that the suspect may be using or what kind of stuff does the suspect leaving behind.

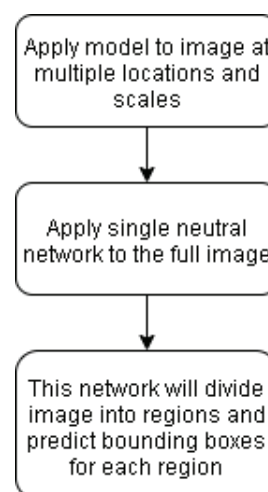


Figure 5: YOLO flow



Figure 6: Example of object detection using YOLO

Darknet

Darknet is a framework to train neural networks. It is an open source framework written in C and CUDA. It supports computation with CPU and GPU. The first repository for the YOLO training done by J.Redmon, which came up with multiple configuration files for training on different architectures.

TensorFlow

TensorFlow is an open-source software library primarily intended for dataflow as well as a math library. TensorFlow may also be used as neural networks for machine learning applications. TensorFlow has become a big hit that even Google itself uses TensorFlow to help them develop a mathematical formulation system.

TensorFlow has the capability to run multiple CPUs and GPUs with optional computational CUDA and SYCL extensions. Not only is Linux supportable, it can even be supported by MacOS, Windows, Android and iOS included. It also supports image captioning that handles quite a handful of queries and replaces them with traditional search-based algorithms.

Video Analytics in CCTV

When a crime occurs, surveillance camera or CCTV plays a crucial part when the camera manages to record evidence that is required by the LEA. The evidence can be either the main objective or a supportive evidence. The main reason on why the LEA wishes to get their hand on the evidence is to ensure that the perpetrators are brought to justice. This can be done by ensuring that the evidence is solidly based on the identification made upon them, a collection of the evidence, thoroughly analyzing all the data to ensure no data overlooked and the presentation of data is relevant to the party for the judgement. Keep in mind that low resolution or bad quality evidence may affect the entire operation and could result in a case failure.

Tracing a potential suspect from large-scale heterogeneous CCTV can be quite exhausting for the investigator and may require more resources either human, time or costs to purchase forensics software.

To overcome this, deploying video analytics such as face detection, recognition and tracking will be helpful for the forensic investigator. This will significantly reduce resources and to keep up with the definition of forensic readiness.

The Limitation

Even though installing a CCTV is helpful and all, there are few factors which must be considered. One of them is the quality of the video. The quality of the video varies depending on the camera type and model. Not all cameras are of the same quality and it may affect the necessary evidence. For example, an investigation currently tracking a suspect via CCTV will have a hard time if camera's resolution is low and the investigator needs to tackle the investigation by making assumptions and making decisions through experience.

Another limitation is surveillance camera placement. Some CCTV placement isn't that strategic which causes a loophole that the suspect can use as a gateway. It is difficult to ensure that all sides are covered due to facts that are multiple reasons that can affect the quality of the output such as the weather, time such as night and day, logical reason, budget, etc.

Summary

CCTV as an investigative tool will definitely be a thing for forensic readiness in the near future. Open source currently has the capability to provide an algorithm and library that is considered useful when developing a CCTV solution as an investigative tool. The lower the cost of creating the software, the more beneficial for the Digital Forensic Department in terms of budget and investigation costs.

Artificial intelligence (AI) or machine learning that is currently part of video analytics by comparing the patterns and traits can deduce the human intervention factor. It can easily classify suspicious human activity, abandoned object detection, face recognition, subject movement and so on.

Forensic readiness aims to maximize an organization's ability to gather and use digital evidence whilst minimizing the costs of related investigations.

References

1. Caroline Gammel and Duncan Gardham (13 October 2010). "7/7 inquest: how investigators traced the bombers after attack". *The Telegraph*. Retrieved from <https://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/8061217/77-inquest-how-investigators-traced-the-bombers-after-attack.html>
2. Intelligence and Security Committee (May 2006). "Report into the London Terrorist Attacks on 7 July 2005". BBC News.
3. Security News (18 August 2015). "Bomb toll revised: 20 dead, 125 injured". *Bangkok Post*. Retrieved from <https://www.bangkokpost.com/news/security/659848/bomb-toll-revised-20-dead-125-injured>
4. Asia News (19 August 2015). "Bangkok bomb: CCTV video shows man leave backpack". BBC News. Retrieved from <http://www.bbc.com/news/world-asia-33969621>
5. Asia News (20 August 2015). "Bangkok bomb: Thai police release CCTV timeline of suspect". BBC News. Retrieved from <http://www.bbc.com/news/world-asia-34002904>
6. Bev Ford, Greg B. Smith and Larry Mcshane (18 April 2013). "Police narrow in on two suspects in Boston Marathon bombings". *Daily News*. Retrieved from <http://www.nydailynews.com/news/national/injury-toll-rises-marathon-massacre-article-1.1319080>
7. Robert Rowlingstone. *A Ten Step Process for Forensic Readiness*. *International Journal of Digital Evidence*, 2004. <https://www.utica.edu/academic/institutes/ecii/publications/articles/A0B13342-B4E0-1F6A-156F501C49CF5F51.pdf>
8. Sarah Khadijah Taylor and Mohd Zabri Adil B Talib. *Standard Operating Procedure of Digital Evidence Collection*. *Cybersecurity Malaysia*, 2013.
9. Halil Ibrahim Bulbul, H. Guclu Yavuzcan and Mesut Ozel. *Digital Forensics: An Analytical Crime Scene Procedure Model (ACSPM)*. *Elsevier Forensic Science International* 233, 2013.
10. Bureau of Justice Assistance. *Video Evidence: A Law Enforcement Guide to Resources and Best Practices*. U.S Department of Justice, 2014.
11. Matthew P.J. Ashby. *The Value of CCTV Surveillance Cameras as an Investigative Tool: An Empirical Analysis*. *Eur J Crim Policy Res*, pages 23:441-459, 2017
12. Redmon, Joseph and Farhadi, Ali, YOLOv3, 2018, ArXiv, Retrieve from <https://pjreddie.com/darknet/yolo/>
13. Technopedia (27 August 2018) What is Facial Recognition? – Definition from Technopedia. Retrieved from <https://www.techopedia.com/definition/32071/facial-recognition>
14. What are Video Analytics? *Video Surveillance.com*. Retrieved from <https://www.videosurveillance.com/tech/video-analytics.asp>
15. About OpenCV (2019). *Opencv.org*. Retrieved from <https://opencv.org/about/>

Cyber Insurance: A Panacea To Mitigate Business Risk?

By | Nazahan bin Nazri & Mohammad Faisal bin Ismail

Cost and frequency of cyber-attacks are on the rise. In one of the biggest data breaches ever, a hacker gained access to more than 100 million Capital One customers' accounts and credit card applications. By the time, the online banking giant realized that its data had been hacked millions of credit card applications which included personal information were exposed. In 2019, Citrix company which provides VPN fell victim to a 'password spraying' attack. It was an attack where a hacker attempted to gain access to a system via brute force. In 2018 GHub was hit with a massive Denial of Service (DoS) attack which led to a blackout for about 20 minutes. As of October 2019, a total of, 9,864 cyber related crimes have been reported in Malaysia and cyber-crime economic related loss stood at USD96.7 million. A 2018 Frost & Sullivan study reveals that the potential economic loss in Malaysia due to cyber-security incidents may hits staggering USD12.2 billion. This is more than 4% of Malaysia's total GDP of USD296 billion.

Ransomware attacks, intellectual property theft, and fraud cost companies billions in recovery expenses, fines, and lost revenues every year. As a result, firms are purchasing cyber insurance to cover losses and expenses resulting from cyber incidents.

However, cyber insurance alone is not a panacea, even organisation that acquire cyber insurance may not be as protected as they think. Unlike traditional lines of business such as private auto insurance, where standardized policies provide liability or collision coverage, cyber insurance policy language is not standardized. The types of risks covered under cyber insurance differ significantly across policies and businesses, and insurers do not always agree on what loss events are covered under those policies. For instance, in the landscapes of a cyber events, which included limited loss history, the unreliability of past data when predicting future events, and the possibility of a large-scale attack are highly correlated across companies, therefore making it problematic to write comprehensive cyber insurance policies. In this article, we examine the extent to which cyber insurance can assist to safeguard businesses and the wider economy

from the costs of cyberattacks and how institutional factors and legal uncertainties may obstruct the development of this market.



What is cyber insurance?

The history of cyber insurance date back to Steven Haase, who helped AIG write the first internet security liability policy in 1997. The first cyber insurance policies were geared toward information technology companies responsible for managing networks and systems used by other businesses and consumers. However, the cyber insurance market has since grown, and current cyber protection comes in three forms: third-party written coverage, first-party written coverage, and implicit silent cyber coverage (sometimes called non affirmative cyber exposure).

Third-party liability cyber insurance reimburses said entities for the costs incurred by their clients because of data breaches, malware infections, or other cyberattacks in which the insured entity was at fault. Third-party liability coverage is the cyber equivalent of medical malpractice, where businesses are insured against harm they inflict on their clients by their action (or, as is usually the case with cyber risk, inaction). Many early policies were of this form.

In the mid-2000s, cyber insurers began offering first-party expense coverage, which expanded insurance offerings to any company that uses technology. First-party expense cyber insurance reimburses companies for the costs of a cyberattack that directly affects their business. First-party policies can be broad or very specific,

depending on the needs of the company, and may cover post-cyberattack expenses such as credit-monitoring and other data breach expenses, hiring crisis management consultants to restore brand reputation or negotiators to handle ransom payments, and data recovery costs.

Silent cyber risk is a third type of cyber insurance coverage that is not a cyber insurance policy at all, but a term that refers to potential cyber-related losses stemming from traditional property and casualty (P&C) policies not specifically designed to cover cyber risks. Consider a scenario where a hotel's computer system is infected with malware, which sets the sprinkler system off, damaging the interior and causing a patron to slip and fall. If cyber perils are not explicitly excluded, the hotel's traditional property and casualty coverage would be expected to cover the damage to the hotel caused by the sprinklers and the medical bills of the injured patron. Silent cyber is steadily becoming less of a risk for insurers as they transition to P&C policies that either explicitly exclude or include losses caused by cyberattacks.

For example, by January 2020, AIG finalized their transition to affirmative cyber coverage across their commercial insurance lines, effectively eliminating most silent cyber risks to their business, while removing the implicit cyber-risk coverage from their existing customers.

Cyber insurance is a rapidly growing business, but it is still a relatively small part of the overall global. P&C insurance market. Today global businesses can get cyber insurance either as a standalone policy or as part of their general P&C coverage in a packaged policy. Standalone and packaged policies, respectively, accounted for USD1.1 billion and USD922 million in 2018 premiums. While the amount of written cyber insurance premiums has more than doubled since 2015, the cyber insurance market is still small, accounting for less than 0.5% of all U.S. P&C business.

Cyber insurance adoption rates vary significantly across firms and industries. About 58% of large businesses have a standalone cyber insurance policy, compared with just 21% of small businesses. Industries with the highest adoption rates were education (66%) and healthcare (62%); technology and communications firms had a 51% adoption rate. Industries with lower adoption rates included financial institutions (27%), manufacturing (30%), retail (39%), and utilities (41%).

Challenges of writing cyber insurance

As the cyber market has matured, insurers have refined how these policies are underwritten and priced. However, there are fundamental aspects of cyber insurance that make it difficult for insurers to write and price policies that cover a broad swath of risks. Let's discuss some of these challenges below.

There is only a limited loss history for insurers to use when setting prices for cyber insurance premiums and coverage loss limits. As such, this introduces risk. When insurers set auto insurance premiums, for example, they can rely on a long history of accidents and damages to model the probability that a driver with a specific set of characteristics will get in an accident and then set premiums to cover this expected loss. Cyber insurers, working in a fast-developing market, instead rely on a number of indirect factors to try to price policies appropriately, including market estimates of the cost of cyberattacks, questionnaires to determine the riskiness of the insured, their own (often limited) underwriting experience, and pricing by other insurance companies.

Current cyber protection comes in three forms: third-party written coverage, first-party written coverage, and implicit silent cyber coverage.

Pricing a new insurance product carries risks: For example, Mohey-Deen and Rosen (2018) explore how under-pricing of another, then new, line of business, long-term care insurance, contributed to the insolvency of Penn Treaty. Penn Treaty used overly optimistic financial assumptions derived from their "experiences with other products," and when those assumptions turned out to be wrong, the company became "the second largest insolvency in insurance guaranty fund history."

Cyber threats are continuously evolving as both private and state-sponsored hackers develop new methods to infiltrate networks. The rapid evolution of hacking capabilities and strategies makes it difficult for insurers, which rely on clients having relatively consistent risk profiles, to assess the true risk of a potential client being hacked. The increased sophistication of hackers is evident, in that both the frequency and costs of cyberattacks have risen in recent years. In U.S. the reported cost of the average cyber-attack rose up 29% from USD21.2 million in 2017 to USD27.2 million in 2018. Despite this, the cyber-insurance market remained profitable for underwriters.

Cyber threats are highly scalable as they can potentially hit thousands of companies simultaneously, causing large interrelated losses for insurers. Due to the design of the internet, there are highly important central nodes. This type of network centralization creates two problems for cyber insurers. One type of problem would occur if an important service, such as a large cloud computing platform used by many policyholders, went down. The insurer may then have to pay claims on all of its policyholders at once. A similar dynamic can be seen in natural disasters, where private insurers are often reluctant to offer flood insurance, because if a single house in a neighbourhood was hit by a flood, it is likely that many houses around it were also hit at the same time. For example, in the 1920s, following series of catastrophic floods along the Mississippi River, private insurers began explicitly excluding flood coverage from their home insurance policies, eventually resulting in the creation of the National Flood Insurance Program (NFIP) to fill the gap.

The type of problem cyber insurance faces is the possibility of cascading failures caused by a cyberattack. One common example of a cascading failure is an attack on a power grid, where the destruction of a piece of critical infrastructure leads to failures across the rest of the grid. Cyberattacks using self-reproducing malware can also spread across a network of computers. Such an attack occurred in 2017, when a piece of malicious Russian code dubbed NotPetya targeted Ukraine. By exploiting a vulnerability in Windows to gain control over unpatched computers, NotPetya used this access to gain passwords of other machines on the network and jumped across the globe, causing over USD10 billion in estimated damages. Such an attack could happen again, and it could be worse next time.

The difficulties in properly pricing cyber insurance products and the looming possibility of a largescale cyberattack encourage insurers to write policies that limit the amount of coverage a business can get, as well as the risks that are insured. Given the restrictive nature of some policies, some businesses may overestimate the amount of cyber coverage they need.

Cyber insurance coverage uncertainties

In July 2019, FM Global, a commercial property insurer, conducted a survey of chief financial

officers (CFOs) at companies with over USD1 billion in revenue. The survey found that 71% of the CFOs reported they believed that their insurer would cover “most or all” of the losses their company would suffer in a cyberattack. However, those same CFOs identified damages they expected to suffer in such an event that are not covered by typical cyber and property insurance policies. Almost half of CFOs said that they expected fallout from a cyberattack to include a devaluation of a firm’s brand; more than one-third said they expected increased investor scrutiny, a decline in revenue, and an introduction of regulatory compliance problems; and a quarter said they expected a decline in market share and share price. None of those costs are normally covered in cyber insurance policies.⁹

This apparent disconnect speaks to the importance of pursuing increased clarity when underwriting cyber insurance coverage, as disputes about coverage between insurers and policyholders are percolating in the legal system. Lawsuits around the country reflect current ambiguities about the nature of responsibility for cyberattacks and data breaches.

Legal uncertainty in cyber space

Adding to the uncertainties insurers face when attempting to structure policies in this new market is the relative lack of legal precedent on core issues pertaining to cyberattacks. When facing uncertainty regarding fundamental questions, insurers may decide to wait until such issues are resolved before offering policies or only write policies with restrictive coverage that are less useful to businesses.

For example, data breaches and data theft are a common source of damages from cyberattacks, yet important case law on this issue is still unresolved. Legal cases involving data breaches rest on the nature of the alleged harm: If personal data are exposed due to a cyberattack on a database, has the person whose data was exposed suffered sufficient concrete harm or does there merely need to be “substantial risk” that future harm will occur? Circuit courts are split on this issue. Several courts have found that victims of data breaches do not have standing to sue when no actual identity theft or fraud occurs, while others have found that the risk of data misuse that results from a breach confers standing. The Supreme Court has yet to directly address the issue of standing in data breach litigation. In March 2019, the Supreme

Court refused to hear an appeal from Zappos.com of a Ninth Circuit Court ruling that plaintiffs who had only alleged that financial losses were imminent also had sufficient standing to sue.

This uncertainty over standing in data breach litigation is important for cyber insurers because it directly affects the probability that an insurer will have to pay claims in the event of a data breach and this, in turn, affects how they should price their insurance policies.

Meanwhile, lawsuits that are directly concerned with cyber insurance coverage have already begun to appear. One case that has significance for the development of the cyber insurance market, between Mondelēz International (an American food company) and Zurich Insurance Group, arose over a disagreement about a common “act of war” exclusion. In June 2017, as discussed earlier, a virus called NotPetya was released into Ukrainian information technology systems. The virus quickly spread to multinational companies, including Mondelēz, leading Mondelēz alone to claim USD100 million in damages from the attack. At the time, Mondelēz had a contract with Zurich that covered “physical loss or damage to electronic data, programs or software” triggered by “the malicious introduction of a machine code or instruction.” The policy contained an exclusion for “hostile or warlike action in time of peace or war,” a common exclusion in such contracts. In February 2018, the White House called NotPetya a “reckless and indiscriminate cyberattack” on the part of the “Russian military” and “the Kremlin.” Mondelēz filed a claim for reimbursement, but Zurich denied it, claiming that the White House’s declaration qualified NotPetya as an “act of war”; Mondelēz filed suit in January 2019. If Zurich successfully argues that NotPetya qualifies as an act of war, it will establish a precedent that many of the cyberattacks that companies face are not covered by their insurance. This case illustrates that not only the nature of the crime, but also the nature of the perpetrator must be written specifically into cyber insurance policies to avoid legal conflicts.

The future of cyber insurance

Currently, the cyber insurance market only covers a small percentage of the overall losses caused by cyberattacks. Measuring the complete impact of cyberattacks on the U.S. economy is difficult. However, the White House Council of Economic Advisers developed a

model using the stock market reactions of firms that had experienced “malicious cyber activity” to estimate the cost of cyberattacks. Using this model, they found cyberattacks cost the U.S. economy between USD57 billion and USD109 billion in 2016, equivalent to 0.3% to 0.6% of GDP. During that same period, U.S. insurance companies incurred USD356 million in claims from policyholders, equivalent to less than 1% of estimated losses. Compare this to natural catastrophes, where 50% of losses between 2015 and 2018 were paid by insurers. This difference in insured losses illustrates the room for growth in the cyber insurance market. But for the cyber insurance market to bridge this gap and continue to grow, it must overcome the challenges we have discussed here.



Insurance companies are already beginning to write cyber insurance contracts that more explicitly define what is or is not covered. This trend should help limit lawsuits and disputes over cyber coverage. Court decisions must help insurers and policyholders clarify language in their contracts. However, the Mondelēz v. Zurich case provides an important litmus test for the future of cyber insurance. Alleged state-sponsored cyberattacks have grown in frequency in recent years, and some argue that these present the greatest cybersecurity threat to the U.S. economy. As long as uncertainty exists over what qualifies as an “act of war” in the context of cyber insurance, it will be difficult for insurers and policyholders to agree on contracts with all parties sharing a clear understanding of what is covered.

Even as insurers acquire additional historical data on cyber loss events, the modelling of cyber risk will continue to present challenges. At the heart of the problem of modelling cyber insurance is that yesterday’s attacks do not

necessarily inform us about tomorrow's risks. To help insurers accurately price future cyber risks, predictive cyber-risk models will have to be developed.

Finally, the cyber insurance industry needs to consider how to deal with the possibility of large loss events. Better modelling of cyberattacks should help insurers measure their accumulation of interrelated risks, and improved cybersecurity standards and practices may help businesses avoid such catastrophic attacks to begin with. Looking at the ways in which the insurance sector has provided comprehensive insurance coverage for natural catastrophes may provide a way forward for the cyber insurance market.

Summary

Cyber insurance is a small but growing market. As cyber incidents become more frequent and more detrimental, people and institutions are searching for cyber coverage that protects them from these risks. However, the cyber insurance industry faces significant challenges, including a lack of historical data, a lack of ability to predict the future of cyber risk, the possibility of large cascading loss events, uncertainties among market participants about what is specifically covered under such policies, and legal battles over fundamental issues. The future growth of the market will depend upon how these issues are resolved.

References

1. Available online, <https://www.businesswire.com/news/home/20190905005481/en/AIGFinalizingTransitionAffirmativeCyberCoverageGlobal>.
2. Data from S&P Global Market Intelligence and authors' calculations.
3. Data on large/small businesses are available online, <https://www.hiscox.com/documents/2018-Hiscox-Small-BusinessCyber-Risk-Report.pdf>. Data by industry are from Marsh PLACEMAP, available online, <https://www.marsh.com/us/insights/research/cyber-insurance-trends-report-2018.html>.
4. Sasha Romanosky, Lillian Ablon, Andreas Kuehn, and Therese Jones, 2019, "Content analysis of cyber insurance policies: How do carriers price cyber risk?," *Journal of Cybersecurity*, Vol. 5, No. 1. Crossref, <https://doi.org/10.1093/cybsec/tyz002>
5. Zain Mohey-Deen and Richard J. Rosen, 2018, "The risks of pricing new insurance products: The case of long-term care," *Chicago Fed Letter*, Federal Reserve Bank of Chicago, No. 397. Crossref, <https://doi.org/10.21033/cfl-2018-397>
6. Available online, https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf#zoom=50.
7. Alejandro Drexler, Andrew Granato, and Richard J. Rosen, 2019, "Homeowners' financial protection against natural disasters," *Chicago Fed Letter*, Federal Reserve Bank of Chicago, No. 409. Crossref, <https://doi.org/10.21033/cfl-2019-409>
8. Available online, <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>.
9. Available online, <https://newsroom.fmglobal.com/releases/cyber-insurance-may-create-false-sense-of-security-among-senior-financial-executives-at-worlds-top-companies-suggests-fm-global-survey>.
10. Cited material in this paragraph is available online, <https://www.insurancejournal.com/news/international/2019/01/11/514553.htm>.
11. Available online, <https://www.wired.com/story/white-house-russia-notpetya-attribution/>.
12. Available online, <https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf>.
13. Based on insurance statutory filings from S&P Global Market Intelligence. Data include both standalone and packaged policies, but not claims paid by surplus line insurers that are not required to report financials to the NAIC.
14. Data from Munich Re NatCatSERVICE for all North American losses.
15. Available online, <https://www.insurancejournal.com/news/international/2019/03/27/521824.htm>.

Factors Influencing Exchange Rates

By | Siti Noriah binti Nordin, Nur Nadira binti Mohamad Jafar, Wan Nur Ariffa binti Wan Abu Bakar Sidek, Shamsul Hairy bin Haron & Muhammad Faizal bin A. Rahman

Introduction

An exchange rate is the price of one country's currency expressed in another country's currency. In other words, the rate at which one currency can be exchanged for another. Exchange rate can be quoted either directly or indirectly. In a direct quotation, the price of a unit of foreign currency is expressed in terms of the domestic currency. In an indirect quotation, the price of a unit of domestic currency is expressed in terms of the foreign currency. For example, if Ringgit Malaysia (RM) is set as a domestic currency, in a direct quotation it would be as $RM1 = USD0.2289$. But in indirect quotation, it would be $USD1 = RM4.3610$.

Exchange rate is an important medium because it allows for conversion of one country's currency into that of another, thereby facilitating international trade for purchases of goods and services or transfer of funds between countries. It allows price comparison of similar goods in different countries. The price difference between similar goods is determined through the goods traded and where they are shipped or sourced. Hence, the exchange rate is a significant factor in determining the competitiveness of agricultural, manufacturing, commodity, as well as services between different countries.

Types Of Exchange Rate Systems

There are three ways the price of a currency can be determined against one another.

1. The Floating Exchange Rates

Floating Exchange rate is commonly used in most countries. Under this market forces, all the economies of developing countries allow their currency to flow freely. When the value of the currency becomes low it makes the imports more expensive but the exports cheaper, thus the country's domestic goods and services will be in higher demand from foreign buyers. A country could withstand exchange fluctuation only if its economy is strong. When the country's economy can meet the demand, then it can adjust between the foreign trade and domestic trade automatically.

2. The Fixed or Pegged Exchange Rates

Fixed or Pegged Exchange Rate is commonly used in small developing countries. Fixed exchange rates are used to attract foreign investments and promote foreign trade. By fixing the exchange rates, a country ensures its investors that their value of investment in that country is stable and constant. In this type the exchange rates the imports become expensive. The exchange value of the currency does not move. This normally reduces the country's currency against foreign currencies.

3. The Pegged Float Exchange Rates

Hybrid of float and fixed exchange rates is commonly used in developed countries. A country allows its currency to fluctuate to some extent for adjusting central value. Pegged allow some adjustments and stability. No artificial rates are found in fixed and floating exchange rates. Pegged can fix the economic problem by itself and provide growth opportunity. When a fixed value is not maintained by the country it cannot follow the fixed exchange rate.

The topic of currency exchange rates and factors influencing their changes have been reviewed by many scholars in the past decades and remains one of the hot topics in international economic studies. For example, Philip Lane¹ built his own model on theoretical and empirical research on long-run exchange rates. He analyzed long run nominal and real exchange rates of 107 countries between 1974-1992 and added to his model such variables like trade openness, country size, central bank independence and government debt.

Factors Influencing Foreign Exchange Rates

The following are some of the principal determinants of the exchange rate between countries:

¹ P.Lane. "What Determines the Nominals Exchange Rate: Some Cross-Sectional Evidence", The Canadian Journal of Economics, vol.32, pp.118-138,1999

1. Differentials in Inflation

As a general rule, a country with a consistently lower inflation rate exhibits a rising currency value as its purchasing power increases relative to other currencies. During the last half of the 20th century, the countries with low inflation included Japan, Germany, and Switzerland, while the U.S. and Canada achieved low inflation only later. Those countries with higher inflation typically see depreciation in their currency in relation to the currencies of their trading partners. This is also usually accompanied by higher interest rates.

2. Differentials in Interest Rates

Interest rates, inflation and exchange rates are all highly correlated. By manipulating interest rates, central banks exert influence over both inflation versus exchange rates, and changing interest rates impact inflation versus currency values. Higher interest rates offer lenders in an economy a higher return relative to other countries. Therefore, higher interest rates attract foreign capital and cause the exchange rate to rise. The impact of higher interest rates is mitigated, however, if inflation in the country is much higher than in others, or if additional factors serve to drive the currency down. The opposite relationship exists for decreasing interest rates — that is, lower interest rates tend to decrease exchange rates.

3. Current-Account Deficits

The current account is the balance of trade between a country and its trading partners, reflecting all payments between countries for goods, services, interest and dividends. A deficit in the current account shows the country is spending more on foreign trade than what it is earning and that it is borrowing capital from foreign sources to make up the deficit. In other words, the country requires more foreign currency than it receives through sales of exports, and it supplies more of its own currency than foreigners demand for its products. The excess demand for foreign currency lowers the country's exchange rate until domestic goods and services are cheap enough for foreigners, and foreign assets are too expensive to generate sales for domestic interests.

4. Public Debt

Countries engage in large-scale deficit financing to pay for public sector projects and government funding. While such activity stimulates the domestic economy, nations with large public

deficits and debts are less attractive to foreign investors. Large debt encourages inflation, and if inflation is high, the debt will be serviced and ultimately paid off with cheaper real dollars in the future.

In the worst case scenario, a government may print money to pay part of a large debt, but increasing the money supply inevitably causes inflation. Moreover, if a government is not able to service its deficit through domestic means (selling domestic bonds, increasing the money supply), then it must increase the supply of securities for sale to foreigners, thereby lowering their prices. Finally, a large debt may prove worrisome to foreigners if they believe the country risks defaulting on its obligations. Foreigners will be less willing to own securities denominated in that currency if the risk of default is great. For this reason, the country's debt rating (as determined by Moody's or Standard & Poor's, for example) is a crucial determinant of its exchange rate.

5. Terms of Trade

As a ratio comparing export values to import values, the terms of trade is closely related to current account and balance of payments. If the price of a country's export rises by a greater rate than that of its imports, its terms of trade have improved favorably. Increasing terms of trade shows greater demand for the country's exports. This, in turn, results in raising revenues from exports, which provides increased demand for the country's currency (and an increase in the currency's value). If the price of exports rises by a smaller rate than that of its imports, the currency's value will decrease in relation to its trading partners.

Other Influencing Factors

There are several influencing factors that determine the exchange rates, which are listed below:

1. **Political Stability and Economic Performance** – Foreign investors seek stable countries with strong economic performance to invest.
2. **Capital Account Balance** – A country with more exports of goods and services may lead to surplus of financial account in which it can attract more capital from others, appreciation in the currency value.

3. **Role of Speculators** – The currency value will rise when speculators believe that currency will increase in near future. It will create demand for that currency, causing the currency value to rise.
4. **Cost of Manufacture** – A lower manufacture cost will translate into export goods at a more attractive price, and hence currency value increases.
5. **Debt of the Country** – Lower debt will attract more foreign investors.
6. **Gross Domestic Product (GDP)** – Consolidation of total government expenses, business output, private consumption, and country's exports. Higher GDP indicates strong economy growth.
7. **Employment Data** – Higher employment rate will increase currency value as more people will earn an income. This leads to higher purchasing power.
8. **Relative Strength of other Currencies** – Currency valuations are also equally affected by global parameters. A country's economic strength is compared with another. If other countries are deemed stronger, more money will move to those countries. It ultimately reduces valuation of the country with comparatively poor health of the economy.
9. **Macroeconomic and Geopolitical events** – Stable macroeconomic and less volatile geopolitics increase currency value.
10. **Political and Psychological factors** – Political and psychological factors are believed to have an influence exchange rates. For example, Swiss Franc is deemed a refuge currency due to its stability.
11. **Capital Movement** – Countries which attract large capital inflows through foreign investments, will witness an appreciation in its currency. While a net outflow of capital would mean depreciation of currency.
12. **Fiscal Policy** – The government's fiscal policy has an impact on the economy which in turn, affects exchange rates. If the government follows an expansionary policy by having low interest rates, it will fuel the engine of economic growth and lead to better trade performance and increased currency value.
13. **Monetary Policy** – In tandem with fiscal policies of a government, monetary policy set by the Central Bank could be a very effective tool in controlling money supply and is used particularly for keeping a tab on

the inflationary pressures in the economy. The main objective of monetary policy is to maintain money supply in the economy at a level which will ensure price stability, full employment, and continued growth in the economy.

14. **Stock Exchange Operations** – Stock exchange operations in foreign securities, debentures, stocks, and shares, influence the demand and supply of related currencies, thus influencing their exchange rate
15. **Balance of Payments** – Balance of payments position of a country is a definite indicator of the demand and supply of foreign exchange. If a country is having a favourable balance of payments position, it implies that there is more supply of foreign exchange and therefore foreign currencies will tend to be cheaper compared to local currency.
16. **Exchange Control** – If a country wants to boost its exports, it could deliberately set the value of its currency low.
17. **Technical Factor** – Technical factors, particularly in the short run, can impact exchange rates. For example, reserve requirement set by a central bank may create a technical position that influences the exchange rates.

Conclusion

A high exchange rate results in higher prices of exports and lower prices for imports. This will reduce demand for exports and hence Aggregate Demand. A reduction in Aggregate Demand will ultimately lead to unemployment and lower economic growth, causing the current account to deteriorate.

Similar effects are added by an increased demand for imports; however, this is all dependent on the price elasticities of exports and imports. Should its price be inelastic, then there is likely to be little change. Lower import prices can be beneficial to customers. Households can buy more goods and services which is likely to increase their living standards.

Fluctuating exchange rates are riskier because they create uncertainty. Uncertainty is a disincentive to trade. For example, producers will be reluctant to buy international stock for fear that its value will depreciate in the future. Similarly, the profit for selling the goods could become lower than what it was initially.

There are ways to reduce exchange rate risk through future markets. This is where firms can guarantee an exchange rate by buying currencies at a fixed future rate. However, there are those who argue for a single currency among countries such as the Euro which would encourage trade and investment.

References

1. Adolfson, M., S.Leseen. J. Linde, and M. Villani, "Bayesian Estimation of an Open Economy DSGE Model with Incomplete Pass" *J.Doc.* vol.19, no.23, pp. 481-511, Apr. 2007.
2. Campbell, J.Y., and R.Shiller. "Cointegration and Tests of Present Value Models" *Journal of Political Economy*, vol.93, pp.1062-1088, Oct.1993.
3. Dornbusch and R., "Expectations and Exchange Rate Dynamics," *Journal of Political Economy*, vol.84, no.5, pp.1161-1176, 1976.
4. Engel, C., and K.D. West, "Exchange Rate and Fundamentals", *Journal of Political Economy*, vol.113, no.18, pp.485-517, Apr 2005.
5. Engel, R.F., and J.V.Issler, "Estimating Common Sectoral Cycles", *Journal of Monetary Economy*, vol.35, no.12, pp.83-113, Mac 1993.
6. Faust, J.,and J. Rogers, "Monetary Policy's Roles in Exchange Rate Behavior", *Journal of Monetary Economy*, Vol.50, no.21, pp.1403-1424, Mac 2003
7. Mark, and N., "Exchange Rate and Fundamentals : Evident of Long - Horizon Predictability," *American Economics Review*, vol.85, pp.201-218, Aug.1995.
8. Rogers and J.H, "Monetary Shocks and Real Exchange Rates", *Journal of International Economic*, vol.49, pp.269-288, Apr 2000.
9. Vahid, F. and R.F.Engle., "Common Trends and Common Cycles", *Journal of Applied Econometrics*, vol.8, pp.341-360, Jun 1993.

Protection Of Personal Data: Understand Your Rights As A Data Subject

By | Ahmad Khabir bin Shuhaimi, Ahmad Sirhan bin Abdul Ghazali, Ida Rajemee binti Ramlee & Naqliyah binti Zainuddin

Introduction

Most of us have received several unsolicited telemarketing and sales calls offering financial products such as insurance coverage. The most common way for telemarketers to get your data is to simply purchase it from a third party provider. Personal information which are often sought after include bank account or credit card details, identification number, phone numbers, medical records and home addresses.

A data breach occurs when a hacker gains access to the database of a service provider or company which contains users' private information. This information can range from usernames and passwords to billing addresses. These lists are then sold online to a black market for commercial transactions such as advertising, marketing, and sales purposes.

In 2017, a massive data breach saw the customer data of more than 46.2 million mobile subscribers in Malaysia leak on to the dark web. The leaked information included customer details, mobile numbers, home addresses, mobile phone models, sim card information including unique IMEI and IMSI numbers. Time stamps indicated that the leaked data was last updated between May and July of 2014. It is believed to be the largest data breach in Malaysian history [1]. Another case which relates to breach of personal data was in January 2018 where local IT portal Lowyat.net reported personal details of 220,000 Malaysian organ donors and their next of kin have been leaked online. Files containing details of pledged organ donors were updated as of August 31, 2016. Among the data distributed were name, address, age, identification card number, gender, race, email and organ to be donated [2].

The cases cited above show that our personal data are indeed exposed to risk when manipulated by irresponsible parties with malicious intent, where the data are used beyond the intended purposes. Personal data relates directly or indirectly to a data subject, which is an individual who is the subject of the

personal data. For example, students, patients, employees, citizens, non-citizens. Once it is compromised, it will put us in danger, and it will threaten our safety and welfare.

Each individual is responsible to ensure his/her own personal data is well protected from abuse. As such, understanding our rights as a data subject, who own the personal data, is crucial.

Our Rights

In Malaysia, personal data protection is addressed by Personal Data Protection Act 2010 (PDPA) which regulates the processing of personal data in regards to commercial transactions. According to Malaysia's PDPA, personal data means any information in respect of commercial transactions that relates directly or indirectly to a data subject, who is identified or identifiable from that information [3] e.g. our National Registration Identity Card Number (NRIC), image, phone number, passport, bank account, credit and debit card, birth dates, full names, e-mail and home address, medical and health records [4]. This includes any sensitive personal data and expression of opinion about the data subject.

In an annual report published by Malaysia Department of Personal Data Protection (DPDP) in year 2018, there were seven (7) cases which regulatory action have been taken under the Act 709 Section 16(4) processed personal data without a certificate of registration. In year 2017, there were 320 complaints received by DPDP through PDP online complaints application, while in year 2018 630 complaints were lodged which showed an increase of 49.21% from 2017 [5].

Understanding the rights of a data subject will enable us to execute necessary action to protect our personal data privacy. Apart from data subject, there are two other important players in personal data protection, which are data user and data processor. A data user is a person who either alone or jointly processes any personal

data or has control over or authorizes the processing of any personal data. While a data processor can be any person, who processes the personal data solely on behalf of the data user, and does not process the personal data for any of his own purposes.

All the players in personal data protection have their important and significant roles. However, this article will explore the rights of data subject in protection of data privacy. According to Malaysia PDPA, there are five (5) rights of a data subject as follows:

a. Right of access to personal data

- An individual is entitled to be informed by a data user whether personal data of which that individual is the data subject is being processed by or on behalf of the data user.

b. Right to correct personal data

- The data subject knows that his personal data being held by the data user is inaccurate, incomplete, misleading or not up-to-date, the requestor or data subject, as the case may be, may make a data correction request in writing to the data user that the data user makes the necessary correction to the personal data.

c. Withdrawal of consent to process personal data

- A data subject may by notice in writing withdraw his consent to the processing of personal data in respect of which he is the data subject.

d. Right to prevent processing likely to cause damage or distress

- A data subject may, at any time by notice in writing to a data user, require the data user at the end of such period as is reasonable in the circumstances, to cease the processing of or not begin the processing for a specified purpose or in a specified manner should the processing of that personal data is causing or is likely to cause substantial damage or substantial distress to him or to another person; and the damage or distress is or would be unwarranted.

e. Right to prevent processing for purposes of direct marketing

- A data subject may, at any time by notice in writing to a data user, require the data user at the end of such period as is reasonable in the circumstances to cease or not to begin processing his personal data for purposes of direct marketing.
- Where the data subject is dissatisfied with the failure of the data user to comply with the notice, whether in whole or in part, under subsection, the data subject may submit an application to the Commissioner to require the data user to comply with the notice.

Our Actions

Apart from knowing our rights as a data subject, there are other precautionary measures to safeguard our personal data. Figure 1 denotes some actions that may be considered to protect our personal data.



Figure 1: Our Actions

As shown in Figure 1, the actions are described in the following sub-sections:

- a. **Stop, Ask and Verify: Know Our Data User.** Be vigilant to online and offline scams. Do not simply share your personal data to an unknown party. Kindly ensure the party or company that you are dealing with, understands and comply with the Act before you surrender your data to them. Do not simply trust and share our information without verifying the party or company. [6];
- b. **Read and Understand the Terms and Conditions.** The terms and conditions (T&C) should be understood before executing any agreement either online or offline and providing our personal data to ensure our rights defined clearly according to the Act. Failing to fully understand the stated T&C may cause us to allow our personal data to be used other than for the intended purposes [7]. This may lead to sharing of our personal data to other parties;
- c. **Stop and Think: Limit Our Personal Data Sharing.** Not every data should be made public. Think before we post. Be careful and don't simply share our personal data online [6]. We need to discern what we can share and what not to share. Do not simply reveal our personal data to public, especially on social media;
- d. **Lodge a Complaint.** If we feel that our personal data has been abused in a commercial transaction by the organisation or data user which processed in breach of any provision of the Act, we may lodge a complaint to the Commissioner for our safety, welfare and right of privacy. The complaint can be submitted to the Commissioner through an online complaint form through the PDP official website at www.pdp.gov.my [8].

Summary

The frequency and severity of data breaches are increasing at an alarming rate. As we use more technology and put more of our information online, there are many potential vulnerabilities. Data breach involving personal data is fast growing in scope, affecting more organizations and people. Much is at stake as data breaches impose financial, reputational, and lost opportunity costs on individuals and organizations. As the threat of these security incidents rises, it's important that companies take steps to protect themselves.

As personal data relates directly or indirectly to a data subject, understanding the rights as a data subject is crucial. By understanding those rights, data subjects can execute the necessary action and be assured that their personal data is not being misused for anything other than the legitimate purpose for which it was originally provided.

References

1. Vijandren, "46.2 Million Malaysian Mobile Phone Numbers Leaked From 2014 Data Breach." <https://www.lowyat.net/2017/146339/46-2-million-mobile-phone-numbers-leaked-from-2014-data-breach/> (accessed Jun. 04, 2020).
2. Vijandren, "Personal details of 220,000 Malaysian organ donors and their next of kin leaked online." <https://www.lowyat.net/2018/153125/personal-details-220000-malaysian-organ-donors-next-kin-leaked-online/> (accessed Jun. 04, 2020).
3. P. D. Protection, "PERSONAL DATA PROTECTION," no. June, 2016. "Personal Data Protection Act 2010 (Act 709)" (2016, June 15) Part I, Preliminary, Section 4. Interpretation.
4. "Ambil Peduli (Data Peribadi)" (2016, September 30) Retrieved on 25th May 2020 from https://www.pdp.gov.my/jpdpv2/galeri_video/psa-ambil-peduli-data-peribadi/
5. "Laporan Tahunan Jabatan Perlindungan Data Peribadi Tahun 2018". Retrieved on 25th May 2020 from URL: <https://www.pdp.gov.my/jpdpv2/assets/2020/02/LAPORAN-TAHUNAN-JPDP-2018.pdf>
6. Data Subject Awareness e-Posters Retrieved from Official Facebook Page of Jabatan Perlindungan Data Peribadi Malaysia.
7. "Baca dan Fahami" (2019, October 15) Retrieved on 25th May 2020 from URL: https://www.pdp.gov.my/jpdpv2/galeri_video/psa-baca-dan-fahami/
8. "Aduan Akta Perlindungan Data Peribadi (709)" (2016, June 24) Retrieved on 25th May 2020 from URL: https://www.pdp.gov.my/jpdpv2/galeri_video/aduan-akta-perlindungan-data-peribadi-709/

“Has My Phone Been Hacked?” – Tips On Common Hardware Failure

By | Nur Qurratu 'Aini binti Rohizan

Introduction

One of the main services offered by Cyber999 is to provide technical assistance for ICT users in Malaysia. It is very common for Cyber999 to receive reports claiming “My phone has been hacked!” whereby users claimed that there had been attempted ‘hacking’ on their mobile phones.

Before we proceed further, we would like to stress that we are not a law enforcement agency and hence, we do not have the authority to investigate hacking-related activities. Criminal offences such as hacking comes under the law of Computer Crimes Act 1997 which is the jurisdiction of the Royal Malaysia Police (PDRM).

A recent reported case involved an e-hailing driver who was using an outdated smartphone. Due to incompatibility issues, his app performance was poor including inaccurate location which led the user to believe that his phone was hacked. This is a classic example where a user claimed his phone had been hacked whereas what it was actually was a hardware-related issue.

Below we identify common hardware failures that affects your mobile phone’s performance:

1. Screen / LCD Display Problem

Causes:

- High impact from accidental drop which could cause screen crack
- Failure to use a protective case or screen protectors
- Heavy pressure on phone for a prolonged period of time

Symptoms:

- Totally blank or black screen. It looks as if the device has been powered off whilst it is still on. This happens where either the screen is not well connected to the PCB or maybe the display IC is faulty. At times it may be due to the actual screen being damaged.

- Screen touch not responsive: It may be due to damage to the whole screen or just the digitizer /calibrator.
- Screen without ink but with visible lines / marks: The screen is shattered: non-reparable but usable
- Screen touch not responsive: It may be due to damage to the whole screen or just the digitizer /calibrator.

2. Hardware Problems resulting from Water damage

Symptoms:

- The phone overheats easily
- Phone speakers or earpiece may stop working or start malfunctioning
- The screen may go blank

3. Hardware problem that can cause your phone to overheat

Causes:

- Water damage
- Using counterfeit or faulty charger
- Third party Apps
- One or two Integrated circuits(IC) is faulty
- Multitasking on your phone
- Excessive video playback
- Multiple connectivity enabled like Wi-Fi, Bluetooth, and data
- Charging a phone and operating it at the same time

Symptoms:

- Your phone gets unbearably hot
- Swollen Battery
- Your phone gives a warning and shuts down on you

4. Phones hardware problems associated with memory/storage

Symptoms:

- Repeated warnings of low memory on your phone
- Some data may disappear automatically
- Your phone may crash
- Some Apps may stop working
- Your phone may enter a boot-loop

5. When Your Phone Speaker is Crackling or Distorted

Causes:

- Water or liquid damage
- Dust contamination
- Phone sustained high impact from dropping
- Wear and tear

Symptoms:

- Poor coverage
- Suddenly no ringtone / volume
- Audio disruption during a phone call. For example, user A calls user B. User A cannot hear the voice of user B and vice versa

6. Motherboard / Processor Faulty

Symptoms:

- A boot stuck at brand's logo
- Unable to turn on the phone
- Low screen backlight where the phone's screen brightness is really dim

7. Charger Port Faulty

Symptoms:

- Your phone does not charge at all
- Your phone charges irregularly.
- There is the constant "not charging alert"

8. Wi-Fi Chipset Fault

Symptoms:

- Unable to detect Wi-Fi connection

9. Antenna Fault

Symptoms:

- No network connection/unable to detect network coverage
- Problem with Internet connectivity, SMS and call services
- Disappearance of network coverage

10. Miscellaneous

Causes and symptoms:

- A physical home button particularly for iPhone. After repairing the home button whether at an official store or any third-party services, there will be a problem where the phone would be unable to detect fingerprint on the home button.
- LCD backlight issues particularly with iPhone 6 Plus. The phone screen is on, but users are unable to view the screen clearly as the screen's light is really dim.

If it's not a security related issue, we will advise users to refer to MyCERT's best practices on safeguarding their mobile phones in our website <https://www.mycert.org.my/>

- Set a password or passcode for your smart phone. Most smart phones now allow users to set password security and automatically lock the phone after a period of inactivity.
- Users are advised to verify application permission and the application author or publisher before installing it.
- Refrain from clicking on questionable advertisement or suspicious URL sent through SMS/messaging services. Malicious program could be attached to collect device information.
- Run a reputable anti-virus on your mobile devices and keep it up to date regularly. Most mobile phone nowadays comes with pre-installed security software.
- Avoid using public Wi-Fi networks for sensitive matters especially banking transactions.
- Turn off Bluetooth connection when not in use.
- Regularly update operating system and applications on mobile devices when it becomes available.
- Avoid rooting your mobile device (for Android) or jailbreaking (for iOS).

- Install application from official sources such as Google Play and App Store.

References

1. <https://www.mycert.org.my/portal/details?menu=431fab9c-d24c-4a27-ba93-e92edafdefa5&id=ad40bf86-69c6-4a21-af96-1c980fe35d00>
2. <https://www.mycert.org.my/portal/details?menu=431fab9c-d24c-4a27-ba93-e92edafdefa5&id=4d245fbd-df65-4e64-b1af-53e524a331f0>

Title Of The Article- COVID-19: Stay Safe On & Offline!

By | Nurul 'Ain binti Zakariah, Nur Fazila binti Selamat, Zaihasrul bin Ariffin, Mohd Nor A'kashah bin Mohd Kamal & Mohd Azlan bin Mohd Nor

Introduction: Coronavirus (COVID-19)

Corona Virus or also known as COVID-19 is a newly discovered virus that is highly infectious. It was first identified in Wuhan City, Hubei Province, China and reported to World Health Organisation (WHO) on 31st December 2019. In less than 3 months, on 11th March 2020, WHO declared COVID-19 a global pandemic.

COVID-19 affects people in different ways. Most infected people will develop mild to moderate respiratory illness displaying symptoms such as fever, dry cough, and fatigue but will recover without requiring hospitalization whilst older people and people with chronic underlying medical problems such as cardiovascular disease, diabetes, chronic respiratory disease and cancer are most likely to develop serious illness that require intensive care in hospitals.

COVID-19 In Malaysia

The COVID-19 outbreak became a pandemic very quickly due to its capacity to spread viciously over multiple countries. Malaysia could not escape the brunt of the pandemic. Consequently, on 13th March 2020, Malaysia Prime Minister Tan Sri Muhyiddin Yassin initiated a Movement Control Order (MCO) in order to curb the spread of the virus.

This MCO was imposed in 5 phases within the duration from 18th March 2020 to 9th June 2020. Malaysia's armed forces, the Royal Malaysian Army was activated and deployed to assist Royal Malaysian Police to enforce the various phases during the MCO period.

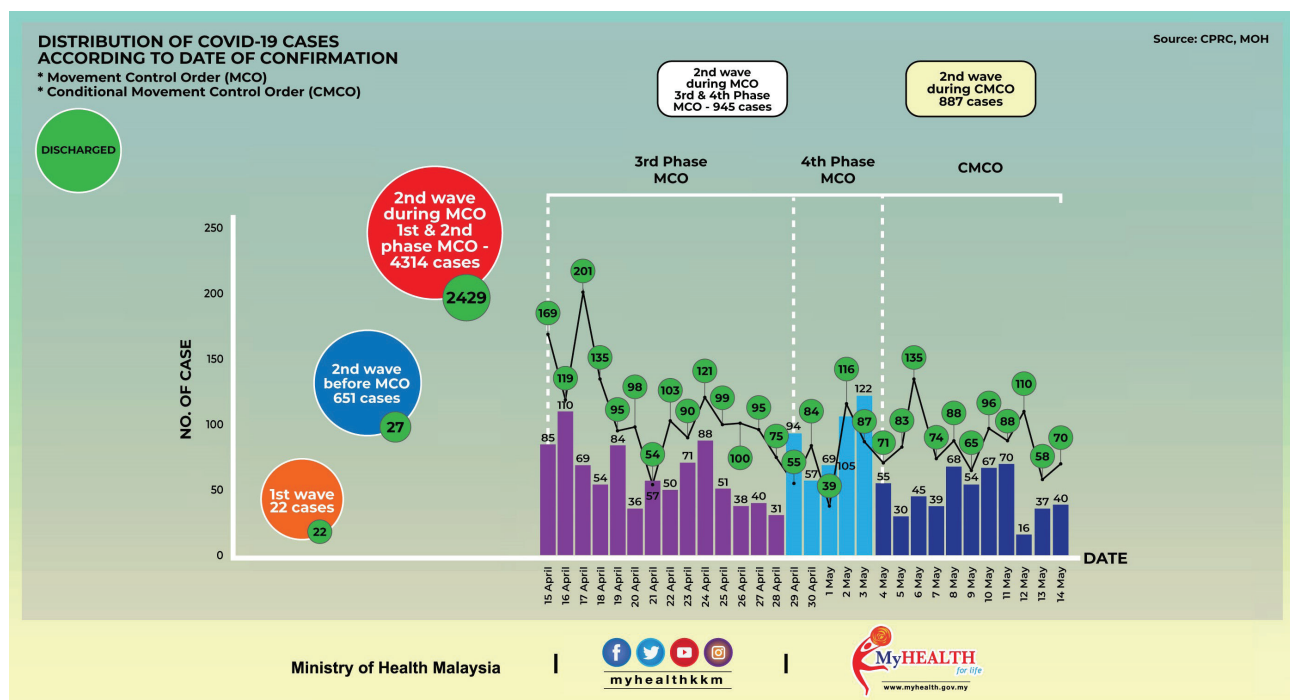


Image 2 : Graph of COVID-19 Statistic in Malaysia as of 14th May 2020 (CMCO Phase) (Source : Ministry of Health (MOH) Malaysia)

During MCO period, the government has taken several blockade & isolation measures which include[9]:-

- a. The general prohibition of mass movements and gatherings across the country include religious, sports, social and cultural activities. To enforce such prohibition, all houses of worship and business premises are closed. Only essential food services such as supermarkets, public markets, grocery stores and convenience stores were allowed to operate but with strict limitations and adherence to Standard Operating Procedures (SOP).
- b. Malaysians returning from abroad are required to undergo health check and self-quarantine for 14 days
- c. Tourists and foreign visitors are not allowed to enter the country.
- d. Closure of all kindergartens, government and private schools and higher education institutions (IPTs)
- e. Closure of all government and private premises except those defined as essential services (water, electricity, energy, telecommunications, postal, transportation, irrigation, oil, gas, fuel, lubricants, broadcasting, finance, banking, health, pharmacy, fire, prison, port, airport, safety, defence, cleaning, retail and food supply.

The Central Bank of Malaysia announced a 6 month moratorium period that allows deferment of loan repayment to ease the impact of business disruption especially those who are unable to work during the MCO period.

Keep Yourself Protected!

COVID-19 spreads through droplets of saliva or discharge from the nose when an infected person coughs or sneezes. Scientist around the world are still working round the clock to develop vaccines and treatments for the novel coronavirus. For the time being, the best way to prevent and slow down the transmission is to adopt new etiquettes and lifestyle changes as advocated by WHO:

1. Maintain at least 1 meter physical distance from those with symptoms

Maintain 1 metre distance between yourself and other people at all times especially from those who sneeze and cough. You may be

infected from the droplets discharged by an infected person.

2. Wash hands frequently with water and soap or use hand sanitizer

Good personal hygiene should be observed at all times. Wash your hands regular hand washing with soap and water or use hand sanitizer especially after coughing or sneezing.

3. Avoid crowded places

Individuals with chronic diseases or underlying health conditions should avoid crowded places. If you need to go out, make sure you wear a surgical mask.

4. Wear mask

If you have running nose or flu like symptoms, you are advised to stay at home. If you need to go out, make sure you wear a surgical mask.

5. Cover your mouth and nose when coughing or sneezing

Dispose tissue after using and wash hands with soap and water or use hand sanitizer after coughing or sneezing. You may also try to cough into a flexed elbow

6. Seek early medical treatment if you have fever, cough and breathing difficulties

Should you have fever or experience cough and breathing difficulties, wear a surgical mask and seek medical attention at the nearest health facility immediately. Accompanying person should also wear a surgical mask.

Keep Safe Online During COVID-19!

COVID-19 has impacted people's lives significantly in many ways. With the implementation of MCO in Malaysia, the general public were largely confined to their abode. This has significantly raised the use smart phones, laptops and other devices to stay connected online for work, meetings, school, shopping, and even entertainment such as online games.

Consequently, more Malaysians who go online are being exposed to cyber-attacks and online

scammers who are seeking to exploit their vulnerabilities.

Below are the tips to help you to stay cyber safe during COVID-19[14]:

1. STAY VIGILANT

Be vigilant with cyber threats via email, text message, social media including phone call from unknown sources that request for your personal or sensitive data.

2. PASSWORD HYGIENE

Ensure all your device and system passwords are updated, validated and secure but don't write them down or share it with your family.

3. SECURE NETWORK

Connect your Internet using secure network and do not use public Wi-Fi. Always connect through your home or mobile network or using virtual private network (VPN).

4. EMAIL SCAMS

Do not open unknown emails from people you don't know. Be particularly careful with any emails especially referencing COVID-19. Threat actors love to exploit real world tragedies and COVID-19 is no different. [16]

5. WORK DEVICE

Do not conduct work and personal activities on the same device wherever possible and don't share access to work device with your family. Always lock your device away when not in use.

6. UPDATE REGULARLY

Update your device and software regularly including mobile devices and any other non-corporate issued devices that you use for work. Antivirus software must be installed and be regularly updated.

7. OFFICIAL DOCUMENT

Do not under any circumstances use free or third-party application to send official documents.

8. BACKUP

Always backup up your data especially when working remotely. Data at rest such as local drives or external hard disk should be encrypted. This will protect your data against theft or loss of device. [17]

9. FAKE NEWS

Always verify the authenticity of any information received via email, text message, social media or even phone call. Refer only to trusted sources, Government-approved website and channels to determine latest information.

a. Sebenarnya.my website - <https://sebenarnya.my>

b. Majlis Keselamatan Negara telegram - <https://t.me/MKNRasmi>

c. Kementerian Kesihatan Malaysia telegram - <https://t.me/cprckkm>

10. ONLINE TELECONFERENCE

Protect your teleconferencing session with strong password and avoid sharing confidential and sensitive documents. Always monitor your teleconference session closely and block unauthorized participant.

11. 20-20-20 RULES

Excessive use of digital device can lead to farsightedness and Digital Eye Syndrome (DES) such as blurred vision, strain and tiredness, dryness and redness as well as headaches. You can practice the 20-20-20 rules to reduce this syndrome.

"After 20 minutes looking at the screen,
Look away for 20 seconds and gaze
at objects about 20 feet away."

12. REPORT

Last but not least, lodge a report to your respective IT department or Cyber999 Emergency Help Centre (<https://www.mycert.org.my>) if your encounter any cyber security threats or incident.

Conclusion

Since COVID-19 was declared a pandemic, work places, schools, and businesses have been temporarily shut, compelling people to stay at home. Protect yourself and others from infection by washing your hands or using an alcohol based disinfectant frequently and refrain from touching your face.

During MCO, businesses are encouraged to operate through virtual meetings while schools deliver their lessons via online platforms to prevent any possible transmission through physical contacts. This is a period when more and more devices are being connected to the Internet, hence increasing cyber risks for all.

Regardless of where we are, everyone is advised to stay cyber safe and vigilant by connecting using secure network. Always be alert for scam emails. Do not click on suspicious links, Keep software updated on all devices. Avoid using third party application for any official documents

or online meetings. Frequent backing up data is also essential to prevent data loss during unwanted incidents.

Scammers or cyber bullies are always on the lookout to exploit people who are vulnerable in cyberspace especially during this outbreak. If you encounter any cyber security threats or incident, you can lodge report to Cyber999 Emergency Help Centre (<https://www.mycert.org.my>)

References

1. COVID-19 (Maklumat Terkini) (2020). Retrieved April 2, 2020, from <http://covid-19.moh.gov.my/>
2. Sipalan, Joseph; Holmes, Sam. (2020, January 25). Malaysia confirms first cases of coronavirus infection. Retrieved from <https://www.reuters.com/article/china-health-malaysia/malaysia-confirms-first-cases-of-coronavirus-infection-idUSL4N29U03A>
3. CyberSecurity Malaysia [@cybersecurity_malaysia] (2020, March 26). Gunakan Internet Secara Berhemah. Elakkan diri dari menjadi mangsa salah laku internet. Laporkan sebarang insiden siber ke pusat bantuan Cyber999. #COVID19Malaysia #PerintahKawalanPergerakan #StayAtHome #DudukDiRumah [Instagram Photo]. Retrieved from https://www.instagram.com/p/B-Le8CBHnE_/
4. CyberSecurity Malaysia [@cybersecurity_malaysia] (2020, March 27). Elak dari menjadi mangsa penipuan pembelian dalam talian #COVID19Malaysia #PerintahKawalanPergerakan #StayAtHome #DudukDiRumah [Instagram Photo]. Retrieved from https://www.instagram.com/p/B-OGDSQHtS_/
5. CyberSecurity Malaysia [@cybersecurity_malaysia] (2020, April 1). BERITA PALSU. Hindar dari sebar berita palsu | FAKE NEWS. Do not spread fake news #COVID19Malaysia #PerintahKawalanPergerakan #StayAtHome #DudukDiRumah #pkp #mco #cybersafe [Instagram Photo]. Retrieved from <https://www.instagram.com/p/B-a1WM1HbUc/>
6. CyberSecurity Malaysia [@cybersecurity_malaysia] (2020, March 31). Perlindungan Kata Laluan | Password Protection #COVID19Malaysia #PerintahKawalanPergerakan #StayAtHome #DudukDiRumah #pkp #mco #cybersafe [Instagram Photo]. Retrieved from <https://www.instagram.com/p/B-YeQneH-uY/>
7. Ho, Yudith. (2020, April 3). Malaysia Braces for Coronavirus Infections to Peak in Mid-April. Retrieved from [https://www.bloomberg.com/news/articles/2020-04-03/malaysia-braces-for-](https://www.bloomberg.com/news/articles/2020-04-03/malaysia-braces-for-coronavirus-infections-to-peak-in-mid-april)
8. Abd Mutalib, Zanariah; Abdul Karim, Luqman Arif. (2020, April 13). 25 kluster, subkluster COVID-19. Retrieved from <https://www.bharian.com.my/berita/nasional/2020/04/676696/25-kluster-subkluster-covid-19>
9. News Strait Times. (2020, March 16). Covid-19: Movement Control Order imposed with only essential sectors operating. Retrieved from <https://www.nst.com.my/news/nation/2020/03/575177/covid-19-movement-control-order-imposed-only-essential-sectors-operating>
10. COVID Guide for Social Distancing. Retrieved from https://www.moh.gov.my/moh/resources/Penerbitan/Garis%20Panduan/COVID19/Annex_26_COVID_guide_for_Social_Distancing_24032020.pdf
11. COVID Guide for Workplaces. Retrieved from https://www.moh.gov.my/moh/resources/Penerbitan/Garis%20Panduan/COVID19/Annex_25_COVID_guide_for_workplaces_22032020.pdf
12. COVID Guide for Special Settings. Retrieved from https://www.moh.gov.my/moh/resources/Penerbitan/Garis%20Panduan/COVID19/Annex_27_COVID_guide_for_special_settings_25032020_.pdf
13. Preventive Measures for Coronavirus Disease 2019 (COVID-19). Retrieved from https://www.infosihat.gov.my/images/media_sihat/lain_lain/images/Banner%20BI%20Final.jpg
14. Cybersecurity & Safety Infographic. Retrieved from <https://www.cybersecurity.my/infographic>
15. Malaysia Computer Emergency Response Team (MYCERT). Retrieved from <https://www.mycert.org.my>
16. How to protect yourself from cyberattacks when working from home during COVID-19. Retrieved from <https://www.weforum.org/agenda/2020/03/covid-19-cyberattacks-working-from-home/>
17. Tips for cybersecurity when working from home. Retrieved from <https://www.enisa.europa.eu/topics/wfh-covid19/tips-for-cybersecurity-when-working-from-home>
18. Coronavirus. Retrieved from https://www.who.int/health-topics/coronavirus#tab=tab_3
19. How to stay safe online during the COVID-19 crisis. Retrieved from <https://www.amnesty.org/en/latest/news/2020/04/stay-safe-online-during-the-covid-19-crisis/>

The Work From Home Checklist

By | Nurul Husna binti Mohd Nor Hazalin & Zaihasrul bin Ariffin

The Coronavirus Disease (COVID-19) was first reported in Malaysia in early January 2020. A massive spike in the number of cases was contributed by the Sri Petaling mosque Tabligh gathering cluster. The Tabligh gathering held in early March saw a significant jump in active cases and forced the government to initiate the Movement Control Order (MCO) starting from 18 March until 31 March 2020. Throughout this phase, only essential services and selected businesses were allowed to operate. The rest

were instructed to stay at home. Employers were strongly encouraged to implement a 'Work from Home' policy for all their employees.

Work from Home (WFH) used to be a privilege accorded by a handful of companies to their employees in Malaysia, but since the imposition of MCO, WFH has become the norm for many. To provide employees with a safe remote working environment, here is a simple checklist for successful remote working.



The infographic is titled "WORK FROM HOME CHECKLIST" in large, bold, blue and orange letters. It features the logos of the Ministry of Communications and Multimedia Malaysia and CyberSecurity Malaysia at the top. The checklist consists of six numbered items, each with an icon and a brief description:

- 1 Network**: choose your home connectivity. Use Virtual Private Network (VPN) to access your company data. (Icon: Cloud with a shield and a laptop)
- 2 Password**: Check your password validity. If it's almost expired, please change it immediately. Use strong and unique passwords. (Icon: Padlock)
- 3 Anti-Virus**: Check your AV status. Make sure that it is updated to the latest one and working accordingly. (Icon: Shield with a virus icon)
- 4 Email**: Verify your email services by trying to send / receive email via your mail client. (Icon: Envelope)
- 5 Technical support**: Make sure that you have all contact of relevant support personnel, which may be needed to assist when you faced any problem when working from home. (Icon: Person in a suit)
- 6 Awareness**: Be aware of any phishing or scam emails and always exercise good security precautions when receiving, sending or responding to emails and calls. (Icon: Two people talking)

The background of the infographic shows a stylized illustration of a person working from home at a desk with a laptop, a clock, and a lamp.

Transformation To Modern Finance

By | Farah Harnum binti Ghulam Haidir

Introduction

For businesses that want to survive in today's fiercely competitive marketplace, change is no longer an option but a necessity. Being agile is vital to business survival. According to Cambridge Dictionary, agile means "able to think quickly and clearly (mind)" or "able to move about quickly and easily (physical)". Agility in business refers to the ability of a business system to rapidly respond to changes by adapting from its initial configuration. In a business context, it means the ability to rapidly adapt to market and environmental changes in both productive and cost-effective ways.

Transformation to modern finance is pivotal to survival in a digital economy. The outdated finance process of transactional data input and financial report generation needs to be overhauled. This task can now be done within seconds by modern finance technology.

Transformation and modernisation require finance leaders and professionals to adopt new traits to become digital finance leaders and professionals. A successful transformation requires change in people, process, and systems.

Evolving Role of a Financial Leader

The traditional role of a finance leader centres on operations and financial responsibilities. While these tasks have been well-defined and executed, it is no longer sufficient in today's business environment. The role of a financial leader is now shifting from traditional back office support function to a more strategic and forward looking one. The Financial Leader must be able to record the past, manage the present and anticipate the future by working closely with other departments to generate valuable insights to drive rapid decision making.

Below are the viable models to describe the various roles of the Financial Leader:

Steward	Protect and preserve the critical assets of an organization and accurately report on the financial position and operations to internal and external stakeholders.
Operator	Balance capabilities, talent, costs, and service levels to fulfil the finance department core responsibility efficiently.
Strategist	Provide financial leadership in determining strategic business direction, financing, capital market and long-term strategies that are vital to a company's future performance.
Catalysts	Catalysts behaviour across the organization to execute strategic and financial objectives and at the same time create a risk intelligent culture.

"Steward" and "operator" are traditional roles. In order to be agile, the Finance Leader and its professional team need to transform and take on "strategist" and "catalyst" roles. The focus is shifting from cost based to organisational value based. The finance function is no longer evaluated purely on how costly it is to run or viewed as a cost centre. Instead, the effectiveness of a finance role will be judged on added values to an organisation and the wider community.

To be agile, finance leaders need to transform and embrace modern finance.

1. Respond rapidly to change. They must become more responsive to dynamic changes in the market, enable new business models and proactively manage risk and compliance. A finance leader must be insightful and provide accurate, timely and actionable information to all stakeholders. In addition, they must be efficient in delivering finance services at a competitive cost while being flexible to demands.
2. Technological advancement has dramatically changed the finance function. A finance leader must embrace technological changes and ensure the entire team adapts swiftly. Key technology areas include Cloud Computing, Intelligent Automation (Machine

learning and Robotic Process Automation), Internet of Things, Blockchain, Big data and analytics, Digital Process and Cybersecurity and next generation Enterprise Resource Planning (ERP) application, which features updated user interfaces and database and cloud computing.

3. The finance function has long been concerned with historical data, reviewing numbers and transactions. The advancement in technology is now enabling Finance Leader to become more forward thinking and proactive, taking on more direct roles in setting a company's strategic direction. Thus, CFOs need to embrace continuous learning. They need to meet regularly with all business managers to discuss critical success factors; identify growth markets and how to capitalize on opportunities for business survival. While some of the new responsibilities may not directly be connected to finance, they could help elevate the organisation's competitive advantage and financial results over the long term.
4. Adoption of agile operating model. The traditional function of finance in an organisation tends to focus on transaction processing, management reporting, budgeting, planning and ad hoc analysis. They do not have time to look beyond their unit-specific tasks and help shape the overall financial strategy of their business. The finance team needs to become more agile in order to mobilize its staff to take on more mission critical functions. For example, they can serve as knowledge and intelligence integrator by collating information from across multiple functions as well as sources within the organisation.

Finance transformation & modernisation mechanism- people, process, and systems

People, process, and systems are three important elements in transformation and modernisation. They help reduce cost, save time, and enhance the capacity to be more strategic and valuable to the organisation.

People

Not all technology and automation can function independently without humans. In this regard, finance professionals need to re-skill in the

face of automation. Cognitive functions still require human intervention which machines are unable to do. Traits such as leadership, creativity, empathy, judgement, ethics and professionalism are critical.

Technology and automation has freed finance professionals from mundane tasks so they could focus on tasks that add real value to the business and organization.

The traditional finance function centres on compliance and cost. This model leads to strategic behaviour on cost minimisation. Such model curtails the full potential of the accounting discipline. Figure 1 shows that the traditional finance focus on compliance while modernisation put more emphasis in delivering value using technological automation.

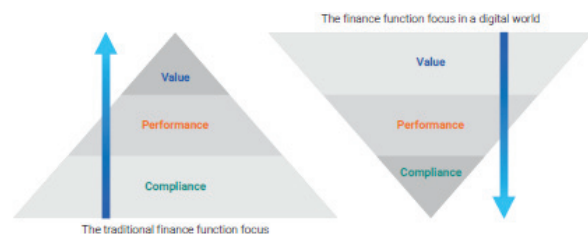


Figure 1: Inverting the finance focus pyramid for a digital world

A research study done by Chartered Global Management Accountant (CGMA) revealed that there is a change in competencies in the digital world. People and machine integration requires new skill sets and competencies. Digital skills and mind sets are essential for digital transformation and modernisation of finance.

Finance professionals could no longer rely just on accounting and finance skills to excel in this digital world. Based on the CGMA Competency Framework, finance professionals need to acquire technical skills and able to apply them in a business context. They must also possess people and leadership skills underpinned by integrity, ethics as well as professionalism to inspire and lead an organization.

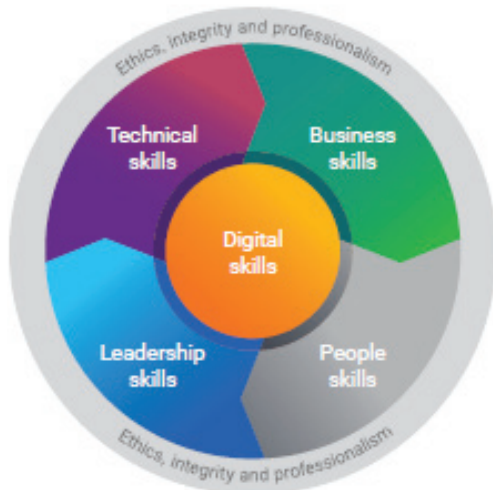


Figure 2: The 2019 CGMA Competency Framework

Process

Finance processes need to focus on providing strategic review support to revamp core business processes. This includes all transactional processes from Account Payables and Account Receivables to Enterprise Performance Management (EMP) that support budgeting, forecasting and financial reporting.

Systems

Systems are the blueprint of modernisation. The finance team needs to revamp key business processes in order to realize benefits of digitalisation. Transactional processing that uses accounting system can be standardised and consolidated with an Enterprise Resource Planning (ERP) System in order to streamline processing and enable a shared services model.

In general, ERP uses a centralized database for various business processes to reduce manual labour and simplify existing workflows. ERP systems typically contain dashboards where users can look at real-time data collected from across the business to monitor productivity and profitability.

Shared services model entails consolidating business operations across multiple parts of the same organization. It is more cost-efficient because they centralize back-office operations which are used by multiple divisions of the same company and eliminates redundancy.

Organizations also need to consider consolidating Human Capital Management (HRM) & Customer Relationship Management (CRM) functions in order to streamline insights and realize process efficiency.

Enterprise Performance Management (EPM) is another system that can support key management process across multiple departments. EPM supports modelling, planning, consolidating, reporting and also analytics via web browser. It is integrated with Microsoft Excel spreadsheet and Office and also be accessed through mobile devices.

By utilizing EPM, the Finance team can replace legacy applications and integrate with ERP and other systems.

Conclusion

Transformation to modern finance compels businesses to revamp each and every part of the organisation and adopt best practices. Such transformation will help the Finance function expand its traditional roles and become more efficient. This reengineering process will also help redefine their roles and maximize the benefits of modernization.

References

1. https://en.wikipedia.org/wiki/Business_agility
2. *Re-inventing finance for a digital world- The future of finance* CGMA
3. *Agile Finance Unleashed- the key traits if digital finance leaders-* AICPA & CIMA
4. <https://www.mckinsey.com/business-functions/operations/our-insights/new-technology-new-rules-reimagining-the-modern-finance-workforce>
5. *Finance In the Cloud-EY*
6. <http://xbrl.squarespace.com/journal/2018/11/2/financial-transformation-and-the-modern-finance-platform.html>
7. <https://blog.aspiresys.com/enterprise-business-application/agile-finance-transformation-story-modern-finance/>
8. <https://go.oracle.com/why-modern-cfos-need-agile-finance-model>
9. <https://www.fmmagazine.com/news/2017/may/agile-finance-function-201716378.html>
10. <https://www.educba.com/agile-finance/>

Social Media For Awareness Program

By | Nor Radziah binti Jusoh

Leveraging Social Media for Effective Awareness Campaign

The COVID-19 pandemic has made a huge impact on our lifestyle since it struck globally. The disease has forced many countries to impose movement restrictions which affect daily routines of almost every citizen. Activities from going to office, shopping at malls for leisure and attending family social gatherings have all come to a grinding halt. The pandemic has forced us to move from physical interaction to a virtual one. This has prompted many to turn to social media.

As an organisation which is tasked to create cyber security awareness for the public, the pandemic has also put a stop to public activities such as seminars and events. Hence, we look to leveraging our social media as an outreach platform.

Below are some useful tips and suggestions on how to effectively reach out to your target audience on social media.

Visual content

Content with colourful and creative visual is more appealing to social media users. Colours and design also projects visual identity. This visual identity reflects an organization's corporate identify. Therefore, sufficient time and resources need to be invested to ensure the identity represent organisation's vision and mission accurately and positively.

Infographics

Social media users are very receptive to infographics because they present facts in a simple, informative and attractive manner. Thus, take time to create your own on social media or share other infographics but be sure to tag the original source. It is also easy for social media users to share the information effectively.

Create short videos

Other than infographics and photos, users love to share funny videos on social media. Simple, catchy, and creative short videos can attract more followers as they are entertaining and engaging.

Different platforms require different approaches

Use different platforms to reach out to a variety of users. People use different social media channels for different purpose. For example, Twitter contents can be less formal than LinkedIn, which is a professional social media channel. TikTok attracts those who love music and dance.

Avoid posting the same content across all platforms

Not all content is suitable for every social media platform. Each social media platform has different characteristics and its own targeted demographic. If the content does not deliver value or strike a chord with your audience, it will not be shared. It is important to create a unique message alongside the information you wish to share.

Quality of Content

Ensure good quality and reliable content is shared on social media channels. Avoid sharing contentious materials that may flout the laws and regulations that will put your organisation and users in a risky situation.

Hashtags are a must

Social media rely on hashtags! Create a unique and easy to remember hashtag but make sure it is relevant to the awareness program. Some social media channels use hashtag as a search tool or to get a post trending and viral fast.

Avoid sensitive topics

Avoid sharing or commenting on sensitive topics such as politics or religion. Instead of awareness, it will draw unnecessary comments from the public and potentially could compromise an organization's image and reputation.

Blogging

Create a blog to share articles, stories, and public feedback to educate social media users on emerging trends and tips that will make their lives better. Blogs also serve as a platform for users to publish their articles to enrich the outreach resources. At the same time, encourage other bloggers to create their own content and share it on your organisation blog.

Respond on time

Whether it is a positive comment, a question, or a malicious comment, you need to respond rapidly and professionally on social media. Words travel fast, so negative comments can spread easily. Responding quickly to positive comments will also ensure your followers and public stay engaged.

Make Feedback a Priority

Social media users love commenting and criticizing online as they can remain anonymous. Pay close attention to the comments, shares, likes, etc. of your posts. You can gain a lot of insight into the diverse interests of your followers which can help shape your future strategy.

Get close to your followers

Get close to your followers, invite them to join activities such as online talks, training, or webinar, appoint them as ambassador and train them to be trainer etc. Make your followers feel like they are part of your community.

Offer give-aways and organize contests

A social media contest is a great way to gain followers and connect with your audience. People love to participate and share contest posts with others. It is one of the best tools to expand your reach and increase awareness. Always remember to generate buzz and excitement about your contest on social media.

Conclusion

Social media can be an effective channel to drive public awareness. However, the content needs to be attractive and insightful to users. Always ensure your message is unique and will be shared by users. Last but not least, visual content in social media should be rich and captivating. After all, we are now living a digital world.

References

1. <https://www.agilecrm.com/blog/increase-brand-awareness-social-media/>
2. <https://ducttapemarketing.com/visual-brand-strategy/>
3. <https://blog.hubspot.com/agency/develop-brand-identity>
4. <https://blogs.spectrio.com/building-out-your-visual-brand>
5. <https://www.canva.com/learn/20-easy-tips-build-visual-brand-identity/>

Disruption, Obnoxious, Exploitation: Web Defacement Based On MyCERT Case Study

By | Faiszatulnasro binti Mohd Maksom, Kilausuria binti Abdullah, Nur Sarah binti Jamaludin & Izzatul Hazirah binti Ishak

Introduction

Website defacement is an attack on a website that changes the visual appearance of a website. The attacker may replace the content on the hosted website with their own messages. The intention is to let users know that they have compromised the web server.

What is the motive behind this? There are many reasons for this but more frequently, it is politically or socially driven. They will alter or create obnoxious content to express their anger or dissatisfaction about a particular individual or organization.

Often times, a cyber-attack will take advantage of an existing vulnerability in a targeted website. This could cause damage to the reputation of the website owner and compel it to regain users' trust.

Trends

The following section discusses the data extracted from MyCERT incident reports through its reporting channel i.e. CYBER999 and explains the motives behind some of the latest web defacement incidents in Malaysia.

Figure 1 shows that over a 5-year period, the highest web defacement incidents occurred in 2016 while the lowest in 2018. However, our analysis will focus on data that was reported in 2019.

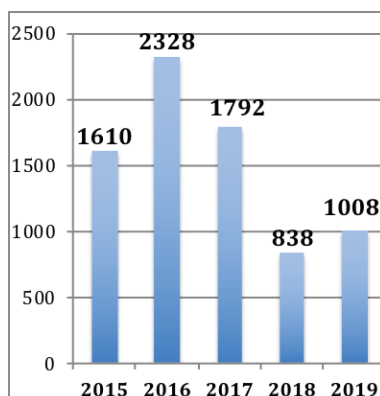


Figure 1: Data is based on MyCERT reports which represent trends over a 5-year year period.

TLD	Total
com.my	327
com	243
my	124
gov.my	72
edu.my	59
org.my	21
net.my	8
org	7
net	6
info	2
tv	2
biz	1

Table 1: Top level domains (TLD) targeted in 2019

As shown in Table 1, the most targeted TLD is .com.my (38%), .com (28%), .my (14%), .gov.my (8%) and .edu.my (7%).

Servers such as Apache, LiteSpeed and Microsoft-IIS/8.5 are the most popular servers targeted for website defacement.

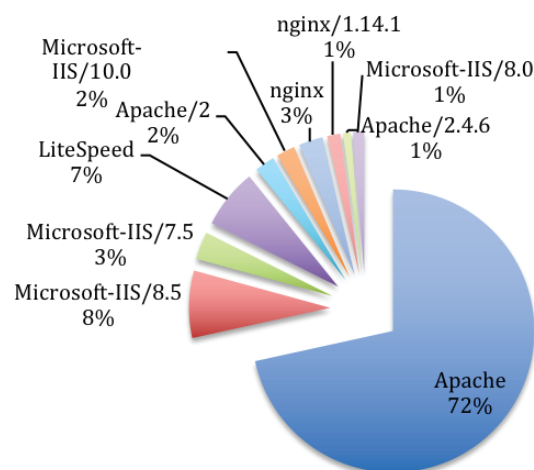


Figure 2: Top 10 targeted servers

Based on observation, 82 incident reports which contained sub domains comprising multiple URLs within the same domain, have been vandalized. It is likely the parent website (domain) has the same vulnerabilities as the sub domains.

Quite a few domains experienced re-defacement within the same year. Re-defacement means the same sites have been defaced repeatedly. This could be attributed to unpatched operating system or application not properly removed. Defacers will revisit the defaced website to check on existing vulnerabilities and execute the same attack method.

There are also cyber-attacks triggered by hacktivists from regional countries due to differences in opinions. But more often than not, website defacement is driven by the need of those who crave for attention.

Looking at the statistics on web defacement incidents and based on analysis study of incidents that we received, there are a few notable trends on how defacement is delivered. The hackers are always trying to exploit vulnerabilities that are not patched properly. From the log analysis, the website vulnerabilities vary depending on exploitability, detectability and impact on software.

Defacers will use the lowest or any advanced programming tools such as Perl, PHP, Python scripts to exploit the security vulnerabilities. The most popular framework or website popularity is also one of the targeted by the defacers. Web sites which use Content Management Systems (CMS) like WordPress, Joomla, and Drupal are the most commonly accessed website online and hence, they are among the most common hacking targets on the Internet. All websites are subject to vulnerability regardless of open-source or proprietary software. This is where website administrator should take preventive measures to minimize risk of exploitation.

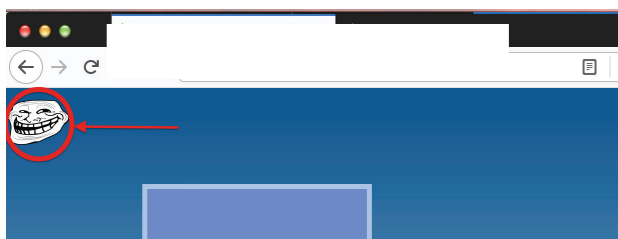


Figure 3: The defacer's image at the corner of the vandalized website

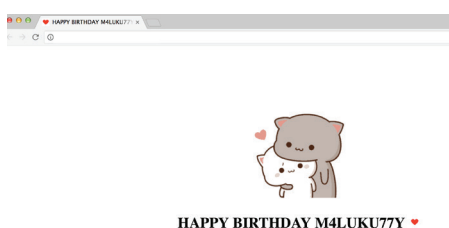


Figure 4: Message left by the defacer for birthday wish

There are various CMS plug-ins and themes, which may be prone to attacks. It may get worse if the website administrator fails to fix and patch the latest updates of CMS plugins and themes.

Most servers' platforms are using Linux and Windows. Each platform has its own limitations depending whether the System Administrator adheres to the SOPs or best practices in securing both platforms. In general, few exploits on Linux (or any Unix) lead to total compromise of the system. Exploits on Windows tend to allow remote execution of code and usually with total administrator privilege, infection with trojans that replicate themselves through the mailer system and infected browsers.

SQL Injection attack is one the most common website hacking techniques. Deploying SQL injection method, a defacer can manipulate the user supplied data, log in to an application without having valid credentials and potentially expose the back-end database. File inclusion attack refers dynamically to external scripts attempting to exploit the referencing function in an application to upload malware (e.g., backdoor shells) from a remote URL located within a different domain or local domain. The consequences of a successful file inclusion attack include information theft, compromised servers and site takeover that results content modification.

From a business perspective, website defacement can result in service disruption, leading to potential data breach, increased cost depending on extent of vulnerabilities, and compromised business reputation.

Best Practices

To reduce the vulnerability to cyber-attack or malicious infection, certain precautions have to be put in place such as using the latest version of applications, operating systems and hardware. Always update your anti-virus software on a regular basis and set the sensitivity heuristic engine. Enable daily scanning of all files in order to prevent further infection within the network.

A full assessment of all critical servers and applications is recommended to further ensure that there are no remaining vulnerabilities and backdoors. This should also include 3rd party code review to identify potential vulnerability in existing script. For example, validate or sanitize user input by including parameter checking before storing information into the database.

In addition, perform regular checks on all current user accounts and terminate inactive user accounts. As a safety measure, login and password for all servers, including database and user accounts must be refreshed at least once every six months. Please do not use a weak password which can leave you vulnerable to hackers.

Last but not least, awareness programs should include a user guide on malware incident prevention which, can help to reduce the frequency and severity of malware incidents. Every end-user needs to be aware of ways in which malware enter and infect hosts; the risks that malware poses; and the respective roles in preventing incidents, with an emphasis on avoiding social engineering attacks.

Conclusion

Despite awareness and advisories on website defacement, the total number of compromised websites in Malaysia remains high based on the statistics above. An attacker will always find a way to compromise a website. There is no concrete evidence why certain websites are targeted. Some hackers deface a website for political or religious reasons; while others do it just for fun. The defacer will always target low hanging fruits.

Keeping up with regular updates is the best way to ensure your website stays secure. Be aware of the latest security patches and remember to apply best practices when maintaining your website.

COVID-19 Theme Cyber Threats In Malaysia

By | Farah binti Ramlee, Sarah binti Abdul Rauf, Nurshuhada binti Mahfuz & Nur Mohammad Kamil bin Mohammad Alta

Introduction

COVID-19 is taking a toll on the world causing widespread illnesses and economic despair. It has affected most businesses in Malaysia, particularly the small and medium enterprises (SMEs). On 18 March 2020, the Malaysian government issued a Movement Control Order (MCO) in a bid to curb further outbreaks of Covid-19. All citizens were required to stay at home.

As a result, businesses had to halt brick and mortar operations, and turn to online platform to continue trading. During the early stages of MCO, consumers in Malaysia had to change their lifestyles and daily routines including shopping online for daily necessities.

The World Health Organization (WHO), governments and authorized organizations started to broadcast information about the virus to educate the public through the Internet, social media and other digital platforms. The pandemic has forced the public to resort to digital platform in seeking information and latest news. As more Malaysian went online, cybercriminals seized the opportunity with new cyber-attack techniques to exploit the sudden surge in online traffic. Since the MCO commenced on 18th March 2020, Cyber999 saw a rise in the number of incidents reported and most of them are coronavirus themed cyberattacks.

Overall, we received about 73 cases related to COVID-19 theme as of May 14th, 2020. From the chart, phishing incidents using the COVID-19 theme was the most dominant with 74% incidents reported. About 10% of all reported incidents were related to fraud purchases, while online scams constituted 8%. Further down, about 4% reported were spams and 2% were malicious code botnet CnC. Malware and content related-intellectual property categories made up the remaining 1%.

Sample of incidents related to COVID-19 theme

The most reported incidents related to Covid-19 theme are phishing and online scam. Most of these sites contained Covid-19 related topics in the URL, false information about Covid-19 in the web content or fake financial aid related to this pandemic. The sites will dupe victims to give their username, password, collect other confidential information as well as deceive victims that they are giving funds to a legitimate organisation. In fact, Cyber999 reported the matter to the respective hosting provider and ISP which hosted the phishing website and since then, most of the sites were taken down.

Incidents reported to Cyber999

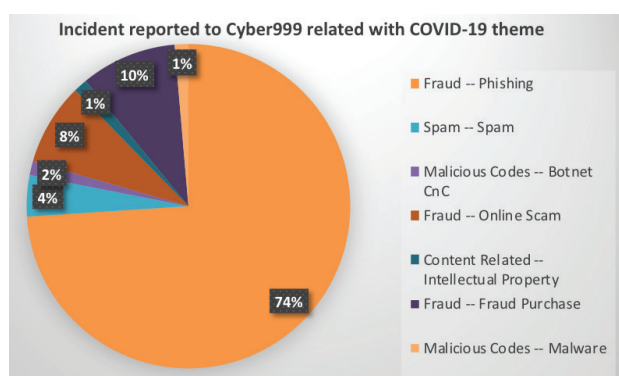


Figure 1: Incident Categories related to COVID-19 theme

Sample 1: Phishing Website

The phishing website below attempted to phish Bank of Ireland 365 online systems.

URL: hxxps://autodiscover.gov-ca-covid19[.]org

IP Address: 101.99.xx.xx

Not secure | autodiscover.gov-ca-covid19.org

Bank of Ireland 365 online

Welcome to 365 online

Secure Login

Please enter your **User ID**

Enter your **Last 4 digits of your card**

Please enter the **Phone number** on file

Enter your **six digits PIN**

Enter the **Date of birth**

Continue

Forgot details Register

Figure 2: Sample of phishing website COVID-19 theme hosted in Malaysia

The phishing website was hosted under a Malaysian hosting provider although it targeted users from Ireland. The website requested victims to key in information such as user ID, last 4 digits of their bank card, phone number, 6-digit pin set by victim with the bank and date of birth. Once the victim entered his or her personal details, it was redirected to cybercriminals who used the information to commit malicious activities.

Sample 2: Online Scam Website

The reported fake website impersonated a Non-Profit known as “GiveDirectly, Inc.” which was allegedly set up for charity purposes. The site claims to collect funds to aid families impacted by COVID-19 in the U.S.

GiveDirectly: Send money to p... x

Dangerous | http://givedirectly-covid19-emergency-fund.ibonline.digital/

GiveDirectly Give Now

We're responding to COVID-19 in the U.S.

By doing what we always do — giving cash.

Give now

We're delivering cash to families impacted by COVID-19 in the U.S.

We're responding to this crisis by doing what we've done for a decade: delivering cash. Each household will receive \$1k, and we expect the main constraint on how many we can reach will be how much we can raise.

We're beginning by targeting vulnerable households enrolled in SNAP, living in the areas hardest hit by COVID-19.

In partnership with [Propel](#), we're able to identify vulnerable households on SNAP. To date, we've paid 1,204 households across 17 U.S. states. Donations to our [general U.S. response fund](#) are distributed across the United States to areas with the greatest need; you can also donate to city-specific funds if you'd like to give to a particular geographic region. We currently have funds set up for the [Bay Area](#), [Las Vegas](#), [New York City](#), and [Seattle](#).

As we scale the program, we're focusing on targeting other populations in need who could be missed or underserved by other programs. We'll update payment size and structure as we learn more about the need.

Figure 3: Sample of the fake website using COVID theme leads to PayPal Phishing

URL: <http://givedirectly-covid19-emergency-fund.ibonline.digital/>
 IP address 111.90.xxx.xx

Unfortunately, the fake website was also hosted under a Malaysian hosting provider although it targeted users from U.S. When a user clicked the "Give Now" button on the fake website, it transferred the individual to a PayPal Donate page – a real PayPal page, but falsely claiming to be funding GiveDirectly.

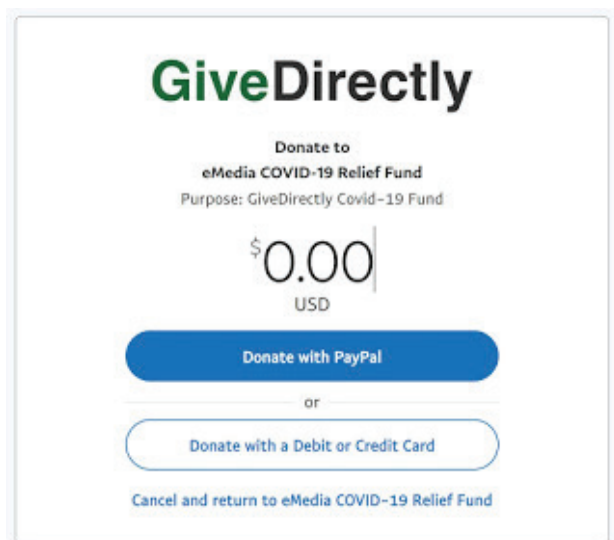


Figure 4: Cybercriminal PayPal's page

As such, victims were actually making authorized transactions to a false account using PayPal services.

Sample 3: Fraud Purchase

Ever since the Ministry of Health Malaysia advised citizens to practice the '3W' Wash, Wear & Warn (3W), the demand for face mask and hand sanitizers has reported a notable spiked. Cybercriminals wanted to profit from the Covid-19 pandemic by creating fake ads to sell the items on social network sites such as Facebook. Cyber999 received a surge of incidents related to Covid-19 products as shown below.

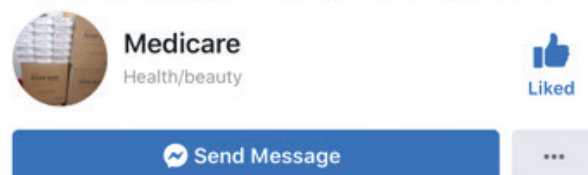


Figure 5: Sample of scam involving face mask

Sample 4: Malware hosting

One of the malware activities employing the COVID-19 theme is a compromised website maintained by a legitimate owner and hosting provider in Malaysia. The website hosted a malicious program which disguised as an acrobat reader icon application but actually contained malware shown below.

URL: hxxps://www.kxxxxx.com.my/wp-admin/images/Covid-19 Check.exe
 IP: 103.6.xxx.xx

The url link downloads a windows executable file name Covid-19 Check.exe and it appears to be COVID-themed ransomware as shown in Figure 6 below.



Figure 6: The malware disguise using Acrobat Reader icon

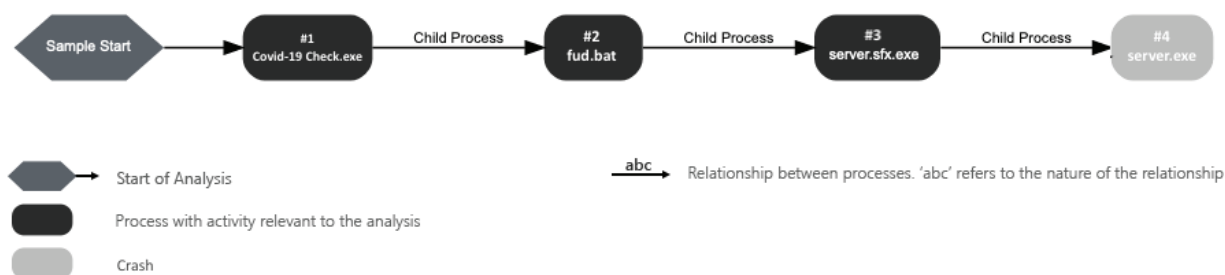


Figure 7: Execution process of the malware

Once a person clicks on the icon, a batch script named **fud.bat** calls to **server.sfx.exe** and provides a password to extract its content. **Server.sfx.exe** is a zip package in executable format with password protect. After extraction, the malware calls another executable named **server.exe** which is the actual binary of the ransomware.

Once activated, the ransomware will drop a ransom note into victim's Desktop folder. The ransom note is named as "Name of your explain.txt".

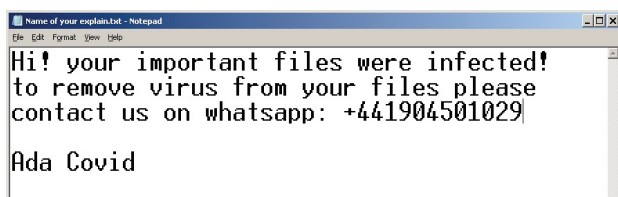


Figure 8: Sample ransom note

However, the sample requires **.Net Framework 4.0** to be installed in order for it to run properly. Cyber 999 has escalated the matter to the respective owner of the website and the URL is no longer available for public view.

Impact

The impact of cyber incidents linked to Covid-19 theme varies. Fraud and related offences can often be devastating as it will cause significant financial loss for victims. It also enables cybercriminals to collect personal identifiable information of victims for their own malicious intent.

Conclusion

Cybersecurity is designed to prevent unauthorized data access and protect users from falling prey to cybersecurity scams which often threatens the confidentiality, integrity and availability of digital information on the Internet

and the entire cyber ecosystem. The coronavirus pandemic has forced many companies to implement remote working. As home-based working becomes the new norm, the corporate world will rely on technology more than ever.

Even with the significantly reduced number of daily reported cases, we believe that the "war" against the spread of Covid-19 may not end until a vaccine is found. Cybercriminals will continue to exploit the situation heavily for financial gain. During the MCO, MyCERT published regular safety messages and advisories to increase public awareness and knowledge on cybersafety.

1. MA-785.042020: MyCERT Alert - Bogus Scam Email <https://www.mycert.org.my/portal/advisory?id=MA-785.042020>
2. MA-782.042020: MyCERT Advisory - Online Video Tele-conferencing (VTC) Application Security Guidelines <https://www.mycert.org.my/portal/advisory?id=MA-782.042020>
3. MA-780.032020: MyCERT Advisory - Work-From-Home : Security Advice & Best Practices <https://www.mycert.org.my/portal/advisory?id=MA-780.032020>
4. MA-779.032020: MyCERT Advisory - COVID-19 Cyber Scams and Campaigns <https://www.mycert.org.my/portal/advisory?id=MA-779.032020>

References

1. <https://any.run/report/7871acfc6f5e839cb764fd120ee9cec7585ead0d4f4e5b1c526baa6a2b936d29/a2f8fcb5-5df4-4fd5-9ebd-fd7a406abfec>
2. <https://hybrid-analysis.com/sample/7871acfc6f5e839cb764fd120ee9cec7585ead0d4f4e5b1c526baa6a2b936d29?environmentId=100>
3. https://www.vmrays.com/analyses/def6c0cbbce/report/behavior_grouped.html
4. <https://twitter.com/jorgemieres/status/1244300732435697664?lang=en>

BLOCKCHAIN: Beyond The Cryptocurrency

By | Isma Norshahila binti Mohammad, Hazlin binti Abdul Rani & Muhammad Syazwan Fizani bin Sahran

Blockchain and Cryptocurrency

Are blockchain and cryptocurrency the same thing? Despite ongoing discussions, people often confuse blockchain and cryptocurrency. Part of the confusion surrounding "what is blockchain" versus "what is cryptocurrency" is due to the terminology used. The word blockchain formed from its informal definition which is "chain of blocks" while cryptocurrency is a sort-of-portmanteau of "cryptographic currency".

Basically, blockchain is the platform which brings cryptocurrencies into play. Blockchain is the technology which serves as the network's distributed ledger. This network provides the means to transact and allows transferring of value and information. Cryptocurrencies are the tokens used within these networks. It is also seen as tool on blockchain that serves as a resource or utility function. Other times, they are used to digitize an asset's value. In essence, blockchain refers to the platform, while cryptocurrency is the application that uses the platform.

Blockchain as a Technology

Blockchain technology is far broader than just cryptocurrencies like bitcoin. The consistent levels of reliable security found in public cryptocurrencies has shown to the world that this new wave of blockchain technologies can provide very similar efficiencies and intangible technical advantages to what the internet has done.

A blockchain is a distributed, peer-to-peer network database of all transactions. By using this technology, participants can validate transactions without having to have central clearing authority. Potential applications may include transfers of money, settling trades, voting, and many other things.

A blockchain is a constantly growing collection of digital records in packages (called blocks) that are connected and protected using cryptography. These digitally recorded "blocks" of data are stored in a linear chain. Each block in the chain that contains data (e.g. bitcoin

transaction), is cryptographically hashed, and time stamped. This blocks of hashed data depends on the previous-block in the chain, ensuring that all data in the "blockchain" itself has not been changed and altered.

How blockchain actually works

In the context of cryptocurrencies, a blockchain consists of a secure chain of blocks. Each one storing a database of previously confirmed transactions. Since the blockchain network is maintained by a multitude of computers distributed around the world, it acts as a decentralized database (or ledger). This means that each participant (node) holds a copy of the blockchain data and interact with each other to ensure that they are all on the same page (or block).

Therefore, blockchain transactions take place within a peer-to-peer global network and this is what makes Bitcoin a decentralized digital currency that is borderless, censor-resistant. In fact, most blockchain systems are considered to be untrustworthy because they do not require any kind of trust. There is no single authority in control of Bitcoin.

A central part of almost every blockchain is the process of mining, which relies on hashing algorithms. Bitcoin uses the SHA-256 algorithm (Secure hash algorithm 256 bits). It takes an input of any length and generates an output that will always have the same length. The output produced is called a "hash" and in this case, is always made of 64 characters (256 bits).

Therefore, the same input would result in the same output, no matter how many times the cycle is repeated. But if a minor change is made to the input, the output changes completely. As such, hash functions are deterministic and most of them are designed as a one-way hash function in the cryptocurrency world.

Being a one-way function means that it is almost impossible to calculate what was the input from the output. One can only guess what the input was, but the chances of getting it correct are extremely low. This is one of the reasons why Bitcoin's blockchain is secure.

Now that we understand what the algorithm is doing, Figure 1 illustrates how a blockchain works with a simple example of transaction and explains as follows:

- i. Someone requests a transaction.
- ii. The requested transaction is broadcast to a peer-to-peer network consisting of computers, known as nodes.
- iii. The network of nodes validates the transaction and the user's status using known algorithm.
- iv. Once verified, the transaction is combined with other transactions to create a new block of data for the ledger.
- v. The new block is then added to the existing blockchain, in a way that is permanent and unalterable.

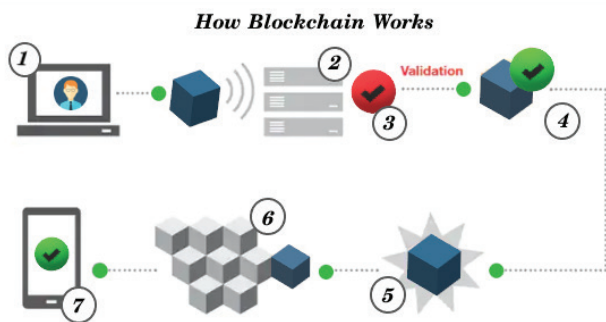


Figure 1 How Blockchain Works

Different Types of Blockchain Technologies

Although blockchain is considered to be a fundamental technology, other exciting innovations such as dApps and smart contract have been developed from it.

i. dApps

Decentralized applications (dApps) are digital applications or programs that exist and run on a blockchain or P2P network of computers instead of a single computer and are outside the purview and control of a single authority.

A standard web app, like Twitter, runs on a computer system which is owned and operated by an organization giving it full authority over the app and its workings. There may be multiple users on one side, but the backend is controlled by one single organization.

dApps can run on both a P2P network as well as a blockchain network. For example, BitTorrent, Tor (The Onion Router), and Popcorn Time (services such as Netflix) are examples of applications that run on various computers that are part of a P2P network where there are multiple participants on all sides. Some are consuming the content, some are feeding or seeding the content, while others are simultaneously performing both functions.

In the context of cryptocurrencies, dApps exists and runs on the blockchain network in a public, open source, decentralized environment and is free from control and interference from any single authority.

For example, a developer can create a Twitter-like dApp and put it on a blockchain where any user can tweet messages. Once posted, no one – including the app creators – can delete the tweets. Editing may be possible by the sender, but the original tweet would be retained forever. Figure 2 illustrates the difference between standard apps and dApps.

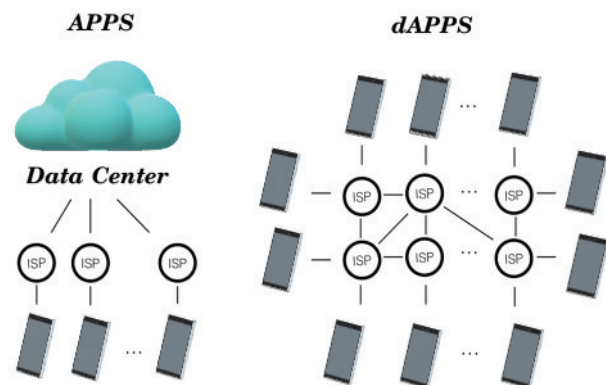


Figure 2 Difference between Apps and DApps

ii. Smart Contract

If you think of a contract, you are probably thinking of two people sitting together reading, agreeing and signing a piece of paper. The efficiencies brought about by the digitization of business, have inspired technologists to revise one of the most important components of modern day business – the contract.

The simple explanation of a smart contract is a computer program that functions as an agreement where the terms of the agreement can be pre-programmed with the ability to self-execute and self-enforce itself.

The main objective of a smart contract is to provide a superior system for contractual

agreements based solely on computer code as compared to what currently exists on the basis of old judicial procedures.

The origins and history of smart contracts is much older than bitcoin and dates back to the 1990s. The word 'smart contract' was first invented in 1994 by one of bitcoin's supposed developers, Nick Szabo, and refers to self-automated computer programs that can satisfy the terms of any contract.

The execution of a smart contract is the same as that of a standard contract – either the deal has been completed and enforced, or has not been fulfilled and has not been executed.

A practical description of a smart contract can be defined as a virtual self-execution agreement. Modern-day blockchain based smart contracts (also known as self-executing contracts, blockchain contracts, or digital contracts) uses Byzantine Fault Tolerant algorithms and Cryptographic hashing through blockchain technology decentralization methods. Since smart contracts are pure computer program code, the logic imputed to the code is extremely important. Smart contract logic is derived from the laws of human logic and the legal systems widely used in industry.

The combination of computer science concepts such as cryptography and distributed computing, combined with centuries-old judicial precedents, provides a self-sustaining and effective counterpart to legal agreements.

Real World Blockchain Applications

Blockchains are already being deployed in many industries such as identity management, finances, healthcare and many more. Below is a list of several real-world applications on blockchain, both globally and in Malaysia.

Global

- **REMME** has allowed more than two hundred million people to transmit information easily and affordably. It is a distributed encryption scheme aimed at replacing logins and passwords with SSL certificates that are stored on a blockchain.
- **Guardtime** – This company uses blockchain to create "keyless" signature systems that

are currently used to secure a million Estonian citizens' health records.

- **MedRec** – An MIT project involving blockchain electronic medical records designed to manage authentication, confidentiality and data sharing.
- **Webjet**: Online travel portal Webjet is developing a blockchain solution to allow empty hotel rooms to be efficiently tracked and traded, with payment routed to the network of middle-men sites involved in filling up last-minute vacancies.
- **STORJ.io** – Distributed and encrypted cloud storage which allows users to share unused hard drive space.

Malaysia

- **WAQF**: Develop by Finterra Technologies Sdn Bhd, The FINTERRA WAQF Chain is the world's first and only platform to develop a blockchain-based solution for WAQF charity, Islamic investment, and peer-to-peer loans
- **Degree verification system**: An online education verification system which leverages on blockchain technology to verify academic certificates.
- i. **Valid8**: A QR Code-based authentication system developed by Universiti Malaysia Pahang. It is used to validate the authenticity of graduation certificates where the data is stored in a blockchain.
- ii. **E-Scroll**: This project is led by UniDLT - Malaysia's Public University Consortium for Blockchain. Every diploma or certificate is tagged with QR codes linked to the blockchain in order to authenticate and verify the diplomas/certificates.
- iii. **myBLOCKCERTS**: Universiti Sultan Zainal Abidin (UniSZA) produced a blockchain-based technology scroll to verify the authenticity of graduation scrolls and to prevent fake certificate issues.

Blockchain for Future

Where news about blockchain used to focus solely on its cryptocurrency uses, blockchain today imagines a future of unimaginable possibilities. Industries from finance and energy to artificial intelligence (AI) are constantly exploring new and exciting ways to use blockchain technology.

Here are four assumptions about the future of the blockchain:

- **Automotive** – Consumers could use the blockchain to control fractional ownership of autonomous cars
- **Financial services** – Faster, cheaper settlements can shave billions of dollars off transaction costs while enhancing transparency
- **Voting** – Using a blockchain code, voters can cast votes via smartphone, tablet or computer, resulting in immediately verifiable results
- **Healthcare** – Patients' encrypted health information could be shared with multiple providers without the risk of privacy breaches

[news.php?id=1780689](https://www.thestar.com.my/news/nation/2018/11/10/fake-degrees-wont-make-the-cut-with-escroll-system/)

11. Fake degrees won't make the cut with e-Scroll system. <https://www.thestar.com.my/news/nation/2018/11/10/fake-degrees-wont-make-the-cut-with-escroll-system/>

12. UMP the first public university in the country to use Blockchain Technology for cert validation for its 2,773 graduates. <http://news.ump.edu.my/convocation/ump-first-public-university-country-use-blockchain-technology-cert-validation-its-2773>

13. <https://www.forbes.com/sites/bernardmarr/2018/01/22/35-amazing-real-world-examples-of-how-blockchain-is-changing-our-world/#79cb3f7343b5>

References

1. <https://www.pwc.com/us/en/industries/financial-services/fintech/bitcoin-blockchain-cryptocurrency.html>
2. <https://blockchain.wtf/what-the-faq/blockchain-cryptocurrency-difference/>
3. <https://www.blockchaintechnologies.com/cryptocurrency/>
4. <https://www.blockchaintechnologies.com/smart-contracts/> X. Fan, K. Mandal and G. Gong. 2012. A Lightweight Stream Cipher for Resource-Constrained Smart Devices. CACR 2012-28 Technical Report.
5. https://www.cryptolux.org/index.php/Lightweight_Hash_Functions
6. <https://en.wikipedia.org/wiki/SHA-3>
7. N. Mouha, B. Mennink, A. V. Herrewege, D. Watanabe, B. Preneel and I. Verbauwhede. Chaskey: a Lightweight MAC Algorithm for Microcontrollers. <http://csrc.nist.gov/groups/ST/lwc-workshop2015/papers/session1-mouha-paper.pdf>
8. A. R. Chowdhury and S. DasBit. LMAC: A Lightweight Message Authentication Code for Wireless Sensor Network. <http://itra.medialabasia.in/data/Documents/DISARM/publications/15.pdf>
9. Jake Frankenfield: Decentralized Applications. <https://www.investopedia.com/terms/d/decentralized-applications-dapps.asp>
10. UniSA produces block-chained technology scroll. <http://bernama.com/en/>

Web Application Firewall Detection And Fingerprinting Tools

By | Nur Sharifah Idayu binti Mat Roh, Siti Fatimah binti Abidin & Nurul Syahirah binti Aspawi

Introduction

A web application firewall (WAF) is a special type of application firewall that applies specifically to web applications. WAF plays an important role in web security whereby it typically protects web applications from attacks such as SQL injection, cross-site scripting (XSS), file inclusion and security misconfiguration.



Figure 1: WAF diagram

Figure 1 shows the WAF basic diagram implemented on the target website [1]. So, how do we know if the website is implementing WAF or not? This article will elaborate the sample of three open-source tools; **WafW00f**, **Whatwaf** and **Nmap** which are used to identify and detect web application firewall (WAF) on the target website. Before a penetration tester starts to execute the testing, he or she must check if there is any WAF in place. This is because of the result of the attack can be affected, and there is a high possibility that the testing may not be successful due to WAF protection.

1. WafW00f

WafW00f is a well-known tool that detects web application firewall. That simple tool can discover the presence of a variety of WAF products. Although wafw00f may not be able to pin-point certain firewalls, the tool can still detect their presence. Let's examine a list of readily supported WAFs.

Command: `wafw00f -l`

```

WAFW00F - Web Application Firewall Detection Tool
By Sandro Gauci & Wendel G. Henrique

Can test for these WAFs:
Profense
NetContinuum
Incapsula WAF
CloudFlare
USP Secure Entry Server
Cisco ACE XML Gateway
Barracuda Application Firewall
Art of Defence HyperGuard
BinarySec
Teros WAF
F5 BIG-IP LTM
F5 BIG-IP APM
F5 BIG-IP ASM
F5 FirePass
F5 Trafficshield
InfoGuard Airlock
Citrix NetScaler
Trustwave ModSecurity
IBM Web Application Security
IBM DataPower
DenyALL WAF
Applicure dotDefender
Juniper WebApp Secure
Microsoft URLScan
Aqtronix WebKnight
eEye Digital Security SecureIIS
Imperva SecureSphere
Microsoft ISA Server
  
```

Figure 2: List of supported WAF by Wafw00f

Figure 2 lists 28 WAF products supported by Wafw00f tools [2]. When a penetration tester finds out the WAF used by the target website, then he or she can validate the WAF type using the next command.

Let's start to detect WAF on the target website.

Command: `wafw00f <target website>`

E.g 1: `wafw00f targethost.com`

```

root@kali:~# wafw00f
WAFW00F - Web Application Firewall Detection Tool
By Sandro Gauci & Wendel G. Henrique

Checking [redacted]
The site [redacted] is behind a Imperva SecureSphere
Number of requests: 9
root@kali:~#
  
```

Figure 3: WAF type detected on target website

Figure 4: WAF detected on target website

Figure 5: List of supported WAF type by Whatwaf

e-Security | Vol: 48 - (1/2020)
© CyberSecurity Malaysia 2020 - All Rights Reserved

```

[01:51:18][ERROR] you must install psutil first. pip install psutil to start mining XMR
[01:51:18][INFO] checking for updates
[01:51:19][WARN] It is highly advised to use a proxy when using WhatWaf, do so by passing the proxy flag (i.e. --proxy http://127.0.0.1:8080) or by passing the Tor flag (i.e. --tor)
[01:51:19][INFO] using User-Agent 'whatwaf/2.0.3 (Language=2.7.16; Platform=Linux)'
[01:51:19][INFO] using default payloads
[01:51:19][INFO] testing connection to target URL before starting attack
[01:51:21][SUCCESS] connection succeeded, continuing
[01:51:21][INFO] running single web application 'http://testhtml5.vulweb.com'
[01:51:21][WARN] URL does not appear to have a query (parameter), this may interfere with the detection results
[01:51:21][INFO] request type: GET
[01:51:21][INFO] gathering HTTP responses
[01:51:53][INFO] gathering normal response to compare against
[01:51:54][INFO] loading firewall detection scripts
[01:51:54][INFO] running firewall detection checks
[01:51:59][FIREWALL] Apache Generic
[01:51:59][FIREWALL] Shadow Daemon OpenSource (WAF)
[01:51:59][INFO] starting bypass analysis
[01:51:59][INFO] loading payload tampering scripts
[01:51:59][INFO] running tampering bypass checks
[01:56:18][SUCCESS] apparent working tamperers for target:
.....
(1) description: tamper payload by inserting random UTF-8 characters into the payload
example: AND 1hude31e<script>alert(4091d'test'&md74);</script>
load path: content.tamperers.randomunicode
.....
(2) description: tamper payload by mask the booleans with their symbolic counterparts

```

Figure 6: WAF type detected on target website

Figure 6 shows by using whatwaf tools, different WAF types protecting the target website can be identified. This is the reason why penetration tester needs to try out other tools as well for detecting WAF type. This will provide insights into how many WAF is implemented for the target website.

3. Nmap

Nmap is an open-source security tool for network exploitation, security scanning and auditing. Nmap is also capable of detecting WAF on the target website. There are two different scripts which can be used for WAF detection. One script will cover for detection and one script will cover for fingerprinting the WAF. Let's start to detect WAF for the target website.

Command 1: `nmap --script http-waf-detect <target website>`

E.g: `nmap --script http-waf-detect targethost.com`

```

root@kali:~# nmap --script http-waf-detect [redacted]
Starting Nmap 7.70 ( https://nmap.org ) at 2020-05-14 05:11 EDT
Nmap scan report for [redacted]
Host is up (0.036s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
[redacted]
http-waf-detect: IDS/IPS/WAF detected:
:80/?p4yl04d3=<script>alert(document.cookie)</script>
443/tcp   open  https
[redacted]
http-waf-detect: IDS/IPS/WAF detected:
:8080/?p4yl04d3=<script>alert(document.cookie)</script>
8443/tcp  open  https-alt
Nmap done: 1 IP address (1 host up) scanned in 62.94 seconds
root@kali:~#

```

Figure 7: WAF detected by Nmap tools

Figure 7 shows WAF is detected on the target website by Nmap tools [4]. The script is an automated malicious payload by Nmap to detect any changes in the response code and content of the target website.

Command 2: `nmap --script=http-waf-fingerprint <target website>`

E.g: `nmap --script=http-waf-fingerprint targethost.com`

```

root@kali:~# nmap --script=http-waf-fingerprint [redacted]
Starting Nmap 7.70 ( https://nmap.org ) at 2020-05-14 07:03 EDT
Nmap scan report for [redacted] (1.41)
Host is up (0.0023s latency).
Other addresses for [redacted] (not scanned): [redacted]:4700:10::6814:129 2606:47
:80:10::6814:29
Not shown: 997 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
[redacted]
http-waf-fingerprint:
Detected WAF
Cloudflare
[redacted]
443/tcp   open  https
8080/tcp  open  http-proxy
Nmap done: 1 IP address (1 host up) scanned in 53.77 seconds
root@kali:~#

```

Figure 8: WAF type fingerprint identified

Figure 8 shows WAF product is detected on the target website by Nmap tools [5]. The script of http-waf-fingerprint will return the identified product name.

Conclusion

Once the penetration tester knows whether the target website is protected by WAF/IPS/IDS, and what kind of WAF is protecting the target website, then he or she can proceed to get information on how to bypass the WAF. This can also help the penetration tester to learn more about WAF behaviour and try different methods or techniques to bypass the WAF and exploit any other web application weakness. It is an important process that must be done for web application testing during the information gathering phase to ensure the potential attack type is successful and the result is accurate. With this information gathered, penetration tester will develop an accurate attack scenario for their test cases according to ethical hacking.

References

1. <https://avinetworks.com/glossary/web-application-firewall/>
2. <https://github.com/EnableSecurity/wafw00f>
3. <https://github.com/Ekultek/WhatWaf>
4. <https://nmap.org/nsedoc/scripts/http-waf-detect.html>
5. <https://nmap.org/nsedoc/scripts/http-waf-fingerprint.html>

Mitigating Terrorism On Social Networks

By | Norhafizah binti Hashim & Ts. Dr. Zahri bin Yunus

Introduction

The Internet is the fastest growing and most extensively used digital tool for mass communication and information distribution in the world. It has removed all communication barriers. Today, we can search for information, read the news, watch television, or even listen to the radio via the Internet. Despite the enormous benefits that the Internet brings, there are certain parties who may use it as a means to communicate within terrorist organizations and disseminate information for terrorist purposes.

According to a recent study by Emarsys, an estimated 3.2 billion users – which equates to about 42% of the world's population – log in, peruse, and converse with friends on social media [1]. This staggering user base means that one can reach out to a vast population easily via social media. Social media also facilitates active interaction among its users regardless whether the content is positive or negative. In Malaysia, the number of active social media users has exceeded 22 million.

Facebook, Twitter, Instagram and WhatsApp have become essential tools in today's daily communication to interact with friends, family as well as different communities. Unfortunately, the speed and transparency in which information is being shared across social media platforms have increased dramatically and this often leads to information overload.

Reliability of Social Media as Source of News

Social media has now become a commonly accepted platform for disseminating information, launching campaign and propaganda. Yet, most of its content are not properly verified or officially confirmed with authorized sources. As such, news or information from social media can often cause misinformation.

Fake news spread easily via social media. Fake news is defined as a deliberate lie. It is content that is "picked up by blogs, retransmitted by hundreds of websites, cross-posted over thousands of social media accounts and read

by hundreds of thousands" that it effectively becomes "fake news" [2]. Content on social media, regardless of its authenticity, becomes real if people tend to believe them if they are delivered creatively and confidently. Fake news also tend to be shared due to its novelty appeal. Therefore, it is pertinent to identify the original sources and authors of information before sharing it on social media.

Why Terrorist Use Social Media

Content sharing has become a norm in social media. Users are also accustomed to voicing their opinions freely over their social media account to reach and engage with their followers. This "freedom" enables a new level of networking among a community, allowing terrorists to easily identify prospects to spread their ideology or recruit.

For years, terrorists have been using Internet resources to communicate and disseminate propaganda through dedicated forums. Today, with rapid technological advancements, they have shifted their focus to social media to advance their interest via online discussions, fundraising and campaigns to spread propaganda, drive recruitment, conduct training and gather intelligence. As social media is cost effective, easily accessible and pervasive, they can now easily establish an international network to plot attacks.

Incidents Caused by Misuse of Social Media: Case Studies

Social media networks can be easily exploited by cyber-criminal groups, state enemies, extremists, and terrorists to launch cyber propagandas to undermine people's perception.

Arab Springs was a series of protests that took place in the Middle East [3]. It was sparked on 18 December 2010 in Tunisia, Egypt and Libya. The civil uprising later spread to Bahrain, Algeria, Yemen, Oman and Syria. Protests were staged through civil resistance that involved strikes, demonstrations, marches, and rallies.

Social media was relied upon to organise, communicate, and raise awareness in the face of state attempts at repression and Internet censorship. Social media users in the Middle East facilitated the entire world in witnessing this revolution. The revolutionaries utilized social media effectively to spread their messages to all corners of the world.

In China, a small group of protesters managed to spark a demonstration despite the government's order to arrest users of other services that has been widely blocked in China. The demonstration used Twitter as their platform to spread information to those who can bypass the Internet censors [4]. This mysterious online call was dubbed "**Jasmine Revolution**" and took place on Sunday, 27 February 2011. As a result, the protest venue in Beijing was sealed off by police and the government swiftly moved to block the word "jasmine" on popular social networking sites and chat rooms.

In November 2014, ISIS terrorist group kidnapped and executed five foreigners and recorded horrific videos before posting it online [5]. These gruesome videos, which were made public and addressed to the government, captured footage of the hostages speaking a few words and then brutally killed in front of the camera. This online threat terrorised the public and caused chaos among many nations.

Social media features are designed to fulfil and fuel users' demands and interest. For example, "Go live" feature on Facebook and several other social media platforms, enable recording of live interaction among the user and its followers. The Christchurch mosque shootings attacks during Friday Prayer on 15 March 2019 in New Zealand was an example of such misuse to feature terrorism and hatred activities [6]. As social unrest become more prominent across nations, people with alternative points of view on issues such as race, religion, lifestyle, orientation, politics, and social organisation took advantage of social media's freedom to express their frustrations.

Measures in Mitigating Criminal Activities in Social Media

Below are several proposed strategies to fight criminal activities in social media:

1. Hashing

If someone discovers a terrorist content in social

media, they can place a unique identifier on the image or video, called a "hash," into a database, which helps others find it on their sites and take it down quickly. Both Facebook and Twitter said the systems have helped them remove more than 90% of ISIS and al-Qaeda content before any users spotted it.

2. Halt encrypted messaging

There are rumours alleging that Facebook is considering encrypting user messages, which make it un-viewable even to the company itself. Should Facebook proceed with such move, it would be impossible to track and follow terrorists, as well as monitor other illegal activities such as human traffickers and illegal drugs. Therefore, it is important for Facebook to reconsider encrypting messages.

3. Specify definition of terrorist content

Facebook defines a terrorist organisation as "any non-governmental organisation that engages in premeditated acts of violence against persons or property to intimidate a civilian population, government, or international organisation in order to achieve a political, religious or ideological aim." Twitter says it monitors and removes posts from sources that fall under "national and international terrorism designations," as well as from "violent extremist groups" that self-identify as extremist, engage in violence, and target civilians.

Conclusion

The Internet has emerged as an extremely important conduit for information and communications. However, the digital space should not become a playground for terrorism. Internet governance is essential and it must be enforced by all stakeholders. It is a collective responsibility of the Government and private sector organizations to establish standards, policies, rules and enforcement in securing the cyber space from acts of terrorism.

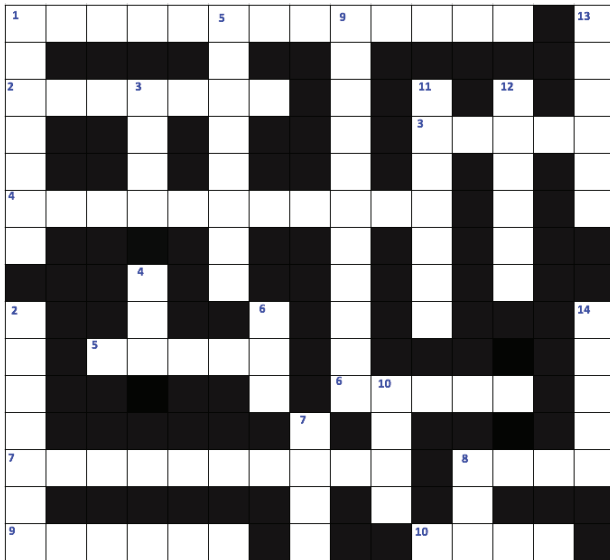
CyberSecurity Malaysia, an agency under Ministry of Communications and Multimedia Malaysia has initiated a program through CyberSAFE (Cyber Security Awareness for Everyone) to educate and enhance community awareness on technological and social issues faced by Internet users, particularly on the risks they face online. This initiative is set to increase awareness on cyber security.

References

1. *Top 5 Social Media Predictions for 2019.* URL Ref: <https://emarsys.com/learn/blog/top-5-social-media-predictions-2019/>
2. *Fake news - Drilling the Democracy.* URL Ref: <https://www.varindia.com/news/fake-news--drilling-the-democracy->
3. *Arab Spring.* URL Ref: [https://en.wikipedia.org/wiki/Arab_Spring#:~:text=The%20Arab%20Spring%20\(Arabic%3A%20%D8%A7%D9%84%D8%B1%D8%A8%D9%8A%D8%B9,starti ng%20with%20protests%20in%20Tunisia.](https://en.wikipedia.org/wiki/Arab_Spring#:~:text=The%20Arab%20Spring%20(Arabic%3A%20%D8%A7%D9%84%D8%B1%D8%A8%D9%8A%D8%B9,starti ng%20with%20protests%20in%20Tunisia.)
4. *Calls for a 'Jasmine Revolution' in China Persist.* URL Ref: <https://www.nytimes.com/2011/02/24/world/asia/24china.html>
5. *Terrorism and social media.* URL Ref: https://en.wikipedia.org/wiki/Terrorism_and_social_media
6. *The Christchurch Attacks: Livestream Terror in the Viral Video Age:* URL Ref: <https://ctc.usma.edu/christchurch-attacks-livestream-terror-viral-video-age/>

CyberSecurity : Crossword Puzzle

By | Zulkifli bin Musnman & Muhammad Zulasyraf bin Mohd Senail



Across

1. A document proving that someone is qualified for a particular specialist
2. Sarah maintained no Face Book or Twitter account, nor could Betsy locate her on any other social _____ sites
3. What do we call this symbol "@"
4. Hackers to damage or destroy a computer network or system
5. Stuxnet, Duqu, Flame, Wiper, I Love You, code red, NIMDA, Heartbleed, Shellshock, Bash bug
6. Mail that's electronically transmitted to you via computer
7. Passing through a complex mathematical process
8. Unsolicited commercial e-mail
9. It houses information and responds to requests for information
10. A regularly updated website or web page, typically one run by an individual or small group, that is written in an informal or conversational style

Down

1. To join, link, or fasten together; unite or bind:
2. A person who circumvents security and breaks into a network, computer, file, etc., usually with malicious intent:
3. Stringlike piece or filament of relatively rigid or flexible metal, usually circular in section
4. Form of user interface that allows users to interact with electronic devices through graphical
5. Systems designed to protect and secure a computer network—everything from a commercial web service to your home WiFi network—from external security risks
6. Internet Service Provider
7. A computer network administration software utility used to test the reachability of a host on an Internet Protocol (IP) network
8. Cryptographic protocols designed to provide communications security, Secure Sockets Layer
9. Is a computer program used to prevent, detect, and remove malware
10. List of options or commands presented to the user of a computer or communications system
11. Component of the deep web that describes the wider breadth of content that does not appear through regular internet browsing activities
12. Form of Internet access that uses the facilities of the public switched telephone network (PSTN) to establish a connection
13. An indicator used to show the current position for user interaction on a computer monitor or other display
14. Device which connects computers or computer systems to the internet

Senario Keselamatan Siber Sewaktu 'Perintah Kawalan Pergerakan COVID-19'

By | Mohd Shamil bin Mohd Yusoff

Pengenalan

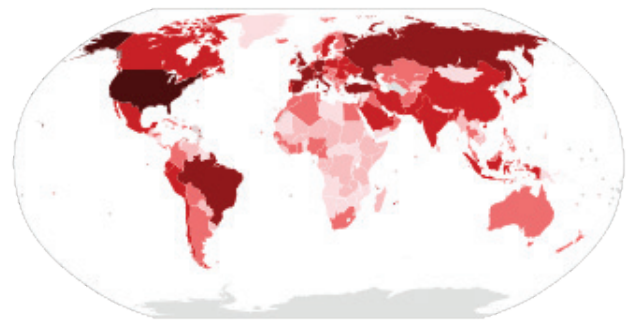
Tahun 2020 membuka tirai dengan satu lembaran sejarah apabila dunia dikejutkan dengan penularan virus yang dikenali sebagai *Novel Coronavirus* atau COVID-19. Wabak ini telah mengejutkan penduduk sejagat, di mana ia menjadi pandemik dan merebak dengan pantas serta meragut ratusan ribu nyawa. Sehingga 30 April 2020, statistik Pertubuhan Kesihatan Dunia (WHO) mencatatkan lebih 3.2 juta penduduk dijangkiti COVID-19, manakala jumlah korban pula mencapai angka lebih 220 ribu nyawa.

CORONA VIRUS DISEASE 19 (COVID-19)											
Jumlah keseluruhan kes: Total cases Dunia / Worldwide		Jumlah kematian keseluruhan: Total deaths Dunia / Worldwide		Jumlah kes sembuh: Total recovered cases Dunia / Worldwide		Negara yang terlibat: No. of countries involved		Jumlah kes sembuh: Total recovered cases Malaysia			
3,204,762		227,849 (7.11%)		982,902 (30.67%)		184		4,171 (69.49%)			
Negara Country	Bil. kes No. of cases	Bil. kematian No. of deaths	Negara Country	Bil. kes No. of cases	Bil. kematian No. of deaths	Negara Country	Bil. kes No. of cases	Bil. kematian No. of deaths	Negara Country	Bil. kes No. of cases	Bil. kematian No. of deaths
Amerika Syarikat	1,040,488	60,999	Bangladesh	7,103	163	Guinea	1,351	7			
Spain	236,899	24,275	Australia	6,752	91	Ivory Coast	1,238	14			
Italy	203,591	27,482	Republik Dominika	6,652	293	Bolivia	1,110	59			
Perancis	166,543	24,121	Serbia	6,630	125	Djibouti	1,077	2			
United Kingdom	166,441	26,166	Panama	6,378	178	Tunisia	980	40			
Jerman	161,539	6,467	Colombia	6,211	278	Senegal	882	9			
Turki	117,589	3,081	Malaysia	6,002	102	Latvia	858	15			
Rusia	106,498	1,073	Afrika Selatan	5,350	103	Cyprus	843	15			
Iran	93,657	5,957	Mesir	5,268	380	Honduras	771	71			
China	83,944	4,637	Finland	4,906	206	Albania	766	30			
Brazil	79,685	5,513	Maghribi	4,321	168	Kyrgyzstan	746	8			
Kanada	52,865	3,155	Argentina	4,285	214	Andorra	743	42			
Belgium	47,859	7,501	Algeria	3,848	444	Lubnan	721	24			
Belanda	38,998	4,727	Moldova	3,771	111	Costa Rica	713	6			
Peru	33,931	943	Luxembourg	3,769	89	Niger	713	32			
India	33,062	1,079	Kuwait	3,740	24	Sri Lanka	649	7			
Switzerland	29,407	1,716	Kazakhstan	3,273	25	Burkina Faso	641	43			
Ecuador	24,675	883	Thailand	2,954	54	Uruguay	630	15			
Portugal	24,505	973	Bahrain	2,921	8	Guatemala	585	16			
Arab Saudi	21,402	157	Hungary	2,775	312	Somalia	582	28			
Sweden	20,302	2,462	Yunani	2,576	139	San Marino	563	41			
Ireland	20,253	1,190	Oman	2,348	10	Georgia	539	6			
Mexico	17,799	1,732	Afghanistan	2,171	64	Kosovo	510	12			
Singapura	16,169	14	Armenia	2,066	22	Congo (Kinshasa)	500	31			
Israel	15,870	219	Croatia	2,062	67	Mal	482	25			
Pakistan	15,759	346	Uzbekistan	2,017	9	Tanzania	480	16			
Austria	15,452	584	Iraq	2,003	92	Malta	463	4			
Chile	15,135	216	Cameroon	1,832	61	Jordan	451	8			
Japan	13,965	425	Iceland	1,797	10	Taiwan	429	6			
Belarus	13,181	84	Azerbaijan	1,766	23	Jamaica	396	7			
Poland	12,781	628	Nigeria	1,728	51	El Salvador	395	9			
Qatar	12,564	10	Bosnia Herzegovina	1,677	65	Kenya	384	15			
Romania	11,978	693	China	1,671	16	Sudan	375	28			
UAE	11,929	98	Estonia	1,666	50	Palestin	344	2			
Korea Selatan	10,765	247	Bulgaria	1,488	65	Mauritius	332	10			
Ukraine	10,406	261	New Zealand	1,476	19	Venezuela	331	10			
Indonesia	9,771	784	Cuba	1,467	58	Montenegro	322	7			
Denmark	9,356	443	Makedonia Utara	1,442	73	Equatorial Guinea	315	1			
Filipina	8,488	568	Slovenia	1,418	89	Maldives	280	1			
Norway	7,710	207	Slovakia	1,396	23	Gabon	276	3			
Czechia	7,581	227	Lithuania	1,385	45	Vietnam	270	0			
(Dikemaskini pada 30 April 2020) (Updated at 30 April 2020)											
Lain-lain / others (Tidak termasuk) (Not included)											
(1-50)											
(51-100)											
(101-150)											
(151-200)											
(201-250)											
33											
14											
10											
0											
4											



Sumber: CPKC Rebasan dan WHO
UKK MOH

Sumber: Saluran Telegram MKN



Situasi ini mengakibatkan banyak negara di seluruh dunia mengambil tindakan dengan melaksanakan lockdown atau sekatan terhadap pergerakan penduduk di negara tersebut. Bimbang akan ancaman wabak berbahaya yang semakin menular, Kerajaan Malaysia telah melaksanakan Perintah Kawalan Pergerakan (PKP) yang merangkumi beberapa fasa termasuk Perintah Kawalan Pergerakan Bersyarat (PKPB) bermula 18 Mac 2020.

Dengan berkuatkuasa perintah tersebut, semua sektor serta industri tidak dibenarkan beroperasi melainkan organisasi yang terlibat dengan penyediaan perkhidmatan penting negara (*essential services*). Selain itu, PKP turut merangkumi sekatan sempadan, sekatan kemasukan pelancong asing, sekatan perjalanan rakyat Malaysia ke luar negara serta merentas negeri dan daerah, larangan perhimpunan, aktiviti keagamaan serta penutupan institusi pengajian termasuk sekolah dan juga universiti.

Penggunaan Teknologi

Menurut kenyataan Suruhanjaya Komunikasi dan Multimedia Malaysia (MCMC) pada 9 April 2020, permintaan terhadap lebar jalur telah melonjak sewaktu pelaksanaan PKP kerana rakyat Malaysia kekal berada di rumah. Pada minggu pertama PKP, peratus peningkatan aliran trafik Internet di seluruh negara adalah sebanyak 23.5%, manakala minggu kedua PKP menyaksikan peningkatan sebanyak 8.6%.

Sumber:

<https://www.mcmc.gov.my/ms/media/press-releases/media->

statement-changing-usage-patterns-influence

Di sektor pekerjaan, kebanyakan organisasi melibatkan kakitangan awam dan swasta turut melaksanakan tugas dengan berkerja dari rumah (*work from home*). Malah, Kerajaan juga menggalakkan aktiviti dilakukan secara dalam talian bagi mengelakkan pertemuan fizikal seperti persidangan video (telesidang), pembelajaran melalui Internet dan pembelian dalam talian bagi mengekalkan penjarakan sosial.

Penggunaan teknologi termasuk Internet dan media sosial juga meningkat kerana orang ramai berhubung, berinteraksi, mengakses maklumat serta informasi menggunakan komputer atau gajet digital untuk pelbagai tujuan seperti pembayaran bil, pembelian barangan, aktiviti

perbankan serta menghabiskan masa dengan *online games*, *online movies* dan sebagainya.

Pastinya penggunaan teknologi sewaktu PKP memberi satu pengalaman baharu kepada warga digital semasa melayari Internet. Namun, penggunaan teknologi juga dikatakan 'serampang dua mata' kerana selain memberi pelbagai kemudahan, ia turut berupaya meningkatkan risiko terhadap ancaman dan serangan siber, sekiranya kaedah penggunaan teknologi tidak dilakukan secara wajar dan selamat.

Statistik Insiden Keselamatan Siber

Umumnya, penjenayah siber sering mengambil kesempatan di atas sesuatu peristiwa atau krisis yang berlaku. Berdasarkan statistik laporan insiden keselamatan siber Pusat Bantuan Kecemasan Cyber999 yang dikendalikan oleh Pasukan Tindak Balas Kecemasan Komputer Malaysia (MyCERT), berlaku peningkatan insiden pada suku pertama tahun 2020 berbanding tempoh yang sama pada tahun-tahun sebelumnya.

SUKU PERTAMA	
TAHUN	INSIDEN
2016	2,470
2017	1,850
2018	1,453
2019	2,322
2020	3,108



Sumber: <http://www.mycert.org.my>

Sewaktu tempoh PKP yang bermula pada 18 Mac 2020 sehingga 30 April 2020, sebanyak 1,987 insiden keselamatan siber telah dilaporkan oleh warga digital Malaysia ke Cyber999 berbanding

dan Multimedia Malaysia (KKMM) yang ditubuhkan bagi membendung penyebaran berita palsu berkaitan COVID-19 bermula 24 Mac 2020.

Sumber: Saluran Telegram MKN

Sekiranya penyebaran berita palsu melalui media sosial ini tidak dibendung, ia akan menjejaskan keselamatan, mengundang kebimbangan, keresahan orang ramai dan akhirnya menggugat kesejahteraan negara serta keharmonian masyarakat.

Inisiatif Kerajaan Dalam Membendung COVID-19

Pelbagai inisiatif dilaksanakan oleh pihak Kerajaan bagi mencegah, membendung dan mengawal penularan wabak COVID-19 seterusnya menjamin kelangsungan kesihatan awam dan kesejahteraan rakyat. Selain mewujudkan langkah-langkah proaktif secara fizikal seperti saringan kesihatan, kuarantin diri, pemakaian topeng muka, gesaan untuk kekal di rumah, penjagaan kesihatan serta penjarakan sosial, Kerajaan juga menggunakan teknologi dengan mewujudkan saluran Telegram khusus oleh Majlis Keselamatan Negara (MKN) pada 12 Mac 2020 serta Facebook, Twitter dan Instagram.


Kementerian Pertahanan Malaysia
 March 26 · 🌐

Mohon rakyat Malaysia menyebarkan lagi maklumat mengenai situasi terkini COVID-19 dengan mengikuti dan mempromosi saluran Telegram, Facebook, Twitter, Instagram MKN Rasmi.

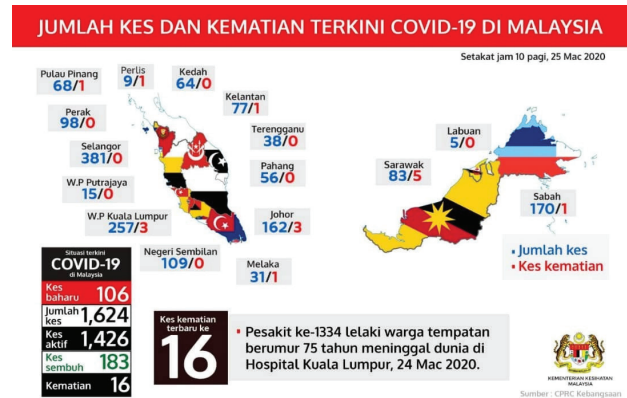
Informasi mengenai keselamatan negara dan usaha menyampaikan maklumat sahih dan tepat kepada masyarakat.

Terima kasih

<https://t.me/MKNRasmi>




Majlis Keselamatan Negara (Rasmi)
 Majlis Keselamatan Negara bertanggungjawab menyelaraskan dasar-dasar berkaitan keselamatan negara dan arahan mengenai langkah-langkah keselamatan termasuk gerakan-




Tujuan utama saluran tersebut dibangunkan adalah untuk menyampaikan maklumat serta perkembangan COVID-19 secara sahih dan tepat kepada rakyat. Sehingga kini, jumlah pelayar saluran Telegram MKN COVID-19 telah mencecah lebih 1.169 juta. Kementerian Kesihatan Malaysia (KKM) pula menyediakan laman sesawang www.doctoroncall.com.my untuk memberi kemudahan kepada rakyat memeriksa tahap risiko terkena jangkitan COVID-19.

Penggunaan teknologi, Internet dan media sosial telah memberi kemudahan kepada Kerajaan untuk menyalurkan informasi mengenai COVID-19. Antara maklumat yang disebarkan melalui platform berlandaskan teknologi ialah situasi semasa jumlah jangkitan di Malaysia (dalam bentuk mesej dan infografik), Siaran Media oleh Kerajaan Negeri, Kementerian dan agensi kerajaan, panduan serta kaedah pelaksanaan sesuatu acara seperti majlis perkahwinan, penjarakan sosial, penjagaan kebersihan, pertuduhan ke atas kesalahan melanggar PKP, penafian berita palsu, nasihat perjalanan di pintu masuk sempadan, larangan dan penangguhan program, gesaan membuat saringan kesihatan dan pelbagai informasi berkaitan COVID-19.



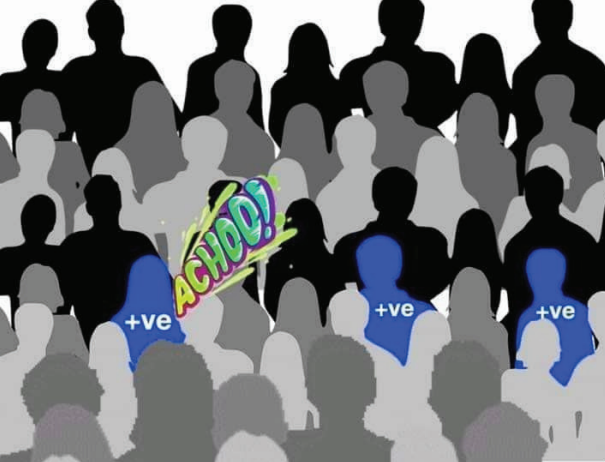
PEKABAR PERDANA MENTERI



“ Kita ibarat sebuah keluarga besar. Kita saling bantu membantu ketika zaman susah. Kita jaga keluarga kita. Kita jaga jiran kita. Kita jaga masyarakat kita. Baik kita di kampung, di kawasan perumahan, di kondominium, di rumah flat. Kita jaga kita. Inilah nilai sebenar persaudaraan rakyat. Malaysia tanpa mengira bangsa ”


YAB Tan Sri Muhyiddin Yassin
Perdana Menteri

@ts.muhyiddin @muhyiddinyassin_official @MuhyiddinYassin www.pmo.gov.my

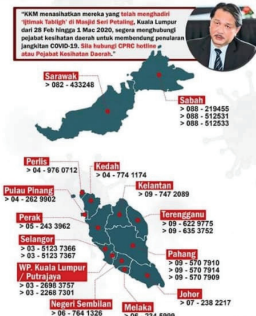


TANGGUHKAN MASS GATHERING
Public Health Malaysia
#SocialDistance

Saranan Cegah COVID-19
Amalkan langkah-langkah pencegahan dan jaga kebersihan diri.
Sumber: Kementerian Kesihatan Malaysia



1. Elakkan berkumpul dengan ramai orang dalam keadaan tertutup.
2. Pakai masker muka.
3. Cuci tangan dengan sabun.
4. Bekerja dari rumah jika mungkin.



Perlis: 04-976 0712
Kedah: 04-774 1174
Pulau Pinang: 04-261 9122
Selangor: 03-235 1237
Negeri Sembilan: 06-704 1328
Melaka: 06-234 0989
Johor: 07-228 2217

Untuk Sebarang Maklumat Berkaitan Wabak COVID-19

Nombor Hotline
03 8881 0200
03 8881 0600
03 8881 0700

COVID-19

(18 MAC 2020 - 31 MAC 2020)

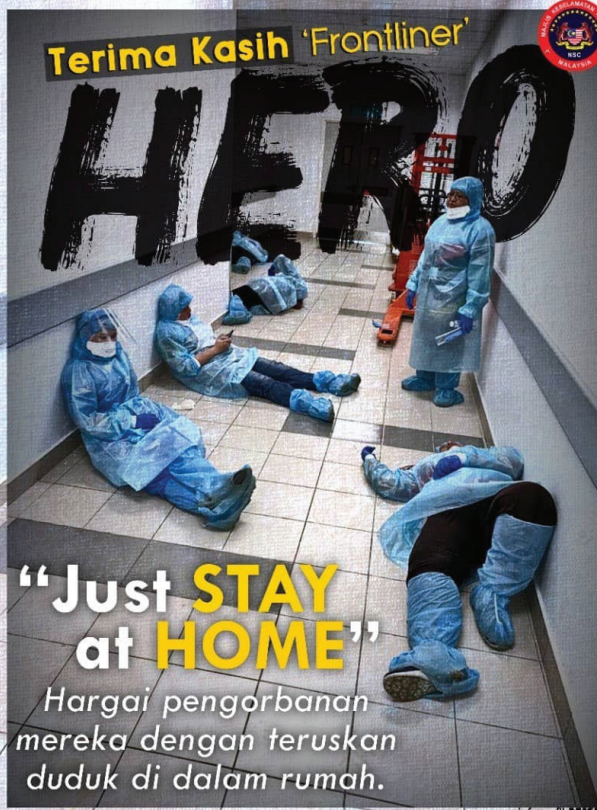


Hukuman
PENJARA ENAM (6) BULAN
atau
DENDA RM1,000.00
akan dikenakan sekiranya orang awam atau majikan didapati melanggar
PERINTAH KAWALAN PERGERAKAN

Kementerian Dalam Negeri (KDN) @KDNPUTRAJAYA kementeriandalamnegeri www.moha.gov.my

Terima Kasih 'Frontliner' HERO

"Just STAY at HOME"
Harga pengorbanan mereka dengan teruskan duduk di dalam rumah.



InfogratiMKM

Peranan CyberSecurity Malaysia sepanjang tempoh Kawalan Pergerakan (PKP)

Sebagai sebuah agensi yang menyediakan perkhidmatan penting negara (*essential service*), CyberSecurity Malaysia turut memainkan peranan sewaktu PKP dengan melaksanakan beberapa inisiatif bagi memberi maklumat dan informasi berkaitan amalan terbaik keselamatan

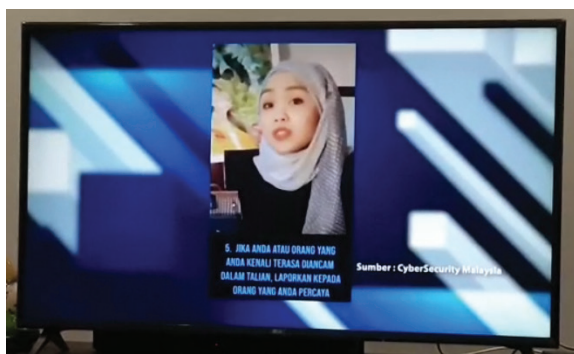
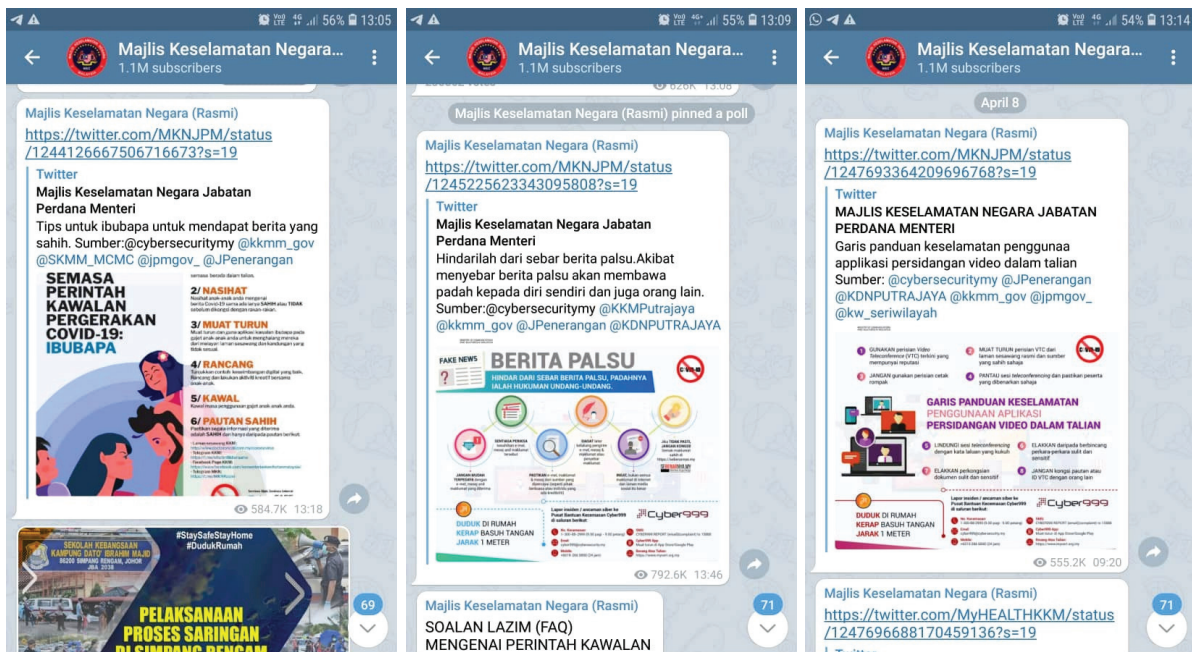
siber. Antara aktiviti yang dilakukan ialah mengeluarkan amaran dan nasihat keselamatan siber berkaitan COVID-19 seperti 'Penipuan dan Scam' (18 Mac 2020), 'Amalan Terbaik Bekerja dari Rumah' (21 Mac 2020), 'Panduan Penggunaan *Online Video Conferencing*' (7 April 2020) serta 'Bogus Scam Email' (15 April 2020). Ke semua amaran dan nasihat ini boleh didapati melalui www.mycert.org.my/portal/index

Pelbagai mesej mengenai tips penggunaan Internet dalam bentuk infografik, video grafik serta klip video turut dikeluarkan melalui platform Instagram, Facebook, Youtube dan LinkedIn. Usaha ini dilaksanakan bagi memupuk kesedaran pengguna Internet serta memberi maklumat mengenai kepentingan mengamalkan nilai etika yang tinggi di alam siber secara berterusan pada setiap masa walaupun sewaktu PKP.

Sehingga 30 April 2019, sebanyak 27 mesej keselamatan siber diterbitkan pada setiap

hari merangkumi isu seperti Scam & Phishing, Tips Keibubapaan Siber, Pelaporan Insiden ke Cyber999, Pembelian Dalam Talian, Tips Remaja, Perlindungan Kata Laluan, Berita Palsu, Tips Kanak-Kanak, Anti-virus, Panduan Persidangan Dalam Talian, Tips Bekerja dari Rumah, Ucapan khas kepada barisan hadapan COVID-19, Perbankan Internet, Permainan Dalam Talian, Peraturan 20-20-20, Kandungan Yang Tidak Sesuai, Hendap Siber, Antun Siber, Buli Siber serta beberapa video yang dilaksanakan dengan kerjasama rakan strategik CyberSAFE mengenai remaja dan kanak-kanak di alam siber.

Tiga infografik tips keselamatan siber tersebut telah dimuat naik oleh pihak MKN ke saluran Telegram dan menerima jumlah jangkauan yang tinggi iaitu Tips Keibubapaan Siber (585 ribu), Berita Palsu (793 ribu) dan Garispanduan Persidangan Dalam Talian (555 ribu). Selain itu, video Remaja turut disiarkan oleh pihak BERNAMA TV di saluran media mereka.



Selain itu, CyberSecurity Malaysia turut menganjur dan mengambil bahagian pada forum dalam talian bersama rakan strategik melibatkan beberapa ahli panel yang mempunyai kepakaran di bidang masing-masing. Antara forum tersebut ialah:

25 Mac 2020: Zoom - "Keibubapaan Siber"

Penganjur: Online Coffee Brea
Jumlah Jangkauan: 1,000 views

Online COFFEE BREAK

RABU 25 MAC 2020 10.30 - 11.30 PG

KEIBUBAAN SIBER
Mendidik Anak-Anak Digital Yang Berdaya Tahan Ke Arah Kesejahteraan Siber.
Ketahu tips keibubapaan di zaman siber yang dilengkapi dengan ilmu dan maklumat yang sangat penting untuk anda dan seisi keluarga.

Penceramah
Lt Col Mustafa bin Ahmad (Retired) CISO
Senior Vice President
Outreach and Capacity Building Division
CyberSecurity Malaysia
An Agency under the Ministry of Communications and Multimedia Malaysia

MODERATOR
IZZAH MAZURA ZULUFLI
KITA BERSAMA SAMA AMPANG JAYA

"GAMES" MUAT TURUN APPS ATAU KE
WWW.KAHOOT.COM
Kahoot!
"Hadiah menarik juga menanti anda dalam Quiz"

SERTAI!
Ceramah melalui online
DI
Zoom

JOIN A MEETING
<https://zoom.us/j/523522105> Password: 005572

Anjuran Bersama
#CARIK COVID-19 #DUDUKDIRUMAH #STAYHOME #STAYSAFE

Dapatkan "link" atau klik dari laman sosial media kami
@ikramaj @warta_sj
IKRAM Ampang Jaya
Warta IKRAM Ampang Jaya
IKRAM Ampang Jaya
Taman Ukay Bistari
ikram-ampang-jaya.blogspot.com

PERSATUAN PENDUDUK TAMAN UKAY BISTARI IKRAM AMPANG JAYA CYBER SECURITY MALAYSIA, MCM

IAJ_PC19-015

13 April 2020:
Sembang Santai - "Mendidik Anak-Anak Digital Semasa PKP Covid-19 Ke Arah Kesejahteraan Siber"
<https://www.youtube.com/watch?v=uTsGONeruHU>

Penganjur: Kementerian Pendidikan & Microsoft
Jumlah Jangkauan: 12, 901 views

SEMBANG SANTAI: MENDIDIK ANAK-ANAK DIGITAL SEMASA PKP COVID-19 KE ARAH KESEJAHTERAAN SIBER

Lt Col (B) Mustafa bin Ahmad
Timbalan Presiden Kanan
CyberSecurity Malaysia

13 APRIL 2020 9:00 - 10:00 PM
Nantikan pautan webinar di Telegram Digital Classroom Malaysia

16 April 2020:
Bicara Siber "When Mak Cik Kiah Goes Digital"
<https://youtu.be/ZtzBaULCvts>

Penganjur: CSM (OCC)
Jumlah Jangkauan: 20,678 views / 691 likes

BICARA SIBER PKP COVID-19: WHEN MAK CIK KIAH GOES DIGITAL

16 APRIL 2020 | 11.00 PAGI

MADIAN MENARIK MENANTI! PEREMANG PEMENANG QUIZZ

YouTube Live CyberSecurityMy

ANJURAN BERSAMA
#CARIK COVID-19 #DUDUKDIRUMAH #STAYHOME #STAYSAFE

LIHAT PANDANGAN
#CARIK COVID-19 #DUDUKDIRUMAH #STAYHOME #STAYSAFE

LIHAT PANDANGAN
#CARIK COVID-19 #DUDUKDIRUMAH #STAYHOME #STAYSAFE

30 April 2020:
"#EduTECHAsia Webinar: Protecting students from cyberattacks and data intrusion"

Penganjur: The EduTECHAsia Team
Jumlah Jangkauan: XXX

EduTECH

LIVE WEBINARS THURSDAYS 30 APRIL 2020, 5PM (+8 GMT)

PROTECTING STUDENTS FROM CYBERATTACKS AND DATA INTRUSION

MATT HARRIS
Owner and Chief Consultant
International EdTech

MAYURI AMBULE
Director of Educational Technology
The British School New Delhi, India

LT. COL. (RETIRED) MUSTAFFA BIN AHMAD
Senior Vice President, Outreach and Capacity Building Division
CyberSecurity Malaysia

NOEL FERIA
Distinguished Educator
Educator, Privacy and Security Advisor
University of the Philippines

KAVITHA MUTHY
Chief Strategy Officer
Intellect Tech Services

WWW.TERRAPINN.COM/EDUTECHASIAWEBINARS | #EDUTECHASIA

5 Mei 2020:
"WFH"Online Meeting Platform Security Demystified"
<https://www.youtube.com/watch?v=PfILPCIVOH>
 E&feature=youtu.be

Penganjur: **CSM (CSPD)**
 Jumlah Jangkauan: **7,452 views / 341 likes**

WFH: ONLINE MEETING PLATFORM SECURITY DEMYSTIFIED

Work from home has become a new norm and as we adapt to this new work environment with Online meetings, once again cybersecurity becomes a predominant concern.

Lately, our headlines buzzed with news on Zoom as many agencies & organizations stopped using them. Join this 1-hour talk to understand the cybersecurity concerns of Online Meeting platforms and to hear from a well-known cybersecurity expert on the tips and tricks to keep us safe during this period.

5 MAY 2020
 11.00am - 12.00pm
 CyberSecurity Malaysia **YouTube LIVE**
 Register at <https://bit.ly/2W5M9NG>

OBJECTIVE

- To help users understand the security concerns of Online Meeting Platforms including Zoom, WebEx, GoToMeeting, Slack and Microsoft Teams before selecting either to use or whether to move away from Zoom.
- To share the tips to stay safe from hackers while working from home.

AGENDA

- MCO and Online Meeting Platforms & Security Concerns (Covers Microsoft Teams, Zoom, GoToMeeting, Slack, Cisco WebEx)
- Zoom phobia: Are we overreacting?
- Microsoft Teams Security
- GoTo Meeting Security
- Cisco WebEx Security
- 15 Security Tips for a safe online meeting

EXCITING PRIZE AWAITS WINNERS
Quizizz

GLOBAL ACE CERTIFICATION 1 CPD Point

SPL KPM (Sistem Pengurusan Latihan, Kementerian Pendidikan Malaysia) Teachers eligible for CPD Hours

MEBT Members eligible for CPD Hours

Corporate Office:
 CyberSecurity Malaysia, Level 11, Tower 1, Menara Cyber Asia, Jalan Impact, 60000 Cyberjaya, Selangor Darul Ehsan, Malaysia
 Tel: +603 8900 7386 Fax: +603 8900 7390 Email: info@cybersecurity.my
 Customer Service Hotline: 1-800-88-2000 | www.cybersecurity.my

8 Mei 2020:
"When Veteran ATM Goes Digital"
<https://www.youtube.com/watch?v=QZJXXB3W-hM&feature=youtu.be>

Penganjur: **Jabatan Ehsan Veteran ATM**
 Jumlah Jangkauan: **338 views / 21 likes**

SEMBANG SANTAI PKP JHEV ATM: TERBUKA KEPADA WARGA JHEV ATM

VETERAN ATM GOING DIGITAL

BIKA MINDA MENJADI INOVATIF
 LONJAK POTENSI DIRI DENGAN PENGGUNAAN DIGITAL DALAM AKTIVITI HARIAN

JUMAAT | 08 MEI 2020 | 11:00 - 12:00 TENGAH HARI

PENYERANAH
 LT COL HESTERITA BIN AHMAD (BERASA)
 NAIB PRESIDEN KANAN
 BANGSAAN OUTREACH & PEMBANGUNAN
 KAPASITI
 CYBERSECURITY MALAYSIA

MODERATOR
 PUAN SURAMAWATI BINTI ABDUL MANAF
 PENYERANAH PROJEK VIBES 2.0
 AKAL KOPRAID SDN BHD

UCAPAN PEMBUKAAN OLEH
 HEDAR JEMAL DATU DOLKARMAN BIN AHMAD
 KETUA PENGARAH
 JABATAN PAM DIGITAL VETERAN JHEV ATM

Peserta diminta untuk daftar masuk lebih awal bermula 10:45 pagi melalui aplikasi Google Meet: <https://meet.google.com/wwx-4myd-qyb>

CyberSecurity Malaysia juga mendapat sokongan pihak media dalam bentuk temubual di beberapa saluran TV, Radio dan juga suratkhbar tempatan. Sila rujuk lampiran 1 untuk senarai dan pautan.

Penutup

Wabak COVID-19 telah memberi satu senario baharu kepada dunia dan Malaysia khusus apabila berlaku perubahan kepada gaya hidup masyarakat dengan amalan norma baharu. Walaupun ia satu pandemik merbahaya, dari sudut positif, penularannya membawa pelbagai kebaikan dan hikmah. Dari aspek teknologi, norma baharu telah menjadikan masyarakat Malaysia lebih cakna dan peka terhadap penggunaan teknologi digital.

Pada tempoh tersebut berlaku peningkatan dalam penjualan dan pembelian secara dalam talian, aktiviti e-pembelajaran sama ada di peringkat sekolah mahu pun pengajian tinggi, penggunaan aplikasi teknologi komunikasi maklumat (ICT) secara kreatif dengan penghasilan karya seni menerusi multimedia serta perubahan landskap perniagaan sektor perusahaan kecil dan sederhana (PKS) yang beralih dari operasi konvensional kepada digitalisasi.

Diharapkan agar warga digital Malaysia akan menjadi celik IT khususnya dari sudut kebergantungan teknologi dan aspek keselamatan kerana wujudnya pelbagai mesej serta tips keselamatan siber yang dikeluarkan bukan sahaja oleh CyberSecurity Malaysia, malah agensi Kerajaan yang lain.

Rujukan

1. Saluran Telegram MKN
2. <https://www.mcmc.gov.my/ms/media/press-releases/media-statement-changing-usage-patterns-influence>
3. <http://www.mycert.org.my/>
4. www.mycert.org.my/portal/index

Corporate Office:

CyberSecurity Malaysia

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

Tel: +603 - 8800 7999

Fax: +603 - 8008 7000

Email: info@cybersecurity.my

Customer Service Hotline: 1 300 88 2999

www.cybersecurity.my

© CyberSecurity Malaysia 2020 – All Rights Reserved



MINISTRY OF COMMUNICATIONS
AND MULTIMEDIA MALAYSIA

