

# eSecurity

www.cybersecurity.my

The First Line of Digital Defense Begins with Knowledge  
Vol 53 - (2/2022)



**Dashboard Camera Footage as Evidence in Vehicle Crash**  
**QR Code: Scan Me or Scam Me?**  
**NFT: A New Medium for Money Laundering?**

*"Security isn't something you buy, it's something you do, and it takes talented people to do it right."*

ISSN 1905-1995





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



## Securing Our Cyberspace

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

For more information, please visit  
[www.cybersecurity.my](http://www.cybersecurity.my)

For general inquiry, please email to  
[info@cybersecurity.my](mailto:info@cybersecurity.my)

Stay connected with us on  
[www.facebook.com/CyberSecurityMalaysia](https://www.facebook.com/CyberSecurityMalaysia) and  
[www.twitter.com/cybersecuritymy](https://www.twitter.com/cybersecuritymy)



### **CyberSecurity Malaysia**

200601006881 (726630-U)

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

T: +603 - 8800 7999  
F: +603 - 8008 7000  
E: [info@cybersecurity.my](mailto:info@cybersecurity.my)

[www.cybersecurity.my](http://www.cybersecurity.my)



## WELCOME MESSAGE FROM THE CEO OF CYBERSECURITY MALAYSIA

Dear Readers,



We are pleased to present the latest edition of our security bulletin, which is dedicated to bringing you the most important and relevant security updates and alerts. In this issue, you will find a selection of informative and interesting articles on all cybersecurity-related matters ranging from various topics, including cybersecurity trends, emerging technologies, and best practices for protecting your organization and personal data.

There are so many emerging technologies and gadgets that we quickly adapt and apply in everyday life. For example, the use of dashcams in vehicles. Social media is flooded with footage of accidents where people can become witnesses by submitting the footage as evidence. Nowadays, if you were involved in a vehicle crash and have dashcam footage, it is important to preserve the footage and provide it to the insurance company and the police. The footage may help to identify who was at fault for the accident and may impact the outcome of any legal proceedings related to the crash. We prepared an article titled *'Dashboard Camera Footage as Evidence in Vehicle Crash'* to look into this topic.

Following the post-pandemic era of Covid-19, we can see the use of QR codes becoming more widespread. QR codes have become an increasingly popular way to make payments and also exchange information quickly and conveniently. From marketing campaigns to online shopping, these codes are being used in a wide range of contexts to provide a seamless user experience. However, as with any technology, it is important to be aware of the potential security risks associated with QR codes. Malicious perpetrators can use these codes to direct users to phishing websites, install malware on their devices, or even steal sensitive information. In this edition of our security bulletin, we touch on QR code security and the measures that can be taken to protect against these risks. We will be discussing best practices for creating and using QR codes, as well as the methods that can be used to scan and verify the legitimacy of these codes in an article entitled *'QR Code: Scan Me or Scam Me?'*

The rise of Non-Fungible Tokens (NFTs) has been one of the most talked-about phenomena in the digital world in recent years. NFTs are unique digital assets that are stored on a blockchain and are designed to represent ownership of a specific item or piece of content, such as artwork, music, or even tweets. While NFTs have been lauded for their potential to revolutionize the art world and enable creators to monetize their work, there is growing concern that they could also be used as a new medium for money laundering. Let's take a further look at this issue in our article *NFT: A New Medium for Money Laundering?*

Apart from that, many other interesting articles in this bulletin will give you cybersecurity awareness and best practices to protect your data and devices. As always, we encourage you to take the necessary precautions to ensure the safety of your personal and sensitive information. Stay vigilant and don't hesitate to contact us if you have any questions or concerns. We hope that you find the content valuable and helps you stay up-to-date on the latest developments in the field.

Thank you for reading.

Be Smart, Be Cybersafe.

**Dato' Ts. Dr. Haji Amirudin bin Abdul Wahab, FASc**  
Chief Executive Officer, CyberSecurity Malaysia

## **EDITORIAL BOARD**

### **Chief Editor**

Roshdi bin Hj Ahmad

### **Editorial Team**

Yuzida Yazid

### **Designer & Illustrator**

Zaihasrul bin Ariffin

Nurul Ain binti Zakariah

### **READERS' ENQUIRY**

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

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



## TABLE OF CONTENTS

1. The Importance of Cyber Insurance .....	1
2. Deepfake Technology .....	3
3. Building Cybersecurity Competency Through Global ACE Certification .....	5
4. Ensuring Business Continuity In The Digital Age .....	8
5. Power Of ISMS: Driving Value & Growth For SMEs In Malaysia .....	11
6. Leveraging MyCC Certification To Boost Malaysia's ICT Exports .....	14
7. Preservation Of Digital Evidence .....	17
8. NFT: A New Medium For Money Laundering? .....	20
9. Dashboard Camera Footage As Evidence In Vehicle Crash .....	23
10. Towards Better Cybersecurity With Key Performance Indicators (KPI) .....	27
11. Tip Untuk Elak Macau Scam (Penipuan Panggilan) .....	31
12. Promoting Data Sovereignty In The Age Of Cloud Computing .....	33
13. Methods And Risk Of Bypassing Apple Device Security .....	37
14. Cyber Incident Trend Analysis 2020 VS 2021 .....	40
15. Physical Access Control: Fail Safe VS Fail Secure .....	44
16. Telegram Account Compromise Incidents .....	46
17. WhatsApp Account Compromise Incidents .....	50
18. Digital Signature Application in Malaysia .....	53
19. Endpoint Detection And Response Platform As A Mitigation Strategy For Advanced Security Operation Center In Managing Security Incidents .....	56
20. Memilih Rancangan Kartun Yang Selamat Untuk Kanak-Kanak .....	59
21. General Data Protection Regulation (GDPR) Comparisons: Malaysia's, Singapore's Personal Data Protection Act (PDPA) And California Consumer Privacy Act (CCPA) .....	62
22. CSM Cyber Range – an Overview .....	64
23. Building Cybersecurity Talent And Capacity Through Global ACE Certification .....	67
24. Pupuk Budaya Integriti Di Sekolah .....	72
25. Pengaruh Penggunaan Internet Terhadap Kanak-Kanak .....	75
26. How To Enhance Information Gathering Results With Alternative Search Engines .....	78
27. Human Resource Factors In Information Security .....	84
28. DNA Techniques In DNA Based Cryptography .....	88
29. Challenges In Patch Deployment .....	91
30. QR Code: Scan Me Or Scam Me? .....	93
31. Cloud As A New Media Storage .....	96
32. Two-Factor Authentication: What Is It And How It Works. ....	99
33. Kebocoran Maklumat Peribadi Dalam Kalangan Pengguna Internet .....	101
34. The Necessity Of Conducting Cyber Security Drills For Organisations .....	103

# The Importance of Cyber Insurance

By | Mohammad Farid bin Azman

Online business has become a popular choice of business model. For this reason, many companies are shifting their business strategy to focus online. One of the reasons online businesses are becoming more popular is the lower barrier of entry. From low-cost structure to easy startup, leading to time savings, businesses do not even need to meet their customers for sales.

Internet technology has greatly changed the daily lives of people for the better. The shift to online platforms accelerated dramatically when the global economy was hit by the Covid-19 epidemic, forcing people to stay and work from home, leading to a new lifestyle norm of buying everything online. Despite the numerous advantages, there are also disadvantages of doing business online, namely exposure to cyber threats and hence businesses need to consider cyber insurance.

## What is cyber insurance?

Cyber insurance is one of the least popular insurance products in society chiefly because it is hardly promoted compared to other insurance products such as health, life and property. Cyber insurance protects businesses and individuals against risks arising from doing business on the Internet. The most common risk is data breach. Cyber insurance typically covers losses from legal claims related to data breaches due to errors, negligence, and omissions. It also covers losses due to network security breaches, intellectual property theft and loss of privacy.

Any business or individual is susceptible to breaches of sensitive customer or employee data. As technology becomes more complex and sophisticated, so do the cyber threats. This is why every business and organization needs to be prepared with cyber insurance.

Cyber insurance is critical to protecting businesses and individuals in the event of a data breach. The cost of a data breach can include business interruption, loss of revenue, property damage, legal fees, public relations expenses, forensic analysis, and costs associated with regulatory notification.

## Examples of breach of customer data

In 2011, Sony's PlayStation network was breached by hackers, exposing personal data of some 77 million PlayStation user accounts. The breach disrupted PlayStation users from accessing the service for 23 days. As a result, Sony incurred costs of more than US\$171 million. Some of those costs could have been covered had Sony purchased a cyber insurance policy. The court ruled that Sony's insurance policy only covered damages from physical property damage. Consequently, Sony had to bear the full amount of costs related to the cyber-attack.

## How can cyber insurance save a business?

Cyber insurance policies can help recoup financial losses caused by cyber incidents. In addition, they can help businesses cover costs, including payments for legal counsel, investigations, crisis assistance and credits or customer refunds. Most insurance policies include first-party coverage, which is used for losses that directly affect the company, as well as third-party coverage, which is used for losses suffered by others due to cyber incidents, based on their business relationship with the company.

## Who needs cyber insurance?

Businesses that store and manage electronic data online such as customer contact details, customer sales, personal numbers, and credit cards, will benefit immensely from cyber insurance. In addition, e-commerce businesses can also consider cyber insurance as cyber incidents can cause them lost sales and customers. In fact, any business that stores customer data online can benefit from cyber insurance.



## Conclusion

---

Cybersecurity insurance provides good protection for businesses which handle transactions and store records online. However, it is important to note that cybersecurity insurance is not designed to bail out businesses in the event of major data breaches, but to mitigate damages suffered. Demand for cyber security insurance is likely to grow in the coming years as data breaches continue to escalate.

## References

---

1. <https://www./cyber-security-insurance>
2. <https://www.cybersecurity-insurance-cybersecurity-liability-insurance>
3. <https://www.chubb.com/my-en/business/cyber-insurance.html>

# Deepfake Technology

By | Indumathi Vijayakumaran

## What is Deepfake?

Deepfake is a technology that uses Artificial Intelligence (AI) to merge, combine, replace, as well as superimpose video clips and images to create fake videos that appear very realistic (Westerlund, 2019). Hyper-realistic videos created using AI are the most common form of deepfake technology. Through emerging social media technology, videos can easily spread, regardless of whether they are authentic or fake. Fake news is created by fabricating an original content to gain the public's trust (Aldwairi & Alwahedi, 2018).

## The Possible Threats of Deepfake

Deepfake technology can be operated not just by professionals, but also any normal person who is computer-savvy, thanks to the embedded AI technology. Thus, a person can learn and deploy the technology to fabricate a clip with little effort. Listed below are the types of threats that deepfake technology could bring.

### Ghost Fraud

Ghost fraud occurs when criminals use identities of deceased people to commit fraudulent activities. Because deepfake technology can realistically imitate a person's voice and image, criminals often use it to create videos impersonating deceased to gain a person's trust for financial benefits.

### Synthetic Social Botnets

A synthetic social botnet, known as a broadcast threat, uses fake social media accounts with synthetic text and images operated by an AI. These botnets are extremely difficult to identify. Criminals often use this technology to cause harm to financial institutions, markets, and regulators (Bateman, 2020) to gain trust from legitimate companies or vendors.

## Fabricated Private Remark

A fabricated private remark is another broadcast threat that makes use of deepfake video to portray a public figure in a false light (Bateman, 2020). Criminals frequently use fabricated private remarks to damage the reputation of a public figure. It is also difficult to detect because the deepfake videos and voices produced are very similar to the original.

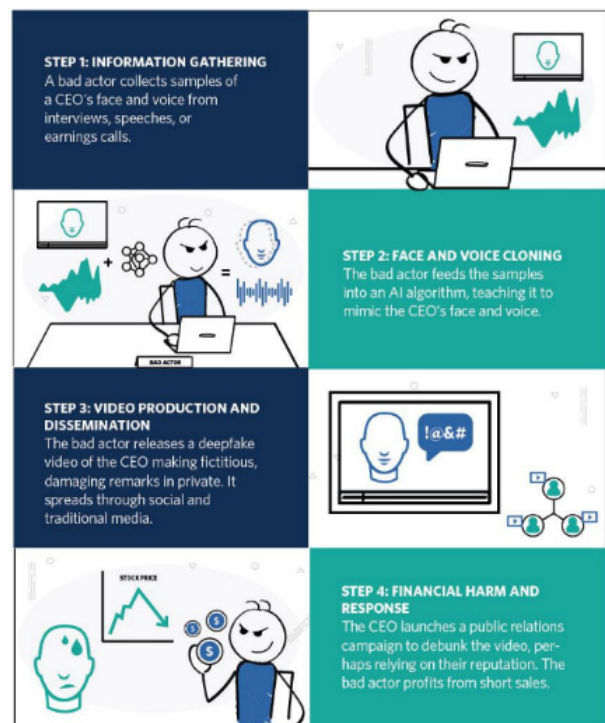


Figure 1: How Deepfake Fabrication of Private Remark Works (Westerlund, 2019)

### i. Cyber Extortion

Cyber extortion is a form of deepfake where the victim is casted in synthetic pornography. Criminals frequently use this method to blackmail victims in order to gain financial benefits from them.

### ii. Payment Fraud

Payment fraud is committed when criminals use deepfake technology to produce face swap videos including the voice of corporate officers to initiate transactions. In early 2020, a case was



reported as underpayment fraud in Hong Kong whereby a bank manager received a call from a man who imposed his company director's voice. The criminal falsely indicated that the company was planning to make an acquisition, which will cost \$35 million (T.Brewster, 2021). The bank manager believed the information when he received an email purportedly from the director, and a lawyer about the acquisition's procedure and funding requirements. He subsequently transferred the requested funds.

### iii. The Benefits of Deepfake

Although deepfake technology is largely used in criminal and fraudulent activities, it is also used in various industries to create informative, entertaining, and useful content. Industries such as education, healthcare, and entertainment are some of industries which have benefitted from deepfake technology. In particular, deepfake technology is widely used in the film industry.

Such technology is frequently used to recreate and edit images of actors, particularly those who have passed away. Deepfake technology is also used to create realistic voices for dubbing in films. Recently in South Korea, an MBN news channel utilized deepfake technology to recreate newsreader Kim Joo-Ha to broadcast their day's headlines. This method was very useful and effective during the pandemic season (JR.B.D, 2021). Although the news anchor was not present for recording, the news channel can still depict the image of the anchor delivering news.



Figure 1: Deepfake image of anchor Kim Joo-Ha (JR.B.D, 2021)

Computer-generated image, voice, and gestures of the news anchor were used to deliver news. The MBN company has said they will continue to use such technology for breaking news in the future. In addition, TikTok is one of the famous social media tools among Malaysians.

TikTok is a popular social media platform in Malaysia where content creators use deepfake technology. For instance, a foreign TikTok account named "deeptomcruise" was created

with the sole purpose of publishing deepfake videos of well-known American actor Tom Cruise.

The account created videos of Tom Cruise communicating with the public (Metz. R, 2021).



Figure 1: Deepfake TikTok Tom Cruise images (Schneider.J, 2021)

The account has since garnered 3.4 million followers, underscoring the popularity of people enjoying deepfake videos of celebrities. All content created under the "deeptomcruise" TikTok account was intended to be entertaining and fun. Thus, deepfake technology has invariably helped various industries promote their products and brands.

## Conclusion

Deepfake AI technology can be viewed as both a threat and advanced tool for marketing. The outcome rests vastly in the hands of users. If the technology is used with good intentions, it will benefit many. However, if used incorrectly, it will definitely impact negatively on individuals, organizations and our society.

# Building Cybersecurity Competency Through Global ACE Certification

By | Wan Shafiuddin Zainuddin, Razana binti Md Salleh & Mohd Haleem Abdul Sidek

## Introduction

Against a backdrop of escalating cyber threats and mass digitalisation, the global cybersecurity job market is growing exponentially with a surge in demand for cybersecurity professionals. As companies of all sizes across the globe migrate to digital platforms spurred by the Covid-19 pandemic, they require cybersecurity experts to design, engineer, and maintain cybersecurity systems and infrastructure.

According to independent market research firm Providence Strategic Partners, the total cybersecurity industry in Malaysia is forecasted to grow by 18.7% CAGR from an estimated RM3.9 billion in 2021 to RM5.5 billion in 2023. Despite the rapid industry growth, Malaysia still lags behind in cyber security talent pool development. Malaysia recorded a shortage of almost 8,000 cyber security professionals in 2020. Meanwhile, Malaysia Digital Economic Blueprint (MyDigital) has set a goal for the nation to produce 20,000 cyber security experts by 2025.

With the escalating threat of cyber-attacks, cyber security spend has also increased dramatically. Based on a report by GlobalData Market Opportunities Forecasts, IT expenditure in Malaysia will reach RM103.75 billion by 2023. As such, there will be a surge in demand for cyber security experts from security analysts and security architects, cyber threat intelligence analysts, consultants and cyber incident analysts.

To protect an organisation against cyber threats, there are three important elements: **people**, **process** and **technology**. In Malaysia, companies tend to focus on purchasing hardware and technology, but still lack in people element.

## What is Global ACE?



The Global Accreditation Cybersecurity Education Certification Scheme (Global ACE) is a national scheme that outlines holistic approach towards cyber security training and certification for cyber security workforce. It is industry driven and vendor-neutral, developed in collaboration with government agencies, industry partners and academia.

The establishment of the scheme is in tandem with international standards such as ISO 9001 on processes, ISO/IEC 17024 on certification of persons and ISO/IEC 27001 on security management, which is vital to assure workforce capability and experience, secure and validate core skills, knowledge, attitude and experience.

Global ACE, supported by the Organization of Islamic Cooperation (OIC) member countries and the ASEAN countries, is recognized by the Malaysia Board of Technologists (MBOT) as the cybersecurity professional certification pathway that needs to be pursued prior to application as a Professional Technologist or Certified Technician under the cybersecurity sector. Participants who pass the certification examination are eligible to apply as **Professional Technologies or Certified Technicians** from the Malaysia Board of Technologists (MBOT) under the Technologist and Technicians Act 2015 (Act 768), subject to MBOT terms and conditions.

Global ACE was named project winner under Category 5 - Building Confidence and Security in the use of ICTs in the WSIS Forum 2020 - the world's largest ICT annual gathering of the 'ICT for development' community hosted by the International Telecommunication Union (ITU), and co-organized by ITU, UNESCO, United Nations Conference on Trade and Development (UNCTAD) and United Nations Development Programme (UNDP) in close collaboration with all WSIS Action Line Facilitators/Co-Facilitators.



## Competency Enhancement through Global ACE

The **Knowledge, Skills and Attitude (KSA)** are the three main tenets upon which Global Ace certification and training is structured. KSA developed through Global ACE Certification forms a reference point for training providers to design cyber security training courses. It also serves as reference for the development of examination questions to effectively assess the identified job roles and functions, thus facilitates delivery of training courses in line with the requirements of the identified job roles and functions.

Global ACE Certification defines competency as a skill equipped with relevant knowledge associated with KSA. It serves as an indicator that an individual meets a minimum standard

of knowledge and skill, which can be used to demonstrate competency for current or potential employers. Through KSA developed, Global ACE Certification enables “transferability of skills” between job functions. It is flexible to encourage lifelong learning and to easily accommodate career change in the cyber security field.

## Ensuring High Competency through Global ACE

The heart of the Global ACE Certification is the framework that provides a standard base and means of acknowledging the “knowledge, skills and attitudes” for the workforce in the cyber security sector. Global ACE Framework (Figure 1) is the base for impartial examinations and guideline for certifications.

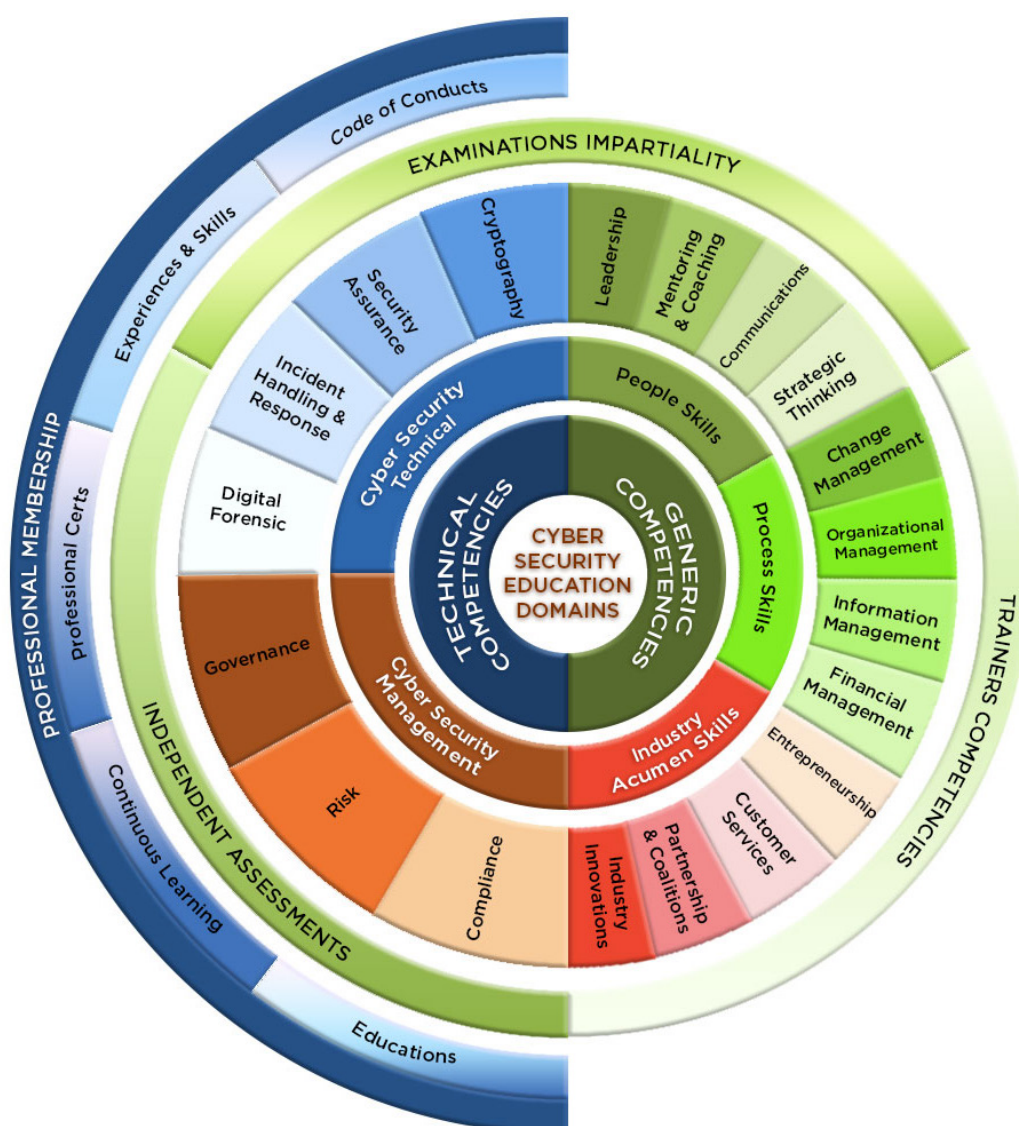


Figure 1: Global ACE Framework

The Global ACE Framework encompasses two broad categories, namely “**Cyber Security Technical Competencies**” and “**Cyber Security Generic Competencies**”. Technical competency refers to technical skills and knowledge required by a professional to conduct its task as a certified professional from Digital Forensics, Incident Handling and Response, Security Assurance, Cryptography, Governance, Risk and Compliance.

Global ACE certification also covers **Generic Competencies** in delivering cyber security services and consultation. Such competency covers three domains in soft skill sets from People, Process to Business Acumen skills. Under the people skills domain, members will learn about people management from leadership, coaching to communications and strategic thinking. In addition to dealing with people, they must also apply process management skills that include change management, organisational and even financial management. Last but not least, a competent cyber security professional should possess good business acumen that nurtures entrepreneurship, customer relations and innovativeness among others.

## Global ACE Membership

Global ACE Certification offers membership to individuals who have passed the certification examination under the programme. As a qualified member of the programme, an individual gains industry recognition, networking opportunities, priority access to professional development events, and access to members-only knowledge banks and whitepapers.

The membership allows participants to continuously increase their respective cyber security capacity and critical cognitive skills through lifelong learning programs and gain new skills at their own pace. It is also a platform for members to share knowledge, expertise, and skills, identify latest cyber threats as well as appropriate mitigation methods.

Global ACE credentials are maintained by either taking the current certification exam or maintaining Continuing Professional Development (CPD) points.

For cyber security practitioners, there are three categories of membership as follows:

### 1. Student Member

This category is for undergraduate students from recognized universities. The aim of this category is to develop cyber security expertise among students. To qualify, the candidate must pass any one of the certifications provided by the Global ACE Certification or has obtained other professional certifications that is recognized by the Global ACE Certification and submit recommendations from two (2) referees (academicians).

### 2. Associate Member

This category is for certified individual with less than 5 years working experience in cyber security. To qualify, a candidate must pass any one of the certifications provided by the Global ACE Certification or has obtained other professional certifications that is recognized by the Global ACE Certification and he/she must possess minimum education qualification of a Degree from recognized universities.

### 3. Professional Member

To be qualified as Professional Member under Global ACE scheme, the criteria required is similar to associate member category but one must have garnered more than 5 years working experience and demonstrated relevant competency and knowledge in cyber security area.

## Benefits of Global ACE Certification

For organizations, Global ACE certification provides confidence that Global ACE certified individuals have been trained, assessed and certified to secure the systems and networks. Global ACE certification ensures certified personnel maintain their knowledge and skills, thus uplifting productivity and competence of local cyber security community.

For individuals, Global ACE certification is a platform for capacity building and advancement in cyber security field. It provides a platform for lifelong learning that allows individuals to develop capabilities at their own pace and flexibilities to pursue continual enhancement through lifelong learning pathways. Certified personnel are able to gain competitive advantage to attest their competence in performing cybersecurity jobs.

# Ensuring Business Continuity In The Digital Age

By | Wan Shafiuddin Zainuddin, Nahzatulshima binti Zainuddin & Mohd Haleem Abdul Sidek

With an unpredictable global weather due to climate change and fresh geopolitical crisis threatening world peace, uncertainty has never been more certain today. Coupled with the spillover effects of Covid-19 pandemic and escalating cyber-attack threats, businesses the world over are facing volatile situations every day.

The flood that had devastated the Klang Valley in Malaysia during December 2021 caused an estimated RM6.1 billion in overall losses. The manufacturing sector accounted for RM900 million. There were also widespread damages to vehicles, business premises and homes. Any major incident that escalates to disaster could have a significant business impact on an organisation.

## What is BCMS?

**Business Continuity Management** or BCMS is defined as the advanced planning and preparation of an organization to maintain business functions or quickly resume after a disaster has occurred. At its highest level, BCM is implemented to keep business operating at its maximum capability. It is also about making proactive and reactive plans to help organizations avoid crisis and disasters and quickly return to a state of normalcy or 'business as usual'.

BCMS emphasizes the importance of understanding an organization's needs and the necessity for establishing business continuity policies and objectives. The system will help establish operating processes, as well as capabilities and response structures in ensuring that an organization could survive any disruption. BCMS mandates that its performance and effectiveness need to be constantly monitored and reviewed so that continuous improvements can be made both qualitatively and quantitatively.

The implementation of BCMS protects the following critical aspects against disasters and major disruptive events:

- **People** – Ensuring safety of employees
- **Key interested parties** – Encompasses shareholders, investors, customers, business partners, suppliers and even visitors
- **Key information and physical assets**
- **Critical business functions**

## What is ISO 22301

**ISO 22301:2019 Security and resilience – Business continuity management systems – Requirements**, is the world's first International Standard for implementing and maintaining an effective business continuity plan. It enables an organization to achieve a more effective response and a quicker recovery, thereby reducing any impact on people, products and the organization's bottom line. This will also help lower costs and lessen any impact on business performance should a disaster or negative incident struck. ISO 22301 also ensures that organisations with multiple sites can refer to a standardised and consistent approach in managing a disaster.

ISO 22301 emphasizes the need for a well-defined incident response structure. This ensures that when incidents occur, responses are escalated in a timely manner and people are empowered to take the necessary actions as required. The standard is also aligned with several other internationally recognized management system standards, such as ISO 9001 (quality management) and ISO 14001 (environmental management). As such, **ISO 22301** can be integrated into an organization's existing management processes.

Attaining ISO 22301 certification demonstrates that an organization has met stringent criteria and adopted international best practices. This will reassure clients, suppliers, regulators and other stakeholders that the organization has sound systems and processes in place for business continuity. In turn, this

further improves business performance and organizational resilience. More importantly, the journey towards ISO 22301 certification will enhance an organisation's understanding of its business through analysis of critical issues and areas of vulnerability.

## Key Components of ISO 22301

---

ISO 22301 covers the following main areas:

**Organization** - An organization needs to understand both its internal and external needs, as well as set clear boundaries for the scope of its management system. More specifically, this requires an organization to find out all the requirements of relevant interested parties, such as regulators, customers and employees. It must also understand the applicable legal and regulatory requirements. This will determine the scope of BCMS.

**Leadership** - ISO 22301 emphasises the need for strong leadership in BCM. Top management need to ensure sufficient resources, establishes policy and appoint people to implement and maintain the BCMS.

**Planning** - An organization must identify risks associated with implementation of the management system and set clear objectives and criteria that can be used to measure its success.

**Support** - For business continuity to be successful, it is important for people with relevant knowledge, skills and experience to contribute and respond to incidents when they occur.

**Operations** - An organization must undertake business impact analysis to understand how its business is affected by disruption and how it changes over time. Steps to avoid or reduce the likelihood of incidents are developed alongside those to be taken when incidents occur. As it is impossible to completely predict and prevent all incidents, the approach of balancing risk reduction and planning for all eventualities is complementary. Essentially, it is about "hoping for the best but planning for the worst".

## BCMS for all

---

The requirements specified in ISO 22301 BCMS are generic. As such, it is applicable to every organization, regardless of industry, size and

type. The intention is to support organizations in effectively managing the impact of a disruption to its normal operation. While business disruptions are inevitable, some are costly but recoverable, while others are cataclysmic and result in the complete loss of business, such as the 2021 major flood in Malaysia that hit businesses in Shah Alam.

BCMS is the tool used to manage a situation after a disruption. It helps guide an organization through the critical steps required to continue its operations. A company needs to understand the extent and type of impact it is willing to accept and develop a business continuity system sized correctly for its need.

**ISCB** is a department within **CyberSecurity Malaysia** that manages certification services that includes BCMS Certification Scheme based on the ISO 22301 international standard. Through BCMS, an organization can implement and maintain a response structure that will enable timely warning and communication to relevant interested parties.

## How to get started?

---

To consider implementing BCMS and readying it for ISO 22301 certification, one must ascertain which parts within an entity are to be included in BCMS, taking into account location, size, nature and complexity. It is also important to identify which products and services need to be included in the BCMS.

The management needs to perform a readiness assessment to know where it stands in relation to the standard's requirements and what level of resources are required to meet them. It must also undertake a business recovery exercise to identify what steps to take should there be a major disruption to its business.

## BCMS Certification Steps

---

### Audit by Certification Body (CB)

A 2-stage audit process will be carried out by CB to audit the organisation's BCMS documentation and evaluate the organisation's location and site-specific conditions. Stage 1 entails CB collecting and documenting information on the scope of the management system, processes and location(s) of the organisation; and related statutory and regulatory aspects and compliance.



10

Stage 2 audit evaluates the implementation, including effectiveness of the organisation's BCMS. Where non-conformities are observed, the CB will formally document it in a Non Conformity Report (NCR)/Opportunities For Improvement (OFI) template. The organisation should define all non-conformities and provide an appropriate set of corrective actions to resolve the identified non-conformities.

### Approval & Issuance of Certificate

All information and audit evidence gathered during audits will be analysed and CB will make a final decision after all non-conformities have been resolved. Once approved for certification, the organisation will be entitled to receive a copy of the BCMS certificate. A CB grants to the organisation, upon receipt of the certificate, a non-exclusive, non-transferable and revocable license to use a certification mark applicable to the scope that has been certified in the manner described by the CB.

### Critical Success Factors

There are several critical success factors in implementing BCMS. First and foremost, strong commitment and support from top management. Implementing BCMS may involve costs for competency development, resource provision and business continuity strategy solutions. Active engagement by the organisations' leaders is therefore vital in ensuring monetary support and critical resources for developing and maintaining a BCMS. Top management buy-in is also crucial to garner more participation and support across every business unit.

The second factor is competency and knowledge of a BCMS leader. He or she must not only be competent in the technical aspects of BCM but also in management systems. BCM focuses on conducting Business Impact Analysis and Risk Assessment, developing BC Plan and Procedures, identifying BC strategy, developing of recovery procedure as well as planning for BC testing. On the other hand, management system entails establishing a framework to ensure the BCM programme is executed effectively and maintained properly.

Last but not least, periodic testing and review is crucial for implementation success. Since BCM will only be brought into action when a disruption occurs, periodical testing and reviews of the system, its processes and rationale is necessary to ensure it remains effective and aligned to a changing organization.

## Is Your Organization Well-Prepared?

---

Disasters can strike at any time, from large-scale natural catastrophes and acts of terror to technology-related accidents and environmental incidents. BCMS implementation involves clear methodical procedures which must be understood and supported at every level. It compels an organisation to regularly update its disaster response procedures and rehearsing its execution. Through BCMS, each and every member of an organisation needs to constantly ask what steps can be taken to prepare for the future. It forces everyone to be 'ready' for anything during these volatile times.

# Power Of ISMS: Driving Value & Growth For SMEs In Malaysia

By | Wan Shafiuiddin Zainuddin, Noor Aida binti Idris & Mohd Haleem Abdul Sidek

As Malaysia progresses swiftly towards becoming a Digital Economy, businesses large or small need to review their operations and processes to embrace digitalisation. Over the past two years, the Covid-19 pandemic has also necessitated Malaysia's SMEs (small and medium enterprises) to digitalise in order to survive due to changing market requirements.

## Why should one care about information security?

The core of a business organisation's assets is its information. Information security protects customers and trade secrets. A strong security ecosystem guards against any information risks – be it externally through cyber breaches or worse still, internally through leaks by employees or associates due to disgruntlement or lure of monetary payoff. Protection of personal records and commercially sensitive information is therefore critical within any organisation.

Data breaches are becoming more rampant and severe, yet many organizations still assume they will never suffer one. Most SMEs underestimate their risk level for cyber-attacks. A report by Chubb found that 67% of Malaysian SMEs believed that they are **less likely** to become victims compared to larger corporations, yet the same report found that 84% of SMEs were victims of cyberattacks in 2018. According to Cybersecurity Malaysia, 8,669 cases of cybersecurity incidents were reported to Cyber999 help centre from January to November 2021, the top three categories being fraud, intrusion and malicious code.

It has become mission critical for information to be secured to ensure its **Confidentiality** – meaning data can only be accessed by authorized people; **Integrity** – by keeping data accurate and complete; and **Availability** – data to be accessed as and when it is required. In short, “CIA” of information management.

Information Security Management System (ISMS) is a system of processes, documents, technology and people that helps manage, monitor, audit and improve an organisation's information

security. One of the most accepted international information security standards is **ISO/IEC 27001**. ISO/IEC 27001 is the international standard for companies that needs a robust approach for managing information security and building resilience. It is a framework that enables organisations to manage security incidents holistically and systematically.

Implementing ISO/IEC 27001 will improve internal working relationships and help retain existing customers, as well as provide a proven marketing edge against competitors. More importantly, an ISO/IEC 27001-certified ISMS also helps protect an organisation against cyber-attacks and the financial and reputational damage as a result.

With ISMS certification, organisational information is secured in all its forms. Rules will be put in place governing how an organization identify risks, to whom risk ownership is assigned, how such risks will impact the confidentiality, integrity and availability of information, and the method of estimating the impact and likelihood of risk. Such methodical approach increases the organisation's resilience to cyber-attacks and provides a centrally managed framework that keeps an organisation's information safe and all in one place.

Robust cyber security requires an ISMS built on three key pillars: **People**, **Processes** and **Technology**. By implementing ISMS, one can secure information, increase resilience to cyber-attacks, and reduce costs associated with information security.

ISMS' holistic approach covers the entire organisation, not just IT. This enables employees to readily understand the risks and embrace security controls as part of their everyday working practices. Most importantly, ISMS offers organisation-wide protection from technology-based risks and other more common threats such as poorly informed staff or ineffective procedures.

The main challenge of ISMS implementation lies in the organization itself – whether its top management has the commitment and determination as implementation requires

resources from all levels. Strong commitment from management helps the staff better appreciate ISMS implementation; and not just for the sake of getting certification. A lack of clear understanding of ISO/IEC 27001 standard and information security will definitely be a stumbling block. Therefore, ISMS implementation must be embraced by all. Achieving such certification increases transparency and efficiency in an organization. It also enables an organisation's capability to become **Measurable, Verifiable and Improvable** for future growth.

ISMS scope and boundaries determine the extent to which ISMS is applied. Identifying the right ISMS scope is crucial because it will assist organisations in meeting their security requirements and planning for ISMS implementation such as determining resources, timeline and budget required.

"This is best determined by the organization itself as they will know what are the critical services or information that need protection in terms of 'CIA'. Many organizations without the "right" scope end up getting little or no commitment from the top management, or being questioned about the benefits of ISMS implementation," said Wan Shafiuddin Zainudin, Head of Information Security Certification Body (ISCB). Therefore, it is important to have good knowledge of ISO/IEC 27001 standard and other 27000 standards group.

The ISMS scope should be derived from an organisation's known risks. For example, in a financial institution, the risks of unauthorised access of online transactions may result in critical impact to its business operations. Thus, the ISMS scope for this financial institution should be on its online transaction services. For clarity, organisations should seek the advice of a Certification Body (CB) on the proposed ISMS scope and boundaries, as and when the need arises.

The **Information Security Certification Body (ISCB)** is a department within the national cybersecurity specialist agency, **CyberSecurity Malaysia**. ISCB manages and provides certification services based on three main international standards and guidelines, namely Common Criteria (ISO/IEC 15408), ISMS (ISO/IEC 27001) and the World Trustmark Alliance (WTA) Code of Conduct. ISCB's **CSM27001 scheme** provides a model for certifying organisations against the internationally recognised MS ISO/IEC 27001 ISMS standard.

The process of ISMS certification can be divided into 6 main stages:

## Engagement with Certification Body (CB)

The organisation can engage with a CB to discuss the organisation's ISMS scope for certification. A CB will verify and ensure that the scope and boundaries of an organisation's ISMS are clearly defined in terms of characteristics of business, its location, assets, and technology.

## Enquiry and Quotation

Organisations should complete an enquiry form and forward it to the CB for application review. If there is a need to obtain more information about the organisation's ISMS, or if there is a need to clarify some of the details contained in the application, then CB will contact the organisation to obtain the required additional information.

Once the CB is satisfied with the organisation's application, a quotation will be generated for the certification work to be done. If the organisation accepts the quoted price, provision for legal agreements will be made.

## Stage 1 Audit

Part of Stage 1 audit is carried out at the organisation's premises to audit the organisation's ISMS documentation and evaluate location and site-specific conditions. The CB will collect necessary information regarding the scope of the management system, processes and location(s) of the organisation; and related statutory and regulatory aspects and compliance. Stage 1 audit findings will be documented and communicated to the organisation, including identification of any areas of concern that could be classified as non-conformity.

## Stage 2 Audit

Stage 2 audit evaluates the implementation, including effectiveness of the organisation's ISMS. Where non-conformities are observed, the CB will formally document it in a Non Conformity Report (NCR)/Opportunities For Improvement (OFI) template. The organisation should define all non-conformities and provide an appropriate set of corrective actions to resolve the identified non-conformities.

## Certification Approval

All information and audit evidence gathered during Stage 1 and Stage 2 audits will be analysed in order to review the audit findings and agree on the audit conclusions. The CB will make the final decision after all non-conformities have been resolved

## Issuance of Certificate

Once approved for certification, the organisation will be entitled to receive a copy of the ISMS certificate. The ISMS certification is valid for 3 years; however ISMS certified status need to be maintained by the organisation and subject to surveillance audits by CB. To renew for a further term of 3 years, an organisation needs to notify their CB and provide updates on their ISMS implementation. A recertification audit will then be conducted before expiry of the certificate. If certification is successfully renewed, similar process of surveillance audits will be carried out by Certification Body.

Information security is only as strong as the weakest link. Through ISMS certification, an organisation can develop a culture of security by integrating security into its corporate structure and daily operations. Utilizing a reputable certification body also enables one to gain customers' trust in certification. Therefore, maximize the return in investment by leveraging on the reputation of a recognised certification authority such as ISCB.



# Leveraging MyCC Certification To Boost Malaysia's ICT Exports

By | Wan Shafiuddin Zainuddin, Hasnida binti Zainuddin & Mohd Haleem Abdul Sidek

Companies and governments around the world depend on information and communications technology (ICT) products and services. They rely on ICT to maintain national and economic security, public safety and law enforcement, as well as protect confidentiality of their data and the data of citizens. These users are also increasingly concerned about cyber security risks. In today's digital world, new cyber security risks emerge every hour of each day. Organizations suffering from hacker attacks are susceptible to losing control of confidential data and millions of ringgit in reputational damage and business losses.

The Common Criteria (CC) is an international standard defining a framework for IT security evaluation and certification. It provides value to customer by having independent third party to evaluate and validate these security requirements against recognized industry standard criteria. More so, if that third party is credible and accredited by government certification scheme.

## Vulnerabilities in IoT Devices

Technological advancements and proliferation of smart devices are requiring higher security assurance levels due to high cybersecurity risks. According to a recent World Economic Forum (WEF) report, consumer Internet of Things (IoT) market size from wearables to electronics and home appliances is forecasted to reach about US\$154 billion by 2028. However, these new ICT products coming onto the market continue to introduce vulnerabilities. The ICT sector is also one of the fastest-growing sectors in Malaysia, which contributed to 19.1 percent of the country's GDP in 2019 and is expected to reach 22.6 percent by 2025.

To ensure a resilient infrastructure for enterprises and safer consumer ICT products, cybersecurity must be an important consideration when companies design their systems and networks. Establishing cybersecurity measures will benefit companies by protecting them from any reputational and financial risks posed by cyber

threats; while more cyber robust consumer ICT products will ensure a pleasant user experience free from hackers.

ICT product companies must therefore adopt a Security-by-Design approach which is more cost-effective than implementing cybersecurity measures only after systems have been designed and built. As such, product assurance, whereby products are evaluated and certified based on international standards such as **Common Criteria (CC)**, is a critical step in reducing cyber-attack surface and make the ICT products more marketable.

## Defining Security Requirements

As mentioned, Common Criteria (CC) is an international set of standardized guidelines and specifications developed to evaluate information security products. It is a framework in which users specify their security functional requirements (SFRs) and security assurance requirements (SARs). Technology vendors can then implement and/or make claims about the security attributes of their products and engage certification bodies to evaluate their products to determine if they meet these claims.

CC provides assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous, standard and repeatable manner at a level that corresponds with its target use environment. Once this process is completed successfully, a vendor achieves Common Criteria certification.

Also known as **ISO/IEC 15408**, CC is the internationally recognised standard for the basis for evaluation of security properties of IT products, while Common Evaluation Methodology (CEM) or **ISO/IEC 18045** is minimum actions required by an evaluator in order to conduct an ISO/IEC 15408 evaluation. Both CC and CEM are the technical basis for the international agreement named as Common Criteria Recognition Arrangement (CCRA).

As of 2019, thirty one countries signed the CCRA, thus providing an unparalleled measure of security for the international commerce of ICT products. Malaysia, through CyberSecurity Malaysia, has been accepted as CCRA Consuming Participant in 2007 and recognized as CCRA Authorizing Participant by 2011. As such, participants can gain access to a global community of technical experts, who together identify and address the threats.

## Common Criteria in Malaysia

In Malaysia, Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme is set up to evaluate and certify the ICT products against the Common Criteria standards. **MyCC Certification Body (MyCB)** is the entity that provides the CC evaluation and certification services against the ISO/IEC 18045 and ISO/IEC 15408 requirements. The MyCB function is operated by Information Security Certification Body (ISCB), a department within CyberSecurity Malaysia.

## Evaluation types in Common Criteria

Common Criteria has two types of evaluation approaches, which are:

- i. Evaluation on ICT products and systems based on the Evaluation Assurance Level (EAL); and
- ii. Protection Profiles (PP) Evaluation focusing on defining the baseline criteria of specific technology or product ecosystem.

EAL defines the depth and coverage of product through security evaluation based on the security functional requirements (SFRs) as defined in the Security Target (ST) document as reference in CC that specifically elaborate the scope of work or Target of Evaluation (TOE). There are seven Evaluation Assurance Levels (EALs). The higher the EAL chosen by the consumer or developer for product evaluation, the level of confidence increases in the method of evaluation onto the SFRs defined by the ST. In another words, the higher the EAL, the better the results of security evaluation and confidence for the intended consumer. Each EAL corresponds with a package of Security Assurance Requirements (SAR).

PP is a document developed by a specific community that defines the baseline of security requirements for a specific type of product/ technology/ ecosystem (e.g., network equipment and single sign on system) which is relevant to the intended end user such as government, industry sector or consumer with set of defined objectives. Product developers or manufacturers may choose to develop products which conform to one or several PPs, whilst submitting their products to be evaluated based on the minimum EAL requirement defined by the PP(s).

## Certification Process

CC addresses protection of information from unauthorised disclosure, modification, or loss of use. The categories of protection related to these three types of security failure are commonly called **confidentiality, integrity, and availability**, respectively.

CC is presented as a set of distinct but related parts:

**Part 1** - Introduction and general model

**Part 2** - Security functional requirements establishes a set of functional components that serve as standard templates upon which functional requirements for TOEs are based.

**Part 3** - Security assurance requirements establishes a set of assurance components that serve as standard templates upon which assurance requirements for TOEs are based.

The first step in submitting an ICT product for CC certification is to complete the Security Target. One needs to describe an overview of the product, its security features, an evaluation of potential security threats, and a self-assessment detailing how the product conforms to the relevant **Protection Profile (PP)**, or the **Evaluation Assurance Level (EAL)** chosen to test against.

The second step is to generate assurance documentation that are required for an evaluation process. Next, the product and its associated documentation are submitted to MyCB via an accredited testing laboratory. MyCB and the testing laboratory shall verify the product's security features and evaluate its compliance based on the specifications outlined in the PP or EAL. Successful evaluation will form the basis for an official certification of

the product conducted by the testing laboratory and MyCB.

In Malaysia, evaluation facilities for the MyCC Scheme is known as **Malaysian Security Evaluation Facility (MySEF)**. There are currently four<sup>1</sup> Security Evaluation Facility (SEF) licensed under MyCC Scheme.

The goal of CC certification is to assure customers that the products they are buying have been evaluated and that the vendor's claims have been verified by an independent party.

CC certification will help ICT product buyers reduce risk by procuring and using products that have sufficient security and integrity for their environments. By factoring security into procurement decisions, buyers in turn incentivize ICT vendors to develop and provide more secure and robust ICT products.

## Challenges of CC Certification

ICT product developer needs to have a thorough understanding of the requirements in order to prepare CC documentation and successfully complete the evaluation. Furthermore, a high level of commitment is required during evaluation so that the project timeline can be met. Budget could present another challenge for smaller organisations as CC typically involves higher cost for the evaluation facility service and certification.

Nevertheless, CC certification achieves the following critical objectives:

- **Better Access to Government Tenders**

Most governments across the globe require Common Criteria certification in their ICT product procurement. As such, Malaysian ICT products which are CC certified will qualify for tender.

- **Enhance Market Competitiveness**

For better market share access, Common Criteria certification is critical to compete with other well-established IT products which have been evaluated.

- **Product Certification Signals Quality**

Certification brings a level of quality assurance for enterprise IT buyers. Stringent evaluation process may uncover previously unknown vulnerabilities that can be addressed before sending a product to market, preventing costly post-release patches.

---

<sup>1</sup> <https://iscb.cybersecurity.my/en/index.php/certification/product-certification/mycc/licensed-mysef>

# Preservation Of Digital Evidence

By | Hanania Aida Mohd Hilmi & Nor Salwani Ja'afar

## Introduction

Digitalization has resulted in information and communication technologies evolving rapidly. As a result, criminals have new opportunities and ideas to carry out cyberattacks. Cybercrime not only affects individuals but also negatively impacts social and economic development. Among the causes of a surge in cybercrime are weaknesses in law enforcement and a lack of public awareness.

The era of digital technologies brings to focus the importance of digital forensics to the courts of laws. A decade ago, digital forensics ransomware used on cybercrime such as online fraud, phishing, ransomware and etc. These days, most information or data are saved or transferred in digital medium which could be used for crime investigation. For example, a man was arrested and investigated under Section 428 of the Penal Code for animal abuse. The sadist incident was committed when the suspect offered some food to a stray cat to lure it out. The suspect then threw a palm-sized stone at the cat's head as the cat was feeding on the food. The case went viral after a shop worker witnessed the suspect's cruel act on the premises' closed-circuit television (CCTV) camera in Taman Semeling Maju in Bedong. The footage was later uploaded to Facebook. In this case, the CCTV's footage became a digital evidence and was used during the court's hearing (Zulkifli, 2022).

Digital forensics is defined as a process that involves multiple phases from identification, preservation, analysis, documentation, to presentation of digital evidence which can be used in a court of law. In this article, we will focus on the second phase, which is preservation process. According to Williams L. (Williams, 2022), preservation could be defined as isolating a network, securing, and copying data from actual digital evidence, packaging, transportation, and storage of the said information.

To ensure that digital evidence gathered is the same as it was first found, not manipulated or deleted, proper procedures and environmental conditions should be followed and adhered to. Preservation is crucial in digital forensics as a control to ensure that the integrity of evidence

is preserved from the point where the subject was first taken to the time it is recorded as exhibits by an investigation officer (IO).

## Preservation Processes

Organisations are encouraged to refer to local law enforcement agencies for guidance on the best way to preserve digital evidence. As the character of a digital evidence is always fragile and volatile, procedures and protocols must be followed strictly to avoid any mishandling that will affect the quality of evidence. The first stage in digital evidence recovery is preservation, which is the process of seizing and securing property of suspects without altering the contents of data stored on the devices (Rafael, 2017).



Figure 1: The process of Preservation in Digital Forensic

## Identification

The step begins by first determining the type of item. If it is unrelated to the digital forensic request, they simply mark it as processed and proceed. If an examiner discovers an item that is incriminating but outside the scope of the original search warrant, it is recommended that the examiner immediately stop all activity, notify the appropriate individuals, including the requester, and wait for further instructions, just as in a physical search (Oliver, et al., 2008). Generally, identification stage involves examining to identify type, location, format and condition. Mobile phones, personal computers, servers, network or etc of storage media can all be a digital source. According to (Cohen, 2009) recognizing and classifying an incident is dependent on indicators. Although this is not directly related to forensics, it is significant because it affects other steps.

## Collection

According to (Palter, 2021) once all of information has been recorded, one can begin collecting the physical media on which digital



evidence was stored or was accessed. During collection, minimize changes to the device's condition as much as possible. The collection is then handed over to legal custody of a repository (if it supports the mission statement of the repository) before planning begins to determine whether to collect digital evidence, acquire data, or both and to ensure that all steps taken towards gathering digital evidence follow the correct procedure. Figure 2 below shows a case management procedure.

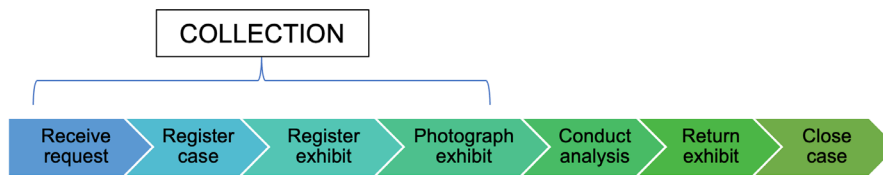


Figure 2: Case Management Procedure

### Receiving a request

The work of the Digital Forensic Laboratory begins upon receipt of a formal request from a Requester. A formal request is acceptable in the form of a letter, an e-mail, or fax. Such request should include the following information: a description of the crime, any related acts, details on electronic evidence, and the case objective as well as the warrant (Interpol, 2019).

### Registering a case

According to (Interpol, 2019), once the Digital Forensic Laboratory determines that the case is viable, the requester will deliver all electronic evidence to the Digital Forensic Laboratory. The Digital Forensic Laboratory assigns a unique running case number and completes a case registration form.

### Registering an exhibit

Once electronic evidence (exhibits) is received, it must be sealed before custody is transferred to the Digital Forensic Laboratory. To remove any reasonable doubt about the evidence's integrity, both the Requester and the Examiner must be able to show that no one else gained access to the evidence during the transfer process. Although this procedure is new and costly for some agencies, the Digital Forensic Laboratory maintains constant monitoring and provides a firm timeline for agencies to start practising this procedure (Interpol, 2019).

### Photographing an exhibit

A photograph of every exhibit is taken for two reasons: to record the exhibit's current state and to enable it to be effectively identified in the future. Photograph is captured of the overall and close-up views of the exhibit. The screen display is photographed as well if it is active. After that, the images should be uploaded to a case folder. It is recommended that you photograph the exhibit before returning it to the Requester for future reference (Interpol, 2019).

## Acquisition

An acquisition is a process of gathering and recovering sensitive data. The approach to performing acquisition depends on the type of digital evidence. For example, the process to acquire evidence from a computer hard drive is different from a mobile device such as a tablet or smartphone.

An acquisition is also important to maintain the integrity of the evidence while analysis is being performed on a copy of it. According to (Interpol, 2021) one of the main premises in the forensic analysis process is that unless there are exceptional circumstances, examination of the evidence should not be performed using the original device.

### Live acquisition and dead acquisition

First and foremost, the method to acquire evidence must be decided. There are two methods of acquisition namely live or dead acquisition. A live system is a system that is up or running and switching it off may cause a loss of volatile data. Conversely, leaving the running systems may cause evidence to be modified or deleted.

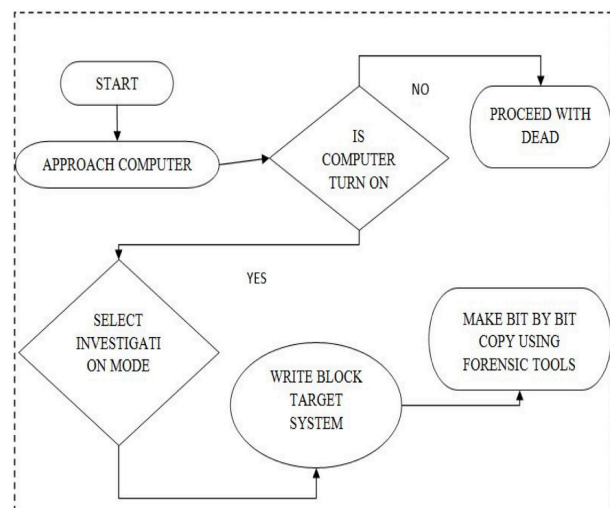


Figure 3: Live Forensic Image Acquisition

For dead acquisition, evidence is extracted from seized digital devices at a forensic laboratory. The acquisition is usually done on devices which are powered off and if in the case of hard disk, removed from its potentially compromised system.

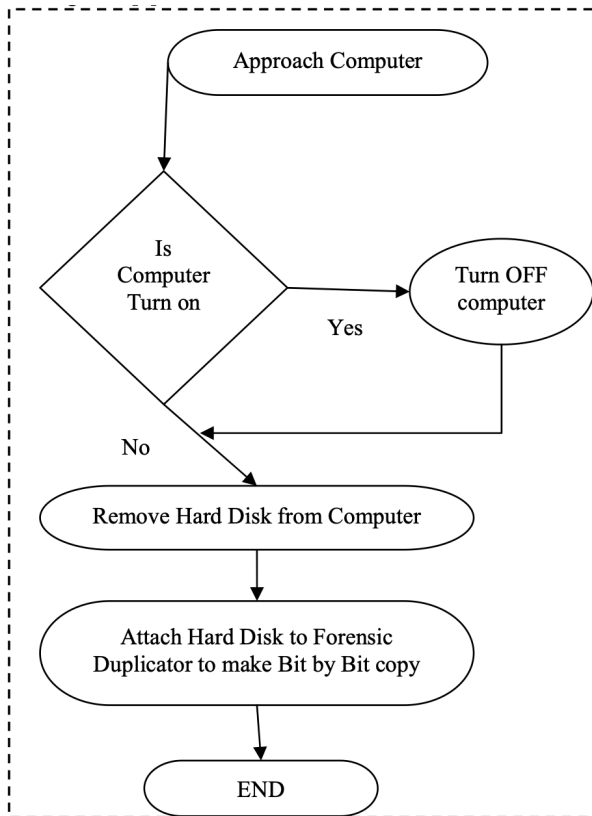


Figure 4: Dead Forensic Image Acquisition

### Clone and Image

A copy must be an extracted bit-by-bit as replica of the original device or digital evidence. There are two formats for processing copies. Figure 3 shows two types of copying process from the original device.

Device to Device (Clone)
<ul style="list-style-type: none"> <li>This can be accomplished by creating an exact bit-by-bit replica of a previously wiped original device in another device of equal or greater capacity</li> </ul>
Device to File (Image)
<ul style="list-style-type: none"> <li>This can be accomplished by creating one or more files containing, linked together, an exact replica of the original device. The most common are "dd" (raw) and "E01".</li> </ul>

Figure 3: Two formats of the process of copying from the original device

The HASH function, also known as summary function, is used to check the integrity of a data set. In other words, it is necessary to obtain its "fingerprint." This procedure is used for electronic evidence during duplication of original devices to ensure that the HASH value of the origin and destination are identical. This is referred to as verification (Interpol, 2021).

The entire acquisition process must be documented from detailed information about the digital devices, hardware, and software used to extract the evidence, as well as when, where, why, and what evidence was obtained. The chain of custody will ensure proper handling of the evidence.

## Conclusion

Handling evidence is the most important aspect of digital forensics. It is imperative that digital evidence remain intact, as such evidence from devices such as smartphones and laptops can be useful in court. Acquiring this evidence correctly is critical for data protection and integrity and to ensure evidence is admissible in court should legal action be taken. It will also help prevent accusations or any risk of improper collection procedures thus rendering such vital evidence inadmissible in the court of law. The aim of digital preservation is to sustain our ability to view, retrieve, and use digital collection, despite a rapid change in the infrastructure and in technological and organizational elements. The digital evidence preservation model increases the admissibility of digital evidence in court. This model takes into consideration all common aspects as well as those required by the courts.

## References

- Cohen, F. (2009). Two models of digital forensic examination. 4th International Workshop on Systematic Approaches to Digital Forensic Engineering, SADFE 2009, 1(3), 42-53. <https://doi.org/10.1109/SADFE.2009.8>
- Interpol. (2019). GLOBAL GUIDELINES FOR DIGITAL FORENSICS LABORATORIES INTERPOL For official use only. May.
- Interpol. (2021). GUIDELINES FOR DIGITAL FORENSICS FIRST RESPONDERS Best practices for search and seizure. Interpol, March.
- Oliver, C., Brannon, S., & Song, T. (2008). Usab5601.Pdf. <http://www.justice.gov/sites/default/files/usao/legacy/2008/02/04/usab5601.pdf>
- Palter, J. (2021, April 19). Preserving Digital Evidence the Right Way: Your 10-Step Guide. Real Time Network. <https://www.realtimenetworks.com/blog/preserving-digital-evidence-the-right-way-your-10-step-guide>
- Williams, L. (2022, July 9). What is Digital Forensics? History, Process, Types, Challenges. Guru99. <https://www.guru99.com/digital-forensics.html>
- Zulkifli, A. (2022, June 21). Suspected cat abuser remanded for 3 days. New Straits Times. <https://www.nst.com.my/news/crime-courts/2022/06/806911/suspected-cat-abuser-remanded-3-days>

# NFT: A New Medium For Money Laundering?

By | Siti Nurzakirah Binti Moham Shahrum, Aisyah Binti Mohamad Hafizul, Sharifah Nurul Asyikin Syed Abdullah & Sarah Khadijah Taylor

In April 2022, Nike sold its NFT sneakers for more than USD100,000 in the marketplace<sup>1</sup>. In March 2021, the first Cristiano Ronaldo NFT was sold for USD290,000 on fantasy soccer game Sorare<sup>2</sup> while on 'Everydays', the most expensive NFT ever sold was USD69.3 million in March 2021<sup>3</sup>. These trends underscore the rise of NFT as a popular way to buy and sell digital artwork among users.

But is there more to NFT than meets the eye?



Figure 1: One of the NIKE digital shoes selling in Opensea.io



Figure 2: First ever Cristiano Ronaldo NFT sold

## What is NFT?

NFT or 'Non Fungible Token', is a digital representation of art, music, and in-game items such as desired outfit for characters, videos, trading cards and so on. These items are regularly purchased and sold online using cryptocurrencies. Each NFT has its own unique identity and feature, making each piece distinct even if they appear similar on the surface. NFTs help establish proof of ownership in the digital world with only one official owner at one time. For example, while there are a lot of Messi football jerseys being sold in the marketplace, only Ali owns the jersey with Messi's signature.

The most well-known and largest crypto market platform for trading NFT is Opensea.io.



Figure 3. CryptoPunk #3100, which was sold for USD7.51 million in March, 2021

## Why NFT?

One of the advantages NFT offers is that it can protect the ownership of any works of art, music or any other property. Paintings and other traditional physical works of art are valuable due to their uniqueness. Digital files, however, can be easily copied. By using NFTs, a digital certificate of ownership for the artwork is "tokenized" and traded. Digital files can be protected by uploading them as NFT to prove originality as the first creator of the art, music or any others.

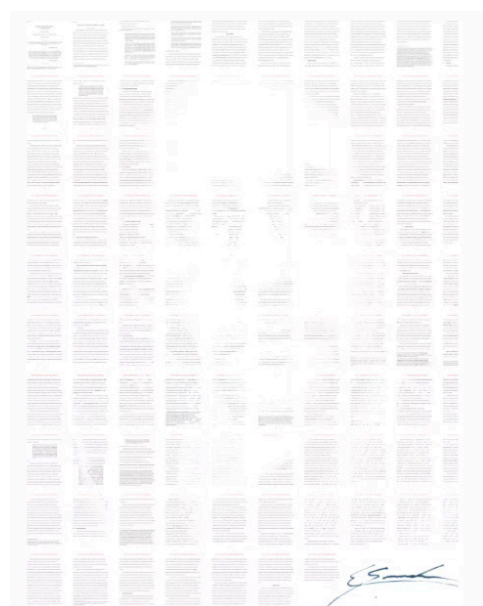


Figure 4. Edward Snowden's NFT called 'Stay Free' sold for USD5.4million in April, 2021

## How does NFT work?

Suppose a piece of digital art has been created. The digital art is then uploaded and minted on a marketplace such as OpenSea.io or Rarible.com. The creator then sets a price for the art and lists it for sale. When an interested buyer paid for the art, the ownership would be transferred to the said buyer. Subsequently, should the buyer succeeded in selling the art to another party, the original creator will receive a sum of royalties for the art that he has created. These transactions between three parties are recorded in blockchain, thus rendering the records immutable. This makes it secure and auditable by any other parties.

### Non-fungible token vs fungible token

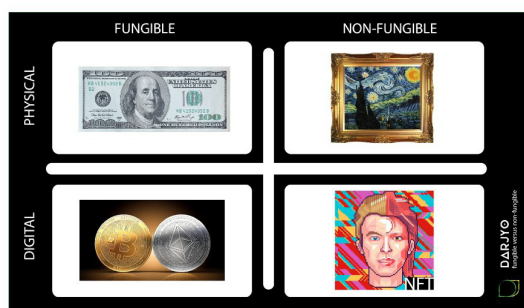


Figure 5. The difference between fungible and non-fungible goods

## NFT Royalties

One of the most notable qualities for NFT is its feature that pays royalties to artists and designers even after their artworks have been transferred.

In NFT, when an artist's work is resold, NFT gives royalties based on a set percentage of the sale price. The royalties will always be paid to the original creator. Thanks to the power of blockchain and smart contracts, the entire process is automated.

The quantity of royalties to be received by each artist is determined by the terms specified in the smart contract when the creator upload the NFT for sale. With OpenSea.io for example, creator can set the royalty up to 10% of the selling price, which means that the artist will earn a full 10% on all subsequent future sale of their artwork.

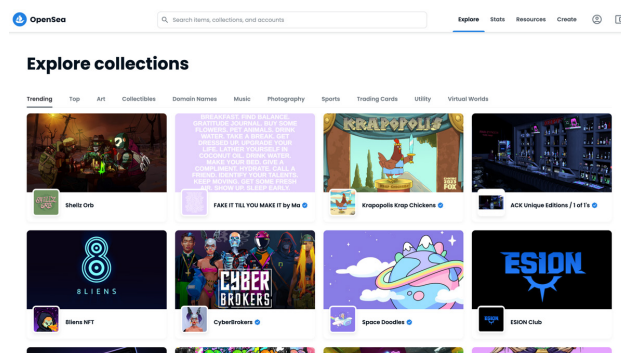
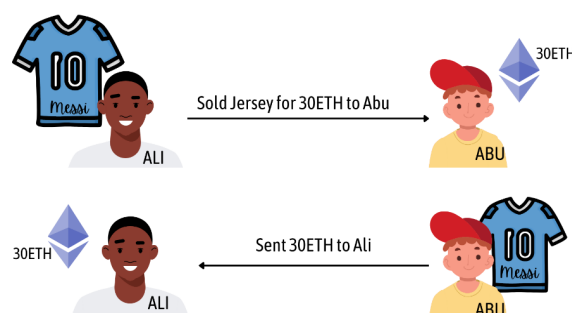


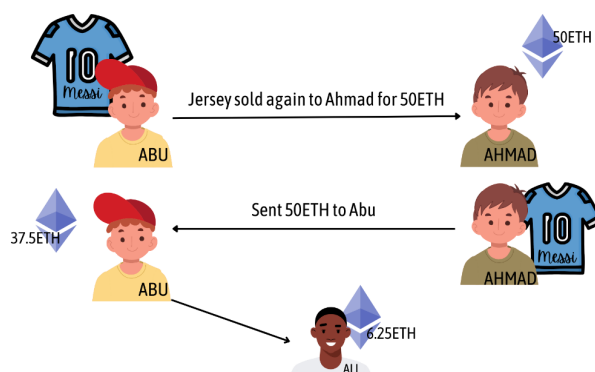
Figure 6. The opensea market, a platform for selling and buying NFTs

The selling and buying process and royalties earned of an NFT can be further visualized below:

1. Ali is selling his NFT for RM30 in OpenSea.io and he has set it to receive 2.5% of each selling price. Abu is interested in buying and agrees to pay RM30 for the item.



2. Now, Abu has the item and wants to sell it for RM50 to Ahmad. 2.5% of the RM50 (RM12.50) will be given to Ali for the royalty and the remaining will be received by Abu.



NFT gives creators full control of their digital artwork because through blockchain, all processes are automated without the use of a middleman, thereby enhancing profits for the creator.



Among benefits of NFT royalties are as follows:

- No dispute over ownership
- Payment methods are completely automated
- Perpetual royalty payments regardless of the number of secondary sales

## NFT and Money Laundering

Could the various advantages of NFTs make them a perfect vehicle for money laundering? Money laundering is a method used by criminals to disguise the source of funds, and their final destination. Laundering is carried out to provide the impression that the earnings come from a respectable source. Through a series of financial transactions, money laundering transforms unlawful income into legal currency or other assets.

NFTs, like any other blockchain securities and traditional art sales, can potentially be used for money laundering. Money laundering is a huge concern when it comes to art trading. It occurs when NFT sales are targeted to 'self-funded' addresses. Self-funded address meaning the transaction of buying and selling was done on different addresses but owned by the same person. According to a report by Chainalysis, a Singapore-based blockchain data platform, which used blockchain analysis has identified 262 users who have sold an NFT to a self-funded address more than 25 times<sup>5</sup>.

In a scenario for NFT money laundering, someone who has made a big sum of money by selling illegal drugs could create an NFT and purchase it back with another account, making it appear as though he obtained the money legitimately by selling a digital asset.

All of these crimes could be propagated due to the anonymous nature of NFTs. Blockchain technology has unwittingly created a favorable environment for money laundering. As NFTs could be worth as much as someone wants to pay for, prices can be absurdly high, and no one could dispute it. Furthermore, because they are often traded using cryptocurrency, it is much more difficult to follow the entire transaction and identify the perpetrator.

There are cases that happened in 2022, whereby NFT creators promised wonders to investors. In the case of Frosties NFT<sup>6</sup>, rogue NFT creators Mr Nguyen and Llacuna shut down their website and any other contactable platform and transferred the money after the NFT was sold. Consequently, the investors did not receive anything in return for buying the NFT.

## Outlook

If nonfungible tokens continue to be adopted across businesses from video gaming, music, art, to digital collections, the market could be worth USD231 billion by 2030<sup>7</sup>. The increasing number of users and transactions using NFTs will pose a challenge for law enforcement agencies and regulatory bodies to track money laundering activities performed by criminals. Law enforcement organisations would need to keep abreast of the new technology in order to stay one step ahead of criminals.

## References

1. <https://www.cbsnews.com/news/nike-cryptokicks-nft-blockchain-metaverse-rtfkt/>
2. <https://cryptobriefing.com/unique-cristiano-ronaldo-nft-sells-290000-sorare/>
3. <https://www.theverge.com/2021/3/11/22325054/beeple-christies-nft-sale-cost-everydays-69-million>
4. Woriji, Lawrence Mike. "Are NFTs Being Used for Money Laundering?" Altcoin Buzz, 8 Feb. 2022, [www.altcoinbuzz.io/nft/are-nfts-being-used-for-money-laundering/](http://www.altcoinbuzz.io/nft/are-nfts-being-used-for-money-laundering/).
5. <https://www.outlookindia.com/business/nft-frauds-on-the-rise-globally-says-study-news-183109>
6. <https://www.irs.gov/compliance/criminal-investigation/two-defendants-charged-in-non-fungible-token-nft-fraud-and-money-laundering-scheme>
7. <https://cointelegraph.com/news/nft-market-worth-231b-by-2030-report-projects-big-growth-for-sector>

# Dashboard Camera Footage As Evidence In Vehicle Crash

By | Muhd Syafiq Shamil Bin Shafie, Fakhru Afiq Bin Abd Aziz, Zabri Adil Bin Talib, Nurul Husna Binti Mohd Nor Hazalin, Muhammad Faridzul Bin Sukarni & Mohd Izuan Effendy Bin Yusof

## Introduction

Dashcams, sometimes referred to as dashboard cameras, are a popular aftermarket equipment among Malaysian vehicle owners. Demand for dashcam is rising primarily due to its many benefits. Currently, dashcam are frequently utilised by drivers, driving instructors, taxi and bus drivers, police patrol personnel, and other road users all over the world.

Dashcam is a low-cost video surveillance device installed on windscreen of an automobile that captures events on the road. It consists of a tiny camera that could be mounted on a car's front or back. Its ability to easily connect with various on-board technologies, such as recorders and GPS devices, is a key feature of this reasonably priced and feature-rich device.

Dashcam are mainly used by drivers who want to protect themselves from false accusations of traffic accidents and insurance frauds [1]. Their primary objective is to record vehicle safety-related incidences. Vehicle safety include accurately documenting traffic incidents or other incidents related to road safety, preventing confusion or misleading facts in witness statements.

## Dashboard Video Footage As Evidence

Evidence is information used by a plaintiff, prosecutor, or defendant at a legal proceeding in order for the court to rule in his/her favour. Without video evidence, a person's case could be instantly dismissed for lack of proof. Evidence could also include witness testimony, DNA or forensic evidence, or anything else that aids the court in determining whether one or both parties have proven the elements of their cases. If one party does not have evidence to back up what he alleges in court, the court or jury will not rule in his/her favour [2].

In terms of evidence, dashboard cameras are now being widely used to produce playback of

any collisions involving vehicles. The dashcam recording will be pivotal in proving one's innocence and reliability of testimony in court. Dashcam video can be used as indisputable evidence by a lawyer to support their legal case.

The investigation officer (IO) utilises dashcam video to substantiate traffic incidents. Normally, IO will conduct a full investigation by gathering data from all vehicles involved, retrieving evidence as well as measuring and mapping the crash site. Evidence Act 1950 mandates an investigation officer to present all photographic and videographic evidence necessary to assist the prosecution and court [3].

Dashcam footage helps insurance companies resolve claims for damage reimbursement. Installing a dashcam could also be advantageous, such as obtaining favourable insurance rates from insurance companies or obtaining evidence that can be used in legal procedures.

## Evidence Extraction

To be able to use dashcam footage as evidence, certain criteria need to be met [4]:

1. High-quality resolution
2. Focused and detailed optical recording
3. Quality recording in low light conditions
4. Sufficient frame rate
5. Immediate recording at impact (during and after the impact)
6. Ability to save and store the recording after impact
7. Ability to record and preserve data in case of severe mechanical damage caused to the camera.

The angles used from the dashcam must be appropriate and relevant. Therefore, the dashcam's viewing angle has to be set correctly. The front view of the dashcam should be in the middle. To ensure an equal field of vision is captured for both sides of a car, place the dashcam at the middle of the windshield, directly behind the rear-view mirror. Putting the

dashcam on any other location would not be optimal as the viewing angle would be limited. In addition, this would not block the driver's view, thus minimizing distractions. The field of view of the dashcam should not be blocked by any objects such as phone holders or windscreen stickers.

To ensure proper extraction, the first and most important step is to ensure correct timestamp recording for the dashcam. Owner of the dashcam should also check the dashcam's time setting once in a while, and note down the time offset between the dashcam and real Malaysia Standard Time, should there be any.

A footage should show the moment when impact occurred (during and after the impact). If the exact impact was not recorded, then the footage available in the dashcam would not be relevant as evidence.

There are three methods to extract a footage from the dashcam.

The first method is to remove the external memory from the dashcam. User can simply remove the memory card and insert it into a card reader [5]. The user can then just copy the video files into a computer without changing anything and leave in its original file format. Immediately produce the MD5 hash value of the copied

video files. This method is only applicable to dashcams with external memory.

If the dashcam does not have an external memory, there are several other ways to extract the footage. User can check if there is a proprietary app for the dashcam [6]. If it does, then it should be used to download the footage to a laptop or a quarantined area. Immediately produce the MD5 hash value of the copied video files after downloading it.

Two key pieces of information will be utilised to preserve the video's integrity as evidence. The MD5 hashing value information is one, while metadata information created after transferring them is another. Refer to Figure 1 and Figure 2 below for metadata example. The metadata shown is extracted by using Media Info software.

The second method is to check if the dashcam has a wireless transfer capability to transfer the footage. Immediately produce the SHA-1 hash value of the copied video files after downloading it.

Lastly, if the dashcam has a USB port, use it to download the data directly from the dashcam to a USB drive. Immediately produce the SHA-1 hash value of the copied video files after downloading it.

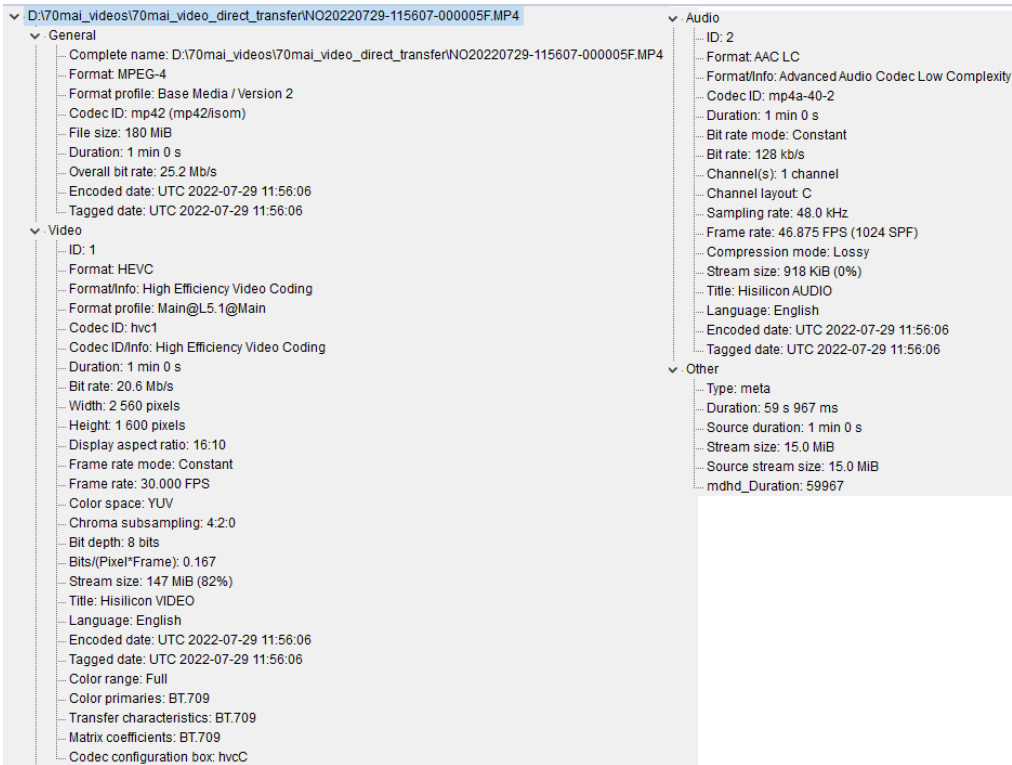


Figure 1: Direct transfer

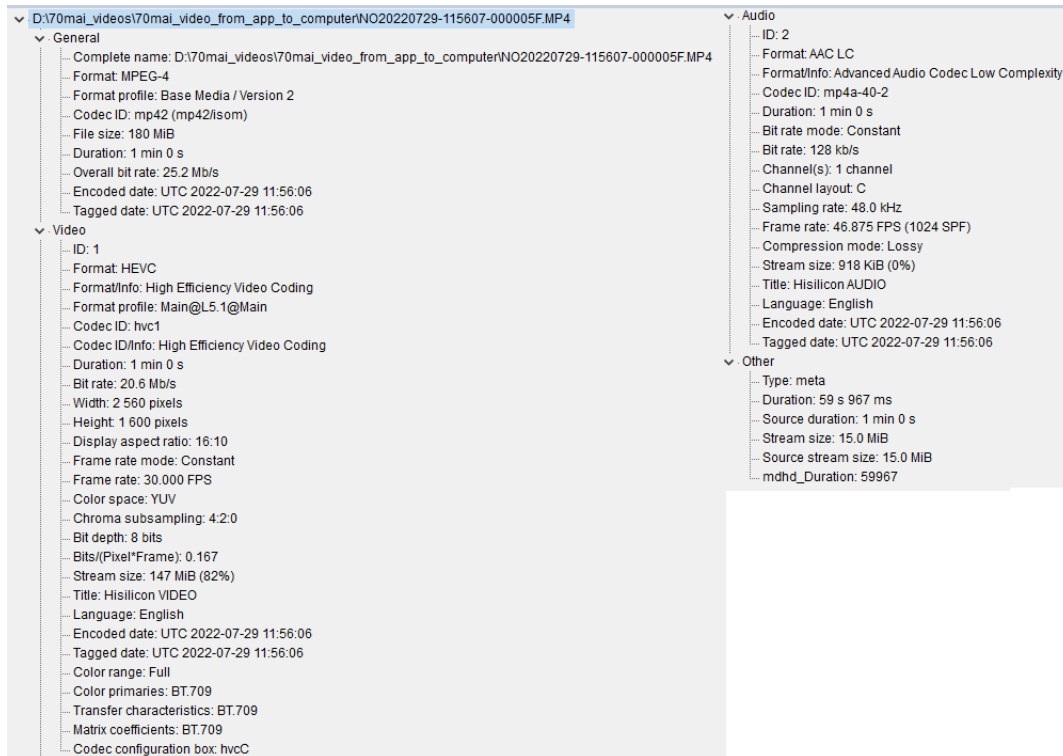


Figure 2: Transfer from proprietary app

The extracted video data should be verified before leaving the scene (or as soon as feasible thereafter) to verify that the retrieval operation has been successful [7]. This includes ensuring the related metadata and audio if they are present.

To verify the integrity of the evidence, footages obtained from direct transfer and transfer from app will be hashed by using Forensic ToolKit Imager. Below is the hash value result for two footages from direct transfer and transfer from app. It shows that the hash value result maintains the evidence integrity.

#### FileHash

MD5	FileNames
604f2cea02e5a99a0e9049078d1ba1e0	HASH\C:\Users\Talino\Downloads\HASH\70mai direct transfer\NO20220729-115607-000005F.MP4
604f2cea02e5a99a0e9049078d1ba1e0	HASH\C:\Users\Talino\Downloads\HASH\70mai transfer from app\NO20220729-115607-000005F.MI

Figure 3: Hash value dashcam file from direct transfer and transfer from app is exactly the same value.

Footage obtained from the dashcam must be maintained in the native file format so as to maintain evidential integrity and preserve picture quality [7]. If any editing is done, such as cutting, compressing, and reformatting video container (eg. AVI to MP4) then the original hashing value will not be maintained. As the footage should be in a physical device to transfer them, it must not be transferred into a text messaging application medium such as WhatsApp as this would compress the footage and damage the integrity of the footage.

Physical media, particularly small devices such as USB sticks or other flash media, should be wrapped to protect and reduce any possibility of damage or loss during travel [7]. When using USB flash sticks as transfer medium, they must be individually identified and recorded in the audit trail. CDs and DVDs should be stored in individual protective cases, not on a spindle. Flash cards should be kept in their original packaging or neatly wrapped. These should be stored in individual boxes with protective inserts and anti-static bags if possible.

All evidence should be packed and labelled in accordance with established processes, and the label on the box should contain enough information to identify the evidence.



## Conclusion

---

Pursuant to Malaysian Evidence Act 1950 (Act 56), dashcam footage can be submitted as a standalone evidence in a court of law, either in a civil or criminal case. While dashcams can be used as a tool to resolve accidents as well as other traffic or criminal-related matters, the devices can also serve as records for drivers to review their driving habits and make adjustments where necessary. The Malaysian Institute of Road Safety Research (MIROS) has lauded the adoption of dashcams as a positive development towards road safety initiative. By installing a dashcam that meets specification guidelines, and following the extraction processes as discussed above, the video footage can be relied upon as evidence.

## References

---

1. <https://www.freemalaysiatoday.com/category/bahasa/tempatan/2022/05/01/semakin-ramai-pasang-dashcam-sejak-kes-kemalangan-penipuan-tular/>
2. <https://www.thesundaily.my/home/rtd-commended-over-app-to-report-traffic-violations-GA9121109>
3. <https://www.mylawquestions.com/how-does-a-lack-of-evidence-affect-a-case.htm>
4. \*Adamová, V. (2020). "Dashcam as a Device to Increase the Road Safety Level." Proceedings of CBU in Natural Sciences and ICT 1: 1-5.
5. <https://www.thedashcamstore.com/how-to-retrieve-videos-from-your-dashcam/>
6. <https://www.70mai.com/support/>
7. <https://www.gov.uk/government/publications/recovery-and-acquisition-of-video-evidence/recovery-and-aquisition-of-video-evidence-v30>

# Towards Better Cybersecurity With Key Performance Indicators (KPI)

By | Ernieza Binti Ismail

## Introduction

Key performance indicators (KPIs) are measurable values demonstrating how effectively an organization achieves its key business objectives. The choice of KPIs will depend on the industry and which element of business performance an organization is looking to track.

Nowadays, virtually every organization has to establish a set of KPIs in order to have a tangible perception of their progress towards reaching their desired targets. KPI is therefore a measurable expression for the achievement of a desired level of results in an area relevant to the evaluated entity's activity (*KPI Institute*).

In cybersecurity, KPIs are effective in measuring the success of a security management program and also aid in decision making. KPIs ultimately help demonstrate the value of cyber security to key stakeholders in an organization.

## SMART Objectives

One of the most widely used business terms in this modern, technology-driven world is "SMART". SMART is an acronym that stands for **Specific, Measurable, Achievable, Relevant** and **Time-based**. Each of these criteria can help an organization set strategic objectives and improve its business performance. Objectives based on SMART are always used to develop KPIs.

**Specific:** Refine your KPI to give the most specific information about your progress. The more specific the KPI, the easier it is to track. By being specific, expectations are clearly defined and there is lower risk of misinterpretation.

**Measurable:** KPIs should be measured frequently enough to help you stay on track, usually on a daily or weekly basis. Define what is being measured. Use a numerical value or percentage to define an expected increase or reduction in a particular activity.

**Achievable:** The goal owner is also responsible

for the KPI and that is what makes it a key performance indicator. A SMART KPI should motivate your employee to work hard to attain it, but also needs to be achievable.

**Relevant:** KPI should be directly connected to a goal. Every KPI needs to align with your business goals, both short and long term. As a key performance indicator, it is crucial to achieving your goal.

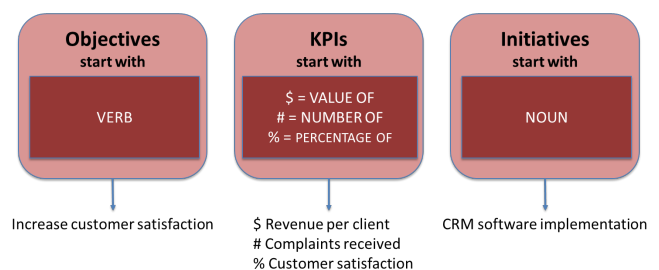
**Time-based:** In addition to your deadline, build key milestones into your KPI so you can stay on track. Setting a time frame for KPIs to be completed helps employees focus on completing the goal. It also makes it easier to track progress and outcomes of the set goals.

Below is an example for SMART Objectives:

Increase market share to 28% by the end of the financial year under the coordination of Marketing Director.

<b>Objective</b>	: Increase market share
<b>KPI</b>	: % Market share
<b>Target</b>	: 28%
<b>Time</b>	: By financial year end
<b>Owner</b>	: Marketing Director

As a standard terminology, KPI must have objectives and initiatives.

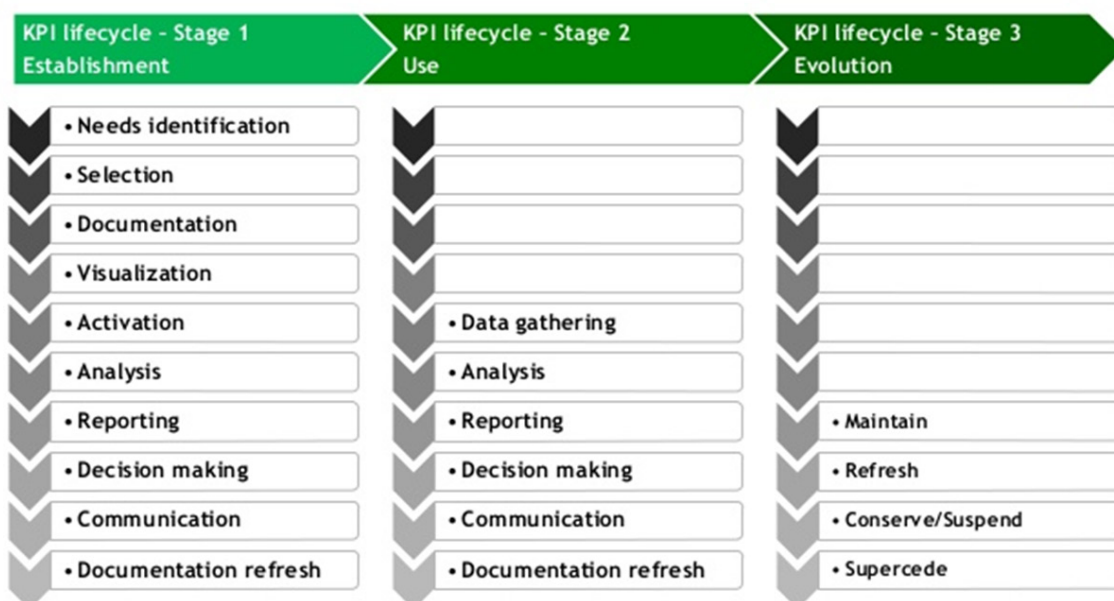


Picture 1: Terminology Standards

## KPI Lifecycle

KPIs can be divided into various lifecycle stages because they are continuously defined, redefined, and at times, superseded. Based on KPI Institute, there are 3 stages of a KPI lifecycle.

# KPI LIFECYCLE



Picture 2: KPI Lifecycle

## KPI Documentation Form

KPI documentation form is a template that structures the most relevant information on a given indicator. Important fields of the form include KPI definition, Calculation formula and Target. In addition, other relevant fields can be used, such as Subordinate measures, Limitations and Notes. Organizations can customize the template that fulfills all the information required. KPI documentation form serves the following functions:

- Ensure understanding of KPI measurement
- Facilitates communication through standardization
- Activation prerequisite
- Automation enabler
- Knowledge management
- Educates stakeholders
- Contributes to buy-in by involving the stakeholders

Based on KPI Institute, organizations use on average twelve different fields to document a KPI. The most popular fields are Name, Definition, Calculation formula, Target, Data source, Purpose, Threshold example, KPI record, Related objective, Unit type, Overall notes and others. The processes for organizations to develop KPI documentation form are:

1. Review internal literature
2. Review external resources
3. Consult with staff collecting or using the data

4. Present to KPI owner for approval
5. Review and approval by KPI architect / Subject Matter Expert / Strategy Manager
6. Add to organizational KPI library

Once the organization decides on the structure and key fields of the KPI documentation form, all the KPIs employed in the organization should be documented using the same format.

## Cybersecurity KPIs

Cybersecurity is not a one-time investment. Cyber threats are constantly evolving and the processes and technologies needed to prevent them are always changing. Organizations need to have measures in place to frequently assess the effectiveness of the safeguards that have been put in place.

There is no authoritative list of cybersecurity KPIs that all businesses or organizations should track. However, with the right KPI selection, an organization's cyber security will be optimised and will help reduce the risk of cyber-attacks and data leakage on the organization's systems. In addition, through KPI, reporting to stakeholders will also be easier and more accurate.

The following are the top Cyber Security KPIs that organizations can consider:

### 1. Level of preparedness

Organizations need to see how well prepared they are for any potential cybersecurity threat

or attack. This means they should review the number of devices on an organization's network and whether or not they are fully patched up and up-to-date. Should they find devices which are outdated or not fully-patched, they need to ensure it is done to rectify the vulnerabilities.

Vulnerability scans and vulnerability management tools are among the best ways to reduce vulnerability risk.

## **2. Unidentified devices on the internal network**

Unfortunately, employees could unintentionally introduce malware and other cybersecurity risks when they bring devices from home such as a laptop or even a tablet. Having a network intrusion detection system can be helpful in this regard.

## **3. Intrusion attempts**

Organizations need to keep an eye on any intrusion attempts to their organization's network and regularly review their firewall logs to check if there are any unauthorized access to the network.

## **4. Mean Time**

### **a) Mean Time to Detect (MTTD)**

MTTD measures how long it takes for your team to become aware of a potential security incident.

### **b) Mean Time to Resolve (MTTR)**

Once your team has become aware of the security threat, they'll need to resolve it. The time period taken to respond to a cyberthreat is known as the Mean Time to Resolve (MTTR).

### **c) Mean Time to Contain (MTTC)**

The Mean Time to Contain (MTTC) measures the time taken to close an identified attack vector across all organization's endpoints. It's the final stage after uncovering and identifying a cyber threat.

### **d) Mean Time Between Failures (MTBF)**

Mean Time Between Failures tracks the amount of time between a system or product failure.

### **e) Mean Time to Acknowledge (MTTA)**

The MTTA is the time taken by your organization to acknowledge an incident or data breach and begin working on resolving it.

## **f) Mean Time to Recovery (MTTR)**

Last but certainly not least is yet another MTTR which measures the amount of time an organization takes to recover after a product or system failure.

## **5. Security Incidents**

The number of times a hacker has attempted to gain access or breached your networks.

## **6. Security Ratings**

One of the best and easiest ways of communicating cybersecurity metrics to non-technical employees and colleagues is to use security ratings. Use a letter-based grading system to review your organization's cybersecurity position. Next, communicate it to non-technical employees so they can understand the severity of different threats. Easy to understand, security ratings support your cybersecurity risk assessment and indicate which information security metrics require your attention.

## **7. Cybersecurity Awareness Training**

Cybersecurity awareness training should involve all employee levels and grades. Make sure this type of training are conducted regularly and its documentation constantly updated.

## **8. Access Management**

How many users have administrative access? Access management refers to the processes and technologies used to control and monitor network access.

## **9. Virus monitoring**

To ensure better security for your organization, you'll need to monitor any potential viruses that are infiltrating your system. Do this by having your antivirus software scan various applications including web browsers, email clients, and instant messaging software for malware.

## **10. Cost per incident**

The cost per incident is a metric that measures the cost of responding to and resolving a cyberattack. The cost per incident should cover employee overtime, reduction of employee productivity, suspension of certain activities, potential loss of communication with customers, system downtime, as well as the cost of investigating the attack.



## Conclusion

---

There is no definitive list of the cybersecurity KPIs that all businesses should be tracking. The KPIs you choose will depend, in large part, on your organization's needs and appetite for risk. Be that as it may, choose KPIs that are clear and easily understood by anyone who looks at your report, including non-technical stakeholders.

Industry benchmarks and comparisons are effective ways to make complex KPIs even more comprehensible. However, the most important element is cost. When presenting KPI proposal to the top management and board, make sure your report can convey how cybersecurity KPIs can help save the organization money or generate revenue.

## Reference

---

1. The KPI Institute: KPI Documentation Form (2014–2019) <http://kpiinstitute.org/wp-content/uploads/Documentation-KPI-1836.pdf>
2. How To Use Smart Goals To Build Your KPIs. (2019, January 17) <https://www.grow.com/blog/how-to-use-smart-goals-to-build-your-kpis>
3. Practical Tips to Help You Develop Effective KPIs. (2022, January) <https://elmosoftware.com.au/resources/blog/how-to-develop-effective-kpis/>
4. Cybersecurity KPIs to Track + Examples (2021, April 14) <https://reciprocity.com/cybersecurity-kpis-to-track-examples/#:~:text=KPI%20in%20cybersecurity,achieves%20its%20key%20business%20objectives.>
5. 14 Cybersecurity Metrics + KPIs You Must Track in 2022 (2022, August 07) <https://www.upguard.com/blog/cybersecurity-metrics>
6. 20 Cybersecurity Metrics & KPIs to Track in 2022 (2019, July 08) <https://securityscorecard.com/blog/9-cybersecurity-metrics-kpis-to-track>

# Tip Untuk Elak Macau Scam (Penipuan Panggilan)

By | Nur Arafah Binti Atan

## Pendahuluan

Sejak kebelakangan ini, semakin kerap kita mendengar laporan media mengenai penipuan yang dibuat melalui panggilan telefon palsu atau nama lainnya Macau Scam. Walaupun Macau Scam bukan sesuatu perkara baharu, namun masih ramai lagi dalam kalangan pengguna internet di Malaysia yang menjadi mangsa penipuan ini. Pelbagai teknik dan modus operandi telah dilakukan oleh penjenayah untuk menipu mangsa dan ia berubah dari semasa ke semasa seiring dengan perkembangan teknologi. Taktik terkini adalah melalui penyamaran sebagai pihak bank, polis, pegawai Lembaga Hasil Dalam Negeri (LHDN) dan sebagainya.

## Latar Belakang

Jenayah yang dikategorikan sebagai *'telecommunication fraud'* (Macau Scam) ini biasanya dilaksanakan melalui empat jenis modus operandi iaitu penyamaran sebagai pihak berkuasa (polis atau pegawai agensi kerajaan); penyamaran sebagai pegawai dari institusi kewangan (Bank Negara Malaysia atau lain-lain bank); penyamaran sebagai pegawai syarikat perkhidmatan (agensi pekerjaan, syarikat penghantaran, kad kredit dan sebagainya) serta tipu culik dan meminta wang tebusan.

Kebanyakan panggilan dibuat menggunakan kaedah *Spoofing* yang merupakan teknik untuk pemanggil (penjenayah) berkomunikasi menggunakan platform *"Voice Over Internet Protocol"* (VoIP) semasa membuat panggilan bagi membolehkan pemanggil meletakkan sebarang nombor telefon untuk mengelirukan penerima panggilan (mangsa). Apabila panggilan dibuat, mangsa akan terpedaya dan menyangka panggilan tersebut daripada nombor yang tertera di skrin telefon walhal ia adalah tidak benar.

Dikatakan masih ramai yang terpedaya kerana mangsa khuatir dan keliru sama ada mereka benar-benar terlibat dengan jenayah seperti yang didakwa oleh penjenayah yang membuat penyamaran selain mangsa turut diugut untuk ditangkap disebabkan kesalahan yang dilakukan, malah mangsa juga dihalang daripada memberitahu sesiapa kerana kononnya ia akan melibatkan Akta Rahsia Rasmi.

## Modus Operandi Penipuan Panggilan (Macau Scam)

Modus operasi yang biasa digunakan bagi penipuan panggilan Macau Scam adalah seperti berikut:

1. Mangsa akan dihubungi daripada nombor yang tidak dikenali kononnya dari pihak berkuasa seperti polis, pegawai Lembaga Hasil Dalam Negeri (LHDN), pegawai bank, mahkamah sivil dan sebagainya.
2. Pemanggil mengatakan bahawa mangsa mempunyai pelbagai kesalahan antaranya saman, langgar lari, tunggakan bayaran hutang, bil, pinjaman dan sebagainya. Mangsa diminta untuk bekerjasama bagi melunaskan bayaran yang telah ditetapkan.
3. Sekiranya mangsa menafikan kesalahan tersebut, pemanggil akan meminta mangsa untuk membuat satu laporan polis secara dalam talian dan panggilan tersebut akan disambungkan kepada pegawai polis yang dikatakan menyelia kes mangsa. Penyamar polis tersebut akan memaklumkan bahawa mangsa telah terlibat dengan kes dan mengugut akan ditangkap.
4. Mangsa diminta untuk memberi kerjasama dengan menyerahkan butiran perbankan atau memindahkan wang ke akaun yang tidak dikenali bagi tujuan siasatan lanjut dan menyelesaikan kes.

## Tip Untuk Elak Menjadi Mangsa Macau Scam (Penipuan Panggilan)

Berikut adalah antara tip yang boleh dilakukan bagi mengelakkan daripada menjadi mangsa Macau Scam.

1. **Abaikan panggilan yang mencurigakan** - Jangan layan panggilan daripada nombor yang tidak dikenali atau putuskan panggilan jika berasa sangsi.
2. **Tenang dan jangan panik** - Jangan sesekali panik dan mengikut arahan yang diberikan oleh pemanggil tanpa terlebih dahulu menghubungi pihak polis atau institusi kewangan yang terbabit untuk pengesahan. Apabila mendapat panggilan daripada bank atau pihak berkuasa tentang isu undang-undang, minta dan catat maklumat yang diberikan oleh pemanggil dan katakan padanya bahawa anda sibuk untuk meneruskan panggilan. **Bertenang dan jangan panik!** Hubungi pihak bank atau pihak berkuasa untuk mengesahkan maklumat yang diperolehi tadi dengan mendapatkan butiran kontak daripada laman sesawang rasmi organisasi berkaitan. Lebih elok sekiranya hadir sendiri ke pejabat mereka untuk mengesahkannya.
3. **Jangan kongsi maklumat perbankan** - Jangan berikan maklumat perbankan peribadi seperti nombor akaun bank, kata laluan perbankan dalam talian, nombor kad kredit atau nombor *Transaction Authorisation Code* (TAC) kepada orang yang tidak dikenali. Sekiranya pemanggil bertanyakan maklumat kad debit atau kad kredit dan perbankan dalam talian, segera tamatkan perbualan.
4. **Jangan muat turun aplikasi yang mencurigakan** - Jangan muat turun sebarang aplikasi atau tekan apa-apa pautan yang diberikan pemanggil kerana dikhuatiri ia mengandungi perisian hasad atau perisian intip yang mampu mencuri data peribadi anda tanpa disedari.
5. **Muat turun aplikasi Truecaller** - Pengguna boleh memuat turun dan menggunakan aplikasi *Truecaller* untuk mengenal pasti nombor yang mencurigakan atau menyekat nombor tersebut dari terus menghubungi pengguna.

## Rujukan

1. Infografik CyberCrimeAlertRMP (instagram) – Jabatan Siasatan Jenayah Komersil, Polis Diraja Malaysia.
2. Macau Scam : Baca Ini Jika Tidak Mahu Ditipu. <https://www.astroawani.com/berita-malaysia/macau-scam-baca-ini-kalau-tak-nak-ditipu-159882>
3. Macau scam masih berleluasa! 6 tips elak penipuan menerusi panggilan telefon. <https://m.sinarharian.com.my/mobile-article?articleid=243673>
4. Macau Scam Tidak Pilih Mangsa. <https://www.bernama.com/bm/news.php?id=1655639>

# Promoting Data Sovereignty In The Age Of Cloud Computing

By | Naqliyah Zainuddin, Nurfaezah Hanis Halim, Ida Rajemee Ramlee & Syafiq Anneisa Leng Abdullah

## Overview

The rapid growth and widespread adoption of cloud computing services have eliminated the traditional geopolitical barriers and created multiple issues on data sovereignty. This has also been exacerbated by the development, implementation and adjustment of new data-driven technologies and related infrastructures. Data sovereignty refers to authority over data that an organization collects, stores, and processes, which are subject to a nation's laws and general best practices where the organisation is physically located. From another perspective, data sovereignty provides governments with the means to prevent unvetted access by foreign contractors, support staff and entities to their sensitive data.

In response to the trend in cloud computing across jurisdictions, many countries have imposed new compliance requirements by amending their current laws or enacting new legislation that requires customer data to be kept within a country where the customer resides. A breach of data sovereignty can happen on-premises, for example on a server, a personal device owned or used by a customer in the cloud. It can also happen in-cloud on a server owned by the cloud service provider (CSP) during data transmission between servers or between a cloud server and customers' devices.

The main concern surrounding data sovereignty relates to the enforcement of privacy regulations and how to prevent data stored in a foreign country from being retrieved by the host country. Data sovereignty laws of some nations impose significant limitations on data transmission where companies doing business in such countries may be prohibited from transferring data to a third-party cloud provider for processing or storage. Data sovereignty can be identified with the control of data flows across national jurisdictions.

## Data Sovereignty Fundamentals

Data sovereignty means any data is subject to the laws and governance structure within a nation where it is processed and physically stored. Different nations will have different laws concerning the use and storage of data including what type of data flows are allowed within its border. This regulation ensures that the user's information does not cross national boundaries without permission and which could potentially violate laws in other countries. Therefore, it is essential to take a closer look at the elements of data sovereignty and their related characteristics to ensure it is upheld.

### Data Sovereignty Elements

A person's data sovereignty is violated when a third party who is using the said data compromises another person's contractual, intellectual property or any other rights or in a way that causes the other person to be in breach of their own legal or regulatory duties. More specifically a breach of data sovereignty is likely to happen in a situation where:

- i. a third party (typically but not always a government agency) has the power to access data belonging to another person (for example, a corporate or individual cloud customer); and
- ii. data falls into the possession of the customer or someone else on the customer's behalf (the cloud service provider) with or without the consent or knowledge of the customer and/or the cloud service provider.

In addition, data sovereignty protocols should also take into account where proof of the physical location of the server on the network is within some acceptable margin of error and that customer data is indeed stored in this location.

### Data Sovereignty Characteristics

Despite numerous regulation, contract, and governance-related issues, the following characteristics need to be emphasized when:

- i. the rights of citizens to privacy and



protection of their personal data are abused;

- ii. the state obtains, collects and uses electronic communications information generated by its citizens without their agreement or knowledge;
- iii. the appropriate balance between the citizens' rights and the state's powers; and
- iv. in the international context, how these rights and powers play out if one state collects or obtains data not about its own, but of another state or citizens

Therefore, it is important that they are empowered to ensure the way their data is regulated.

## Data Sovereignty And Cloud Computing Issues

While consumers are often the ones who benefit from data sovereignty requirements, businesses must find ways to comply with the relevant privacy and data security laws of each country. It is therefore important that in order to be aware of local, regional, and international data privacy laws, organizations need to develop new infrastructure or use existing infrastructure for data collection, processing and storage that is consistent with all relevant data sovereignty requirements.

The distinction is less relevant between processing and storage on-premises and in the cloud outside the arena of investigative powers. When the processing or use of organizational data (wherever) violates contracts, third-party intellectual property or other rights, the same rule would apply at any processing and storage location. Other potentially malicious or criminal activities such as hacking, denial of service, malware or screen scraping may pose a risk to the security of an organization's data, whether that data is stored on-premises or in the cloud. Cloud data sovereignty risks, both in relation to investigative powers and rights violations and more broadly on breach of obligations, should therefore be viewed on a continuum that includes on-premise and cloud data storage and processing.

For this, they need a cloud provider that not only could offer transparency about the location of their data but also provide various in-country offerings combined with robust data security protocols, standards and take into account that data stored in cloud computing services may

be subject to the jurisdiction of more than one national law.

## Legal Concern

The migration of computing to the cloud raises novel legal issues on data whether as processed and stored in-cloud data or data transited between user and cloud service provider. These evolving legal issues concern principally the following:

- i. data rights: the intellectual property and other proprietary rights that arise in relation to data;
- ii. data protection: the legal rights and duties that arise specifically in relation to personally identifiable information;
- iii. data security: the mix of management, legal, technical, operational and governance controls that an organisation puts in place to ensure desired information security outcomes; and
- iv. data sovereignty: a person's right to control the disclosure of and access to his own data (whether or not the data is personally identifiable information) to a third party (typically, although not exclusively, a state agency). Data sovereignty involves, or can be identified with, the control of data flows across national jurisdiction.

## Cloud Specific Issue

- i. A service level agreement (SLA) contract is used by CSP to preserve and make data available for retrieval under several levels of durability. In addition to availability, SLAs also guarantee that data will be stored only at data centres within a specific geographical region (e.g., within a state, time zone or political boundary) for performance, regulatory and continuity reasons. Verifying if CSPs could meet their defined SLA in their contractual geographic obligation is a big challenge and one that would be a critical issue.
- ii. Many organisations do not have an adequate policy in this area. Their existing document management policy may not cover jurisdiction or location, nor recognise challenges thrown up by a somewhat chaotic, hybridising cloud services environment.
- iii. Data privacy and sovereignty regulations vary from one jurisdiction to another, imposing different legal obligations on companies to keep customer data secure and governing where a business should store its sensitive

data. Some require that certain data be kept in the customer's own country, which means that multinational corporations may be required to maintain data centres across multiple countries, possibly in each country which it has customers. Some countries' data sovereignty laws lack clarity, or clear guidance to businesses, and do not adequately spell out enforcement procedures. As a result, many companies are reluctant to utilize cloud technology because of fears of their inability to maintain sovereignty over the data for which they bear significant legal responsibility.

- iv. Information stored in a cloud environment can be subject to more than one nation's laws. The legal protection applicable to a single piece of data might change from one moment to the next, as data is transferred across national borders, or under the control of a different entity. Depending on where the data is being hosted or by whom it is controlled, different legal obligations regarding privacy, data security, and breach notification may apply.
- v. Enforcing privacy regulations and preventing data stored in a foreign country from being subpoenaed/accessed by the host country's government.

## Achieving Data Sovereignty

The complications of data sovereignty has posed challenges for organisations to stay compliant and vigilant. Here are four suggestions to uphold and achieve data sovereignty:

- i. Utilize Cloud Capability
  - The three main cloud computing services are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) can provide the necessary data protection for any organisation.
  - There are also three deployment models which are Public Cloud, Hybrid Cloud, and Private Cloud which can achieve and cater for each different nation's data sovereignty requirements.
- ii. Cloud Contract
 

Many cloud providers offer only standard form contracts containing boilerplate terms which are heavily biased against the customers. The detailed standard wording of a contract often fails to meet the cloud customer's particular business needs.

- A company should focus on contract language, which sets forth precisely the parties' obligations in a number of critical areas. Attention should be paid to empowering users to take responsibility and control where appropriate, not become passive participants. More companies are now insisting on negotiating the terms of the cloud contract in order to protect themselves from serious exposures.
- Sensitive data, breach: The contract should detail all matters related to the protection of sensitive data and equitably assign liability in case of inadvertent or negligent disclosures.

### iii. Data Governance

- Good data governance could help implement and update cloud data location and jurisdiction policies with strict regulations that help reduce risks surrounding data accessibility to various parties.
- A complete data governance process ensures adherence and continuous risk assessment and mitigation that is maintained regularly.
- Due to wide differences in data sovereignty laws, data governance ensures consistency on agreed definitions for a shared understanding of data. Accordingly, data governance enforces policies that help prevent data errors.
- Data Breach Management Policy addresses and outlines internal corporate prevention, detection, and incident response processes to a security breach. It could help defend any allegation that the company fail to take reasonable care in handling a data security breach.

### iv. Confidentiality, Integrity, and Availability (CIA) Triad

- Preservation of CIA must be maintained to ensure data protection.
- Confidentiality amounts to privacy. Integrity involves consistency, accuracy, and trustworthiness of data. Availability is all about where information should be consistently and readily accessible only to authorized parties.

## Conclusion

Although data sovereignty concerns have not been properly emphasized when firms plan their cloud strategy, they are now likely as the regulatory environment becomes more complex. Additionally, even if public clouds give businesses a variety of options on the geographic locations of their data, this may not be enough to stop them from utilising edge or hybrid architectures, which provide even more control.

In the present cybersecurity environment, there is an urgent need to foster closer working relationships between countries to deter future cyber threats and cyber-attacks. Every country must be prepared for the possibility of a cyber-attack. It is no longer a question of will a cyber-attack happen, but when it will occur. Furthermore, protecting information or data is crucial as improper use of data can lead to various negative impacts i.e., financial, brand/reputation, operational and regulation. A proactive and comprehensive measure is required to address evolving cyber threats especially involving cloud computing.

To cope with emerging new technologies, an intelligent and holistic strategy needs to be adopted by using new cyber tools. In a nutshell, the approach also needs to be adaptive, dynamic and innovative covering people, process and technology. Early preparation and constant preparedness are essential in fighting global cyber-criminal activities. Readiness and a rapid response could deter cyber-criminals from their nefarious activities. Moreover, cloud data could be subject to more than one nation's laws. Depending on where it is being hosted or by whom it is controlled, different legal obligations regarding privacy, data security and breach notification may be applicable. Despite the benefits of flexibility, scalability and cost savings offered by cloud infrastructure, companies adopting cloud need to consider potential security and data sovereignty issues.

Lastly, data sovereignty regulations should be made flexible enough to accommodate ICT developments and the government's interest in data security. Continuing diplomatic efforts and international cooperation in relation to data sovereignty in cyberspace is necessary to ensure that there is agreement between nation-states, as well as global private sectors, on how to manage cross-border data transfer in cyberspace.

## Reference

1. blueAPACHE. (3 September, 2014). blueAPACHE. Retrieved from Data Sovereignty and your Cloud: <https://www.blueapache.com/data-sovereignty-and-cloud/>
2. David Vaile, K. K. (2013). Data Sovereignty and the Cloud - A CIO's Guide. Technical, Legal and Risk Governance Issues Around Data Hosting and Jurisdiction, 1-91.
3. David Vaile, K. P. (2013). Data Sovereignty and the Cloud- A Board and Executive Officer's Guide . UNSW Law Research Paper No. 2013-84, 1-90.
4. E.Fine, J. (2022). Tech Transactions & Data Privacy 2022 Report: The Current Landscape of Data Sovereignty Laws and A Universal Compliance Strategy. Tech Transactions & Data Privacy 2022 Report, Volume XII, Number 255.
5. Kemp, R. (2015). Cloud Computing and Data Sovereignty. Kemp IT Law, 1-33.
6. Patrik Hummei, M. B. (2021). Data Sovereignty : A Review. Sage Journals -Big Data & Society, 1-17.
7. Tolson, B. (18 December, 2019). Archive360. Retrieved from What Is Data Sovereignty and its Role in the Age of the Cloud?: <https://www.archive360.com/blog/is-data-sovereignty-a-myth-in-the-age-of-the-cloud>
8. Tolson, B. (14 February , 2019). Archive360. Retrieved from What is Data Sovereignty and the GDPR: Do You Know Where Your Data is Located?: <https://www.archive360.com/blog/data-sovereignty-and-the-gdpr-do-you-know-where-your-data-is>
9. Vitaris, B. (11 August, 2020). What Is Data Sovereignty? Everything You Need to Know. Retrieved from Permission.io: <https://permission.io/blog/data-sovereignty/>
10. Yudhistira Nugraha, K. A. (2015). Towards Data Sovereignty in Cyberspace. International Conference on Information and Communication Technology (ICICT) (pp. 1-7). Nusa Dua, Bali, Indonesia: IEEE.

# Methods And Risk Of Bypassing Apple Device Security

By | Kamarul Baharin Bin Khalid, Muhammad Nasim Abdul Aziz, Ahmad Aizuddin Aizat Bin Tajul Arif & Muhammad Edwin Bin Ambo Rifai

## Introduction

Due to rapid development of digital technologies, mobile phones have evolved into smartphones with processing capabilities of a minicomputer. Apple mobile devices such as the iPhone and iPad are good examples. Nowadays mobile devices are packed with sophisticated features beyond just making phone calls and sending SMS. Mobile devices can now be used for creating documents, checking emails, playing games, performing online shopping, and much more at the fingertips of a user.

With advanced features, private data are stored inside their mobile devices. It is considered a data bank by itself and holds tremendous amount of private information of users, which is extremely valuable. Cybercriminals are constantly working to find ways to steal private data by installing malicious software into mobile devices. Scammers install malicious apps as beta apps through Apple's platform via TestFlight during the testing of the pre-release software phase. This proves that criminal activities are being created by organized crime to infiltrate Apple's mobile devices.

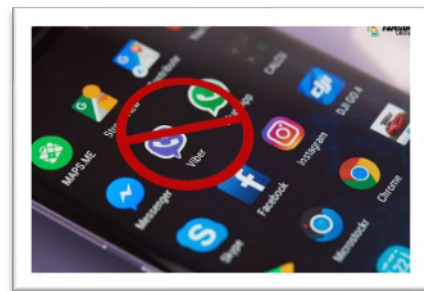


Apple disallows third-party application to be used on its mobile devices and regularly updates its Operating System (iOS) to prevent security vulnerability in its products. Apple has implemented a myriad of security features inside their mobile devices to protect users' personal data.

## Risk Of Installing Apps From Untrusted Sources

Installing unintended programs into a mobile device can lead to many harmful consequences for users. Utilizing a compromised mobile device creates security risks such as data being used elsewhere, passwords being stolen, or the device being used by cybercriminals. One of the reasons for the compromise is installation of certain apps from an untrusted source. Apple implements security features to prevent the installation of untrusted applications into its devices from untrusted sources known as sideloading.

Sideloading is downloading and utilizing of a mobile application not authorised by an official retailer such Apple store and installed through a third-party source. Sideloading an application not from Apple App Store creates a security risk as it bypasses all security checks by the Apple security team. This means that applications from untrusted sources may contain malicious code that will allow the exploitation of vulnerabilities in the mobile device.



To prevent and protect Apple users' mobile devices from sideloading any untrusted application, Apple only grants users to install applications from the App Store. Apple mobile devices strictly check the validity of the application certificates (Developer, Apple app store, and User) before installing or running any application. Should fraudulent or malicious apps make its way into the App Store, Apple would immediately remove and block future variants. If any of the certificates are revoked or expired, Apple mobile devices will block the application.



from being installed or executed. With this, only applications installed from the Apple App Store can be installed or executed on Apple mobile devices.

## Bypassing Apple Security

There are many ways that advanced users or malicious actors can bypass the Apple mobile platform. Three main methods to bypass apple security are jailbreak, self-signed, and beta testing. These three methods would enable mobile devices to have a compatible system like the normal Apple platform.

### 1. Jailbreak

Jailbreak is the use of an exploit to remove security restrictions posted by Apple through a series of kernel patches. It allows root access within the iOS which in turn permits the ability to install unsigned software which are not recognized by App Store. Jailbreak action is a violation of Apple's end user license agreement and allows Apple to discontinue access to device roots.



Jailbreaking bypasses Apple provision for the end user as it includes modifying the iOS, installing unsigned applications through sideloading, and allowing the user to have administration level privilege. Jailbreak enables expansion of Apple platform features in mobile devices, and permits unsigned programs not allowed by Apple to run. Users install unsigned programs to personalize and customize the mobile interface created by third-party developers.

Cyber perpetrators jailbreak the apple platform to install malware into their victims' devices. This would allow not only data to be stolen, but also to control the mobile devices and use it for criminal gain. Through jailbreaking, built-in security of devices is lost as kernel patches are removed, disabled, or modified. Mobile devices would be using the inferior iOS version that is no longer supported by Apple and potentially

experience security threats as older versions of iOS are known to have security vulnerabilities and exploits.

Apple protects its mobile devices through validation of the application certificates. Unsigned applications do not have any certificate attached. If the unsigned application is found to be rogue or malicious, Apple cannot revoke the application certificate and block the unsigned application from being installed and executed.

### 2. Self-signed (free)

A self-signed certificate is a digital signature verified on the user's behalf through a public key contained in a certificate within the mobile device. The risk of a self-signed certificate is that the apps are not properly encrypted allowing data to be easily acquired by cybercriminals. Self-signed certificates allow attackers to spoof the identity of the victim as security has been compromised. Self-signed certificates are free and allow for internal software testing on mobile devices and bypassing Apple device security. For security reasons, Apple allows self-signed applications to be installed and executed for 7 days only. After that period, the self-signed application needs to be re-signed and re-installed before it can be executed again.

### 3. Beta testing (Developer signed)



Beta testing is a phase where external users test newly developed apps or software that are still in the process of development and not officially launched to the market. It allows the discovery of errors and bugs and provides feedback to software developers of their apps.

TestFlight and installing developer certificates are types of beta testing allowed by Apple which are subscribed annually in Apple developer program. Even though Apple approved the developer certificate, Apple does not vet the development of the application which may lead to malicious activities.

### a) TestFlight

TestFlight is a tool that allows developers to test their app's development to the public before it is released to the market via App Store. It also collects valuable feedback from up to 10,000 testers using their e-mail address or a public link.

Scammers take advantage of TestFlight to distribute malware encoded into the newly developed apps without being vetted by Apple. Apple however advised testers not to download and install apps from unknown sources or developers as a precautionary measure to avoid scams.

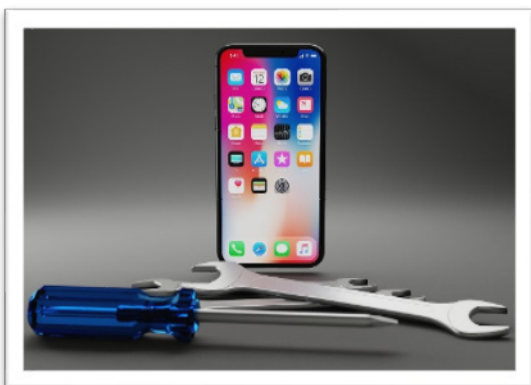
### b) Install developer profile certificate

Developer profile certificates allow developers to test their newly developed application within the developer organization without going through the security measures in apple mobile devices. This is to enable apps to be tested by the developers as well as to configure system behavior towards the apps. Even though this feature should be used only within the organization, developer or threat actors may ask users to install the developer's profile certificate on their device. This will minimize the security of their mobile devices as the applications are not vetted by Apple review procedures and pose as a security risk.

## Recommendation

Based on the above explanation: mobile users must avoid downloading and installing apps from an untrusted source. It is also advisable that users must always be aware of untrusted developers or untrusted sources when trying out apps during the Beta testing stage.

Do not click on suspicious URLs sent through SMS/messaging services/social media. These may lead to phishing activities and malicious programs could be attached to collect users' information.



Do not root or jailbreak your phone.

Avoid side loading (installing from non-official sources) where you can. If you need to install software from a source other than the trusted marketplace, be sure it is coming from a reputable source or developer.

If your smartphone is found to be infected with malware, you can simply uninstall the malware from your smartphone. However, if uninstalling does not remove the malware, then you need to reinstall the smartphone's Operating System (refer to phone manufacturer) to completely remove the malware.

## Conclusion

Even with tight security, malicious actors still find ways to bypass security features in Apple devices. Users should protect their devices by always updating their Apple iOS whenever a new software update is released. It is important that users avoid jailbreaking iPhone or iPad as it will diminish the security of iOS in the mobile device. Once a mobile device is compromised, it would be difficult to contain the data acquired by cyber criminals to be used indiscriminately without the users knowledge. As such, bypassing Apple security features should be discouraged.

## Reference

1. Scammers have been using Apple's TestFlight to distribute malicious iOS apps
2. A Risk-driven Model to Minimize the Effects of Human Factors on Smart Devices
3. Building a Trusted Ecosystem for Millions of Apps - The important role of App Store protections
4. Building a Trusted Ecosystem for Millions of Apps - A threat analysis of sideloading
5. How to sideload iOS apps and why it's dangerous
6. Sideloading iPhone apps creates a security risk says Apple's Tim Cook, so don't force us to support it
7. iPhone Pun Tak Selamat, 'Scammer' Jumpa Cara Pasang Aplikasi Hasad Pada Peranti iOS
8. <https://pixabay.com/>
9. Unc0ver 3.7.0 A12X Jailbreak For iPhone XS, XS Max, XR, 2018 iPad Pro Released, Download Now

# Cyber Incident Trend Analysis 2020 VS 2021

By | Sarah Rauf, Kilausuria Abdulah & Norlinda Jaafar

## Introduction

This 2020 and 2021 comparative trend analysis report provides an overview of incidents during the year under review. The report is based on data obtained from MyCERT's incident reports. Emerging trends identified are analysed against 2020. Some of the present key analysis findings include:

- Whether cyber incident is on the increase or otherwise
- Any new modes or techniques used in cyber-attack
- Whether mobile APK was widely used for phishing and malware

## Statistics

Below are statistics reported by MyCERT. Table 1 highlights the type of incidents for the two years (2020 and 2021). Figure 1 shows a chart on number of incidents in 2021 and 2020.

Type of Incident	2020	2021
Content Related	170	91
Cyber Harassment	596	417
Denial of Service	16	22
Fraud	7,593	7098
Intrusion	1,444	1410
Intrusion Attempt	116	159
Malicious Codes	593	648
Spam	145	102
Vulnerabilities Report	117	69
	10790	10016

Table 1: Number of incident for the year 2020 and 2021

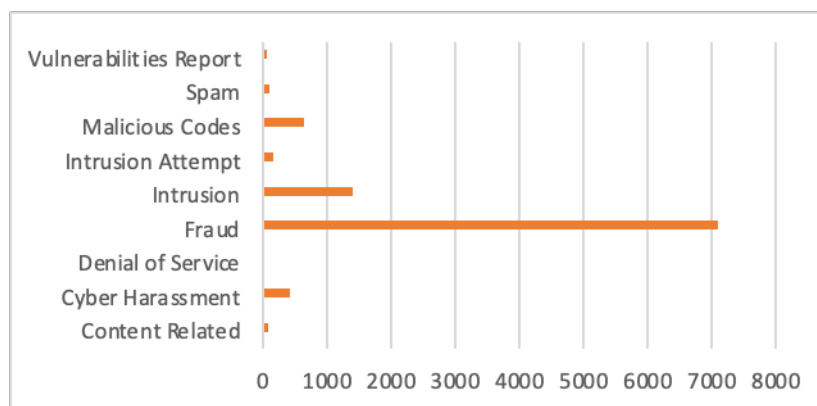


Figure 1: Number of incident for the year 2021

Type of Incident	2020	2021	Percentage
Content Related	170	91	-46.47%
Cyber Harassment	596	417	-30.03%
Denial of Service	16	22	37.50%
Fraud	7,593	7098	-6.52%
Intrusion	1,444	1410	-2.35%
Intrusion Attempt	116	159	37.07%
Malicious Codes	593	648	9.27%
Spam	145	102	-29.66%
Vulnerabilities Report	117	69	-41.03%

Table 2: Percentage increase or decrease of incident

Based on Table 2, 3 types of incidents increased in 2021, as compared to 2020. These are Distributed Denial of Service (DDoS), intrusion attempts, and malicious codes.

## 1. DDOS Incident

DDoS incidents were mainly on NTP amplification attacks which involved IPs in Malaysia targeting foreign organizations. NTP amplification attacks is a type of Distributed Denial of Service (DDoS) attack in which the attacker exploits publicly-accessible Network Time Protocol (NTP) servers to overwhelm them with User Datagram Protocol (UDP) traffic. NTP amplification is essentially a type of reflection attack involving eliciting a response from a server to a spoofed IP address. The attacker sends a packet with a forged IP address (the victim's) and cause the server to reply to that address.

## 2. Intrusion attempt

Intrusion attempt incidents detected were mainly SSH brute-force attempts, PHP injection attempts, as well as CVE exploitation. IPs in Malaysia were also involved in targeting foreign organizations. An intrusion attempt attack is one in which an attacker uses trial and error in guessing the credentials to access a particular server. Unlike a lot of other tactics used by cybercriminals, brute force attacks do not rely on existing vulnerabilities. Instead, cybercriminals rely on weak or guessable credentials. Brute Force attacks are simple and have a high success rate, as there are tools and programs available for attackers to use. Once an attacker correctly guesses valid credentials, they could view, copy, or delete important files or execute malicious code.

## 3. Malicious code

Malicious code incidents include ransomware, mobile APK, botnets, malware hosting, and much more. As new technologies continue to develop rapidly, especially in mobile communications, malicious codes have also evolved to compromise mobile platforms such as mobile banking. The purpose of malicious code is to steal credentials and personal information for monetary gain.

## In-depth Trend Analysis

### 1. COVID-19 Cyber Scam

As new way of working from home proliferated due to COVID-19 pandemic, perpetrators

quickly shifted to new methods of cyber scams targeting such groups who work from home. According to observations by MyCERT, there were multiple malicious campaigns leveraging such situation by spreading malware through emails with malicious attachments and links to phishing websites. Some of them used COVID-19 to lure the public into searching information about the virus. The severe impact of the pandemic has given threat actors more grounds for credential and information theft, as well as malware infection.

### 2. Malicious Android APK

Malicious Android APK was a new malware campaign targeting Malaysian Internet users who downloaded new patient tracking and COVID-19 latest information app. MyCERT discovered some malware which were loaded with complex and sophisticated functionalities such as information harvesting, automation, dropper and remote access capabilities. One of such APK was the #StayAtHome app.

Some of the features of #StayAtHome Android malware include:

- Extensive use of its services to exfiltrate information it requires,
- Extend capabilities by downloading and dynamically load additional binary during runtime,
- Compromise user privacy by collecting credential, personal information, and track user activities.

To effect information exchange and downloading of additional Android executables, this malware needs to communicate with its Command and Control (C2) Server. All data and communication are encoded and encrypted even though it is via HTTP. Based on these capabilities, this malware could be used as banking trojan for financial gain and spyware for corporate espionage. MyCERT have received incident reports from financial institutions that their customer have been affected by this malware, causing financial loss.

### 3. SMSSpy using Malaysian Law Enforcement

This malicious android application leverages on local Law Enforcement Agency's theme to manipulate users. The application disguises as a mobile antivirus and an application that tests mobile signal for Malaysian users purportedly created by Royal Malaysian Police (PDRM), a trusted organization.



#SMSSpy malware:

- appears to be a fake mobile application that intercepts received SMS messages and forward them to a remote site.
- could collect all contact information including contact name, phone number, email address, street address, and organization.
- capable of modifying any contact data.
- capture SMS inbox content possibly with an intention to retrieve any TAC numbers sent through SMS.

#### 4. Misuse of Personal Data

Jabatan Perlindungan Data Peribadi (JPDP) had received multiple reports on Unlicensed Online Loan Provider collecting and misusing personal data through mobile loan applications. Under the cooperation between JPDP, CyberSecurity Malaysia (CSM) and Suruhanjaya Komunikasi dan Multimedia (SKMM), an investigation paper was opened under Seksyen 5 Akta Perlindungan Data Peribadi (PDPA act) on several online mobile loan applications operated by Unlicensed Online Loan Provider. These unlicensed providers could access, copy, and illegally keep personal data through mobile loan applications from debtors without a debtor's consent. The data collected could be used for harassment and other fraudulent activities.

#### 5. Mass Web Defacement

Cyber999 had received several reports on mass web defacements of Malaysian websites, which has been on the rise since 29th December 2020. Most of the defaced websites were left with hate and disgruntled messages about Malaysia. System Administrators are advised to take necessary steps to secure their systems against unwanted incidents and other security threats.

##### Alert 2020

*MA-798.122020: MyCERT Alert - Mass Web Defacement*

*MA-797.122020: MyCERT Alert - MyCERT Alert – Misuse of Personal Data by Unlicensed Online Loan Provider*

*MA-790.072020: MyCERT Alert - SMSSpy using Malaysian Law Enforcement as theme*

*MA-789.062020: MyCERT Advisory - StayAtHome malicious APK campaign*

*MA-788.062020: MyCERT Alert - Malicious Android APK theme Covid-19 targeting Malaysia users*

*MA-779.032020: MyCERT Advisory - COVID-19 Cyber Scams and Campaigns*

In year 2021, MyCERT received 22 incidents of denial of service (DoS) which was reported through Cyber999. According to its record, the number increased compared to the previous year by a total of 16 incidents. The figure has increased due to proactive reporting from other national CERTs on NTP amplification attacks that involved IPs in Malaysia.

In the first quarter of 2021, during an ongoing COVID-19 pandemic in Malaysia, MyCERT noticed a spike in incidents of APK files downloads as well as SMS's diverted to fraudster's devices.

As shown in the statistics above, 2 categories of cyber incidents have increased, namely Intrusion and Malicious Code with 37.07% and 9.27%, respectively. Despite continuous educational awareness, malicious incidents including malware hosting continued to grow and remained the most reported technical incidents in our constituency.

Below is an example of a modus operandi observed. Most of them were fairly similar with some small variations.

1. Victims find an advertisement in social media such as Facebook or Instagram.
2. Advertisement depicts a promotion with attractive offers of various services.
3. The victim then clicks on the advertisement where they will chat with the scammer via WhatsApp.
4. Scammer will provide APK file, 3rd party application for victim to download.
5. Victim installs the Apps and APK file is subsequently downloaded to the victim's mobile device.
6. Upon launching, the malicious application will prompt to "grant" or "allow" access to their messaging apps.
7. Unaware of the consequences, the victim will grant permission to the application.
8. Victims will be made to make payments on a fake online payment system website and their banking credentials sent to the attacker.
9. Transaction is validated using PAC SMS(s) sent to victim's mobile number where the application got the access to those SMS(s).
10. Attackers then make an illegal transactions after receiving the victim's credentials.



MyCERT strongly advises Internet users to play their role in increasing security awareness (self-educating, educating employees) and to follow standard security measures (best practices). Victims are advised not to panic and never follow instructions from unknown sources without first contacting law enforcement agencies such as the police or a financial institution. If not secured properly, social media, mobile computing and interconnected devices can become the perfect avenue for attackers to mount cyber-attacks which are highly sophisticated and difficult to detect.

#### **Alert 2021**

*MA-799.012021: MyCERT Alert - Best Practices and Guidelines Addressing Potential Intrusion and DDoS Attack*

*MA-824.122021: MyCERT Alert - Tips on Protection and Business Continuity Against Ransomware*

*MA-803.042021: MyCERT Advisory - Potential Phishing Campaigns Arising from Facebook's Data Leak*

## **References**

---

1. <https://www.mycert.org.my/portal/advisories?id=431fab9c-d24c-4a27-ba93-e92edafdefa5>
2. <https://www.mycert.org.my/portal/publications?id=7f17bda3-7d91-42e2-93fd-39476d75d35f>
3. <https://www.mycert.org.my/portal/statistics-content?menu=b75e037d-6ee3-4d11-8169-66677d694932&id=77be547e-7a17-444b-9698-8c267427936c>
4. <https://www.mycert.org.my/portal/statistics-content?menu=b75e037d-6ee3-4d11-8169-66677d694932&id=2650ed29-88be-4cec-86cc-13f8e07ae228>

# Physical Access Control: Fail Safe VS Fail Secure

By | Mohd Syamsyul Shuib

## Introduction

In order to fulfil the requirements for safety and security in a physical access control system, two designations associated with electronic locks known as fail safe and fail secure are mandated. There are many factors to consider in determining the correct designation for the space which will be elaborated further below:

## Fail Safe VS Fail Secure



Fail safe or fail secure refers to scenarios when the door controller unit fails and/or there is no power to the unit. All electronic door locks are power activated. The terms “safe” and “secure” indicate the condition of the door from the outside, where you would insert a key or scan an access card to open it. Fail safe means when there is no power supply, the door will be unlocked; fail secure means when there is no power supply, the door will continue to be locked.

In other words;

**Fail Safe:** Unlocked when power is removed. Power is applied to lock the door. Commonly used for public access area such as general office space, lobbies and stairwells.

**Fail Secure:** Locked when power is removed. Power is applied to unlock the door. Commonly used for secured areas such as IT rooms, storage closets, and sensitive areas.

Fail-safe locks are intended to keep people safe.

In default state, it is unlocked. During normal business operations, power is applied to lock the door. Should power be interrupted or fail, the door automatically unlocks or releases to let people out of the space. That is why it is termed “safe” – it is safe for people - not the space! If there is an emergency and the power has gone out, entry points should be unlocked so fire and medical personnel can quickly enter the building.

Fail-secure locks are intended to keep things secure. For example, if a bad storm causes the power to go out, you still want to limit access to server rooms or storage area. So as previously mentioned, if the power is interrupted or fails, the door stays locked. That is why it is called “secure”: Its default state is locked or secured. In other words, fail secure lock keeps the door locked even when power is removed. However, since the doors are being locked in emergencies, most of them can be manually unlocked with a key as a back-up precaution. This mechanical override key is limited to only a few people with highly restriction of use that would otherwise be too complex for many to operate. Furthermore, this key override should also allow access by emergency personnel; otherwise, emergency personnel will need to use the necessary tools and force entry during emergencies.

## Misconception

The most common misconception is that people would think fail safe locks are there to allow fast exit in case of emergency. This is called “egress” which means the action of going out of or leaving a place. Remember, the terminology of fail-safe and fail-secure describes the status from outside of the door. It regulates ENTRY control into a space. This means you can always exit a space, regardless of the power situation. In the event of a fire or other emergency, when people need to exit the building, both locks still permit egress. If all doors would be inaccessible during a fire, fire fighters or medical staff could be hindered to provide help properly.

The second most common misconception is that typically when people want to prevent fail safe locks from unlocking during power outages,

they install back-up batteries. However, this actually defeats the purpose of fail-safe locks being installed in the first place. One big reason why many offices do this is because of the usage of glass doors which look a lot better and more popular. Since typically only magnetic locks (maglock) work on glass doors, the company wants to operate them like a fail secure magnetic lock instead which is ineffective in the first place.

## Conclusions

---

In considering safety and security aspects, our space will likely need a combination of fail-safe and fail-secure locks. During an emergency, people can move freely throughout a space, but there are certain areas of the building that may not need unlimited access every time there's a power outage.

Apart from that, power consumption is also something to be considered. In practice, fail-safe locks are more expensive since they constantly require power to operate. On the other hand, fail-secure locks use less power because they only require power to unlock.

## References

---

1. Bernhard Mehl (2018). Fail Safe vs Fail Secure- and what most people get wrong; <https://www.getkisi.com/blog/fail-safe-vs-fail-secure>
2. Lori Greene (2017). Decoded: Fail Safe vs. Fail Secure – When and Where? <https://www.allegion.ca/en/home/newsroom/2018/FailSafevsFailSecure.html>
3. Pritchard, Dakota Michael (2019). "Permanent Magnet Locking (PerMagLock) System: A Fail-Secure Alternative". Honors Capstone Projects and Theses. 535. <https://louis.uah.edu/honors-capstones/535>
4. Bob Mesnik 2021. Access Control Locks FAQ-Fail-Secure or Fail-Safe; <https://kintronics.com/access-control-locks-faq-fail-secure-or-fail-safe/>

# Telegram Account Compromise Incidents

By | Nur Qurratu 'Aini Binti Rohizan, Lukman Hakim Bin Abd Rahman, Imran Bin Hasnan & Nurshuhada Binti Mahfuz

## Introduction

The incidence of a compromised messaging account was previously more prevalent in WhatsApp application. The perpetrator would often impersonate as the account owner, asking for money from friends and contacts. However, we now see a rise of similar incidents targeting Telegram messaging app. Compared to WhatsApp accounts, which require verification code via SMS to ensure successful takeover of an account, it is much different for Telegram. This article attempts to explain the techniques and tactics employed by cybercriminals.

Users must be wary of the latest scam tactics and learn to strengthen their account's security as such attacks could happen to anyone. Examples of such attacks are screenshot below:



Figure 1: A perpetrator impersonating as UMNO president



Figure 2: Screenshots of the conversation, requesting money to be transferred



Figure 3: A tweet by the Prime Minister informing that his account has been hacked.

## Incident Statistics

Cyber incident reference center, Cyber999, one of the services offered by MyCERT, regularly receives reports from Internet users regarding on cyber incidents of Telegram accounts. In 2018, only 1 report was received. Over the years, the incidents have risen drastically up to August 2022. It is suspected that the number of unreported cases could be much higher. Figure 3 below illustrates the number of Telegram accounts compromised reported to Cyber999.

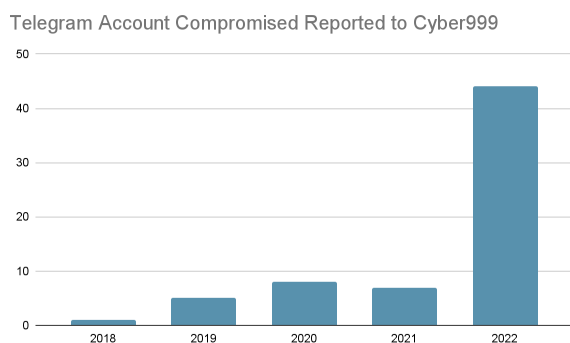


Figure 4: Telegram Account Compromised Reported to Cyber999

## Techniques and Tactics

There are many techniques and tactics used by hackers to hijack a victim's Telegram account, mostly with the objective of obtaining the 5-digit OTP code and gaining access to the Telegram account. One of the most popular and trending techniques based on current incidents reported via Cyber999 is hijacking using a screenshot of the Telegram main conversation list menu.

In Telegram, the OTP can be seen on the main conversation list menu, since Telegram supports multiple device logins, and will send the OTP internally within the Telegram app itself so that users are able to get the OTP on already logged in devices to register a new device.

For this technique, the victim will receive a message within the Telegram app containing a 5 digit login code which is an attempt by the perpetrator trying to register the user's phone number. At the same time, the perpetrator will impersonate as a friend by sending a message to the targeted user as follows:

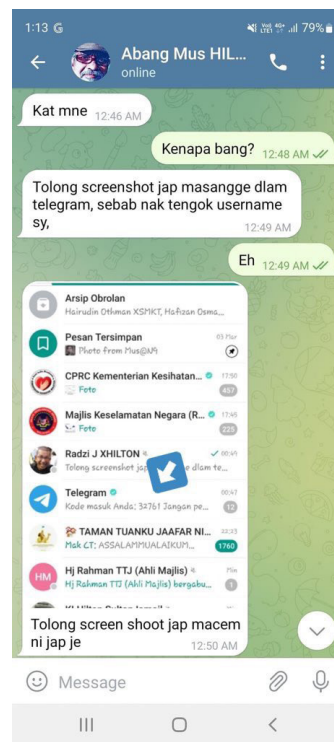


Figure 5 - Text message sent via Telegram from the perpetrator asking the victim to take a screenshot that will also show the 5 digit OTP code.

The hacker usually uses an already compromised account, to hijack other accounts, which are mutually connected with the previous victim, targeting users of community groups such as school parent-teacher groups, local community groups and work related group chats. The hacker will chat with the victim and mention as if they have been hacked and request that the victim share a screenshot from their device for verification.

Victims will usually respond without checking as the hacker could have imitated the language and chat style based on previous chat history of the stolen account.

Once the hacker obtains the screenshot from the victim, the hacker will then login the Telegram account and attempt to unlink all other devices, and enable two-factor authentication, locking out the victim and making it more difficult for the victim to recover the account.

The hacker, with the newly acquired stolen account, will then further impersonate the new victim to either target other mutual contacts within the users Telegram or chat with mutual friends and family to ask for money to be transferred into a mule bank account controlled by the hacker.



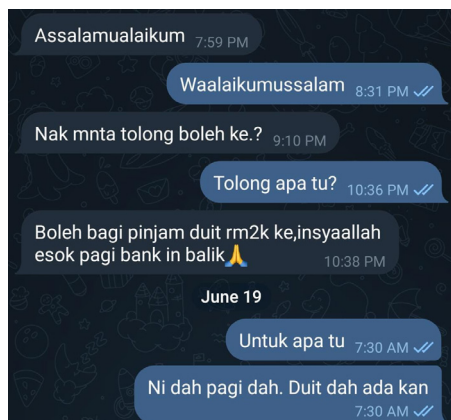


Figure 6 - Text message sent via Telegram from the perpetrator asking for money to be transferred into a mule account.

## Mitigation Steps

Telegram has created a set of self-help tools that affected individuals can use to report.

Report Abuse (This method also can be used to report Spam, Fake Accounts, Violence, Pornography, Child Abuse, Copyright & Other)

1. First run the Telegram app.
2. Now select the channel you want from the Telegram homepage chat list and tap on it.
3. Now we go to the channel. Tap on the three dots on the right. From the menu that opens select the report option and tap on it. You will see that a menu opens and includes the following options: Spam, Fake Accounts, Violence, Pornography, Child Abuse, Copyright & Other.
4. Select the option to report.
5. From the chat/message, tick/select the reported content/message and Report Message.

### Report Account compromised/hacked

1. Enable two-step verification:
  - Open the Telegram app and sign in
  - Tap the “menu” button on the top-right corner
  - Go to “Settings” and then to “Privacy and Security”
  - Tap “Two-Step Verification
  - Create a strong password and re-enter it for confirmation
  - Create a hint for the password

- Enter your email address and tap the “green check” icon
- Go to your inbox, open the email, and click the “confirmation link”

2. Terminate telegram active sessions  
This feature is located under Settings > Devices > Terminate other session
3. Set a Passcode Lock  
This feature is located under Settings > Privacy and Security > Passcode Lock

My phone was stolen, what do I do?

<https://telegram.org/faq#q-my-phone-was-stolen-what-do-i-do>

Delete Account or Manage Apps

<https://my.telegram.org/auth>

General advice to safeguard personal details and online accounts:

- Users must verify the authenticity and reliability of the contact that requests personal details. This can be done by calling the person directly.
- Users must not respond to messages they receive through mobile phones that request their personal details.
- Take precautions on websites that circulate through mobile phone messages that contain untrusted links that request users' personal details.
- Users must never share sensitive data and information with any known/unknown parties or websites.
- If users encounter any such websites or suspicious messages that request personal details, they must be reported to relevant Law Enforcement Agencies.
- If you suspect your personal details have been leaked or manipulated for malicious activities, you need to lodge a police report at a nearby police station with evidence.
- Avoid sharing personal details or private information on social networking sites, online instant messaging and SMS.
- Set a password for your smartphone. All the major smartphone operating systems allow you to set a password and automatically lock your phone after a period of inactivity.
- Enable two-factor authentication on every online accounts, including Telegram, WhatsApp, Email, online banking apps, etc.

- Verify application permission and the application author or publisher before installing it.
- Do not click on adware or suspicious URL sent through SMS/messaging services. Malicious program could be attached to collect the user's information.
- Always run a reputable anti-virus on your smartphone/mobile devices, and keep it up to date regularly.
- Don't use public Wi-Fi networks for bank transactions and turn off Bluetooth connection when not in use. These can be open windows for eavesdroppers intercepting a transaction or installing spyware and other malware on a user's smartphone/tablet.
- Update the operating system and applications on smartphone/tablet, including the browser, in order to avoid any malicious exploits of security holes in outdated versions.
- Do not root or otherwise 'jailbreak' your phone; avoid side loading (installing from non-official sources) as much as possible. If you do install Android software from a source other than the Play Store, be sure that it is coming from a reputable source.

## Conclusion

The techniques and tactics used by hackers to steal accounts are constantly evolving, as more tools become accessible in the Web. Internet users need to equip themselves with awareness to be extra careful and vigilant to protect and prevent any fraud incidents.

Guidelines and best practices to safeguard social media accounts and online fraud incidents have been published in our website:

<https://www.mycert.org.my/portal/details?menu=431fab9c-d24c-4a27-ba93-e92edafdefa5&id=d2ea8e03-0436-4a07-a20f-df98d00e35f1>

## References

1. <https://www.mycert.org.my/portal/details?menu=431fab9c-d24c-4a27-ba93-e92edafdefa5&id=6fdeca93-313f-48d7-9947-a27e4a11e169>
2. <https://www.mycert.org.my/portal/details?menu=431fab9c-d24c-4a27-ba93-e92edafdefa5&id=4d245fbd-df65-4e64-b1af-53e524a331f0>
3. <https://www.mycert.org.my/portal/details?menu=431fab9c-d24c-4a27-ba93-e92edafdefa5&id=ad40bf86-69c6-4a21-af96-1c980fe35d00>
4. <https://www.mycert.org.my/portal/details?menu=431fab9c-d24c-4a27-ba93-e92edafdefa5&id=e6b9dd94-3209-4a33-b600-8027d32b302a>
5. [https://faq.whatsapp.com/619670298808780/?cms\\_id=619670298808780&published\\_only=true](https://faq.whatsapp.com/619670298808780/?cms_id=619670298808780&published_only=true)
6. <https://www.mycert.org.my/portal/details?menu=431fab9c-d24c-4a27-ba93-e92edafdefa5&id=d2ea8e03-0436-4a07-a20f-df98d00e35f1>
7. <https://twitter.com/NewsBFM/status/1493955815245770752>
8. <https://twitter.com/IsmailSabri60/status/1556559359613669376?t=vjY1GKtXJI6MZ2tgRgqP7A&s=08>

# WhatsApp Account Compromise Incidents

By | Nur Qurratu 'Aini Binti Rohizan, Lukman Hakim Bin Abd Rahman & Kilausuria Binti Abdullah

## Introduction

There has been an upward trend of WhatsApp accounts—a popular instant messaging app, being compromised. In brief, the incident involved a perpetrator impersonating a friend, family members or WhatsApp Support Team, requesting a 6-digit verification code that was sent to the user's phone number. Once the user shares the verification code, the perpetrator will then take over the account.

Jumaat jam 15.11 saya telah menerima panggilan luar negara nombor +12677236558 ada tulis di hp saya suspected scammer dan saya tidak angkat panggilan tersebut walaupun dipanggil beberapa kali saya tetap tidak angkat.

Jam 19.00 saya membuka whatsapp mendapati ianya tidak dapat dibuka kerana telah dikunci degan nombor PIN yg kemungkinan nya telah diset oleh scammer. Slepas itu saya menerima banyak panggilan dari contact, yg saya telah remove mereka dari grup whatsapp, memadam grup dan telah menukar gambar profile saya kepada gambar yang amat mengerikan sedangkan saya tidak berbuat demikian.

Figure 1: A screenshot of a police report made by a victim whose WhatsApp account was hacked

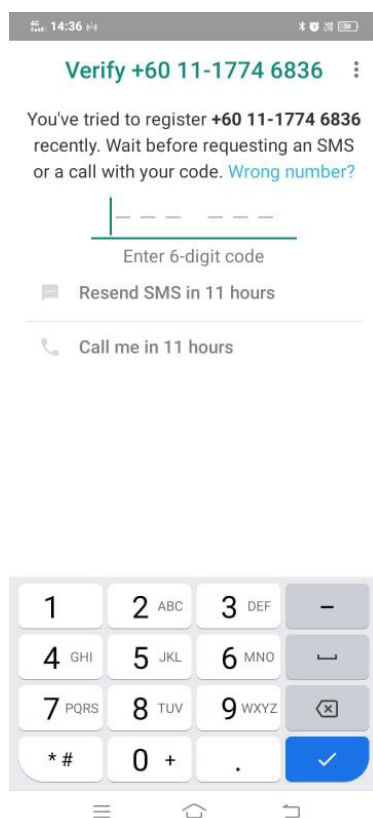


Figure 2: A screenshot of the victim's phone showing an attempt to regain access into hacked account.



Figure 3: A screenshot of a WhatsApp conversation whereby the perpetrator is requesting money from the victim

Did this incident happen due to security weakness of the app or the perpetrator's trick using social engineering? This article will delve into the techniques and tactics.

## Incident Statistics

Cyber incident reference center, Cyber999, one of the services offered by MyCERT, often receives reports from Internet users regarding on cyber incidents of WhatsApp account being compromised. In 2017, a total of 21 reports were received from affected users. The incident increased in 2018 with a total of 34 reports.

The figure rose again in 2019 with 40 reports from public users. In 2020, it increased to 62 reports and reached a total of 74 reports in 2021. Figure 1 below illustrates the number of WhatsApp accounts compromised within the past 5 years.

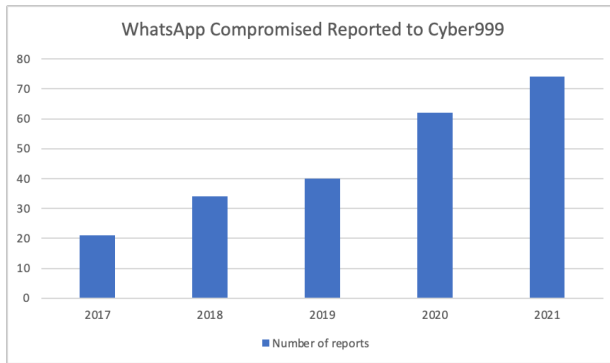


Figure 4: Number of WhatsApp Compromised Reports continues to rise

## Techniques and Tactics

There are several techniques and tactics used by hackers to compromise and gain access to WhatsApp accounts. The objective of the hackers is to obtain the 6-digit authentication code that is sent over by WhatsApp automatically to the account owner's phone via SMS or call. Below are some of the techniques used by hackers to trick victims into giving away the codes:

### 1) Phishing techniques

Hackers will attempt to login by entering the victim's phone number on their device and trigger a SMS to be sent by WhatsApp to the victim's phone. Once the SMS is sent over, the hacker will then contact the victim via call or text impersonating WhatsApp support team or staff and request for the code. If the victim gives over the 6-digit code to the hacker, the hacker will gain access to the account and can unlink all other devices, including the device that the victim is using.



Figure 5 - Text message sent from hacker to the victim to steal the 6-digit code

The hacker could proceed to enable two-factor authentication on the hacker's device with the hijacked WhatsApp account, making it harder for the victim to recover the account from the hackers.

### 2) Voicemail Hijacking

Another famous technique used by hackers

to obtain the 6-digit code is by hijacking the code using the voicemail feature of the victim's mobile number subscription. Most victims are not aware of the ability for their voicemails to be accessed from other phone lines, a feature primarily used by business travellers who travel abroad, leaving their country and phone line inactive, which requires a PIN code that can be set by the user.

Hackers will attempt to login using the victims phone number into WhatsApp and trigger the "Call Me" feature in WhatsApp, so that WhatsApp will trigger a call and read-out the 6-digit code to the victim's phone number.

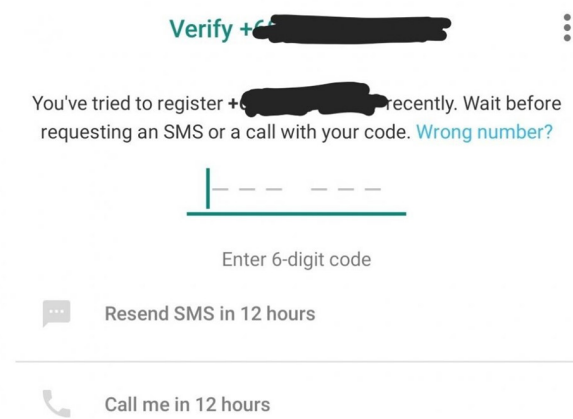


Figure 6 - "Call Me" feature used by hackers to hijack the account via voicemail

Once the hacker triggers the "Call Me" feature, the hacker will also call the victim directly, rendering the victim's phone line busy, thus forcing the call made by WhatsApp to read out the code via call to be redirected into the victim's voicemail inbox. To spoof the victim, the hacker may impersonate or act as if mistakenly called the victim.

The hacker then will dial the default number code (according to each telco provider) to access the voicemail inbox and attempt to use the default PIN code. It is unlikely most users would have changed the default PIN code as they rarely use this feature. The hacker will be able to play back to the 6-digit code readout and attempt to login using the code, and gain access to the WhatsApp account.

This method is more discrete as the victim can hardly notice the missed call and will only realize once the WhatsApp account has been successfully hijacked.

The hacker will then use the hijacked account to impersonate the victim and chat with mutual



52

friends and family to ask for money to be transferred into a mule bank account controlled by the hacker.

## Mitigation Steps

---

There are several mitigation steps that users could follow to secure their WhatsApp account. User can better secure WhatsApp account by following these tips:

### **Never share your registration code or two-step verification PIN with others.**

Registration code is to confirm that you own the phone number. The 6-digit registration code will be sent to you via SMS or phone call. Verifying your phone number with a registration code is the only way you can activate your account, and you must be able to receive the code on your phone.

### **Enable two-step verification and provide an email address in case you forget your PIN.**

The two-step verification has an option to enter your email address. This will allow WhatsApp to email you a reset link in case you forget your PIN, and also helps safeguard your account. The two-step verification PIN is different from the 6-digit registration code you receive via SMS or phone call. Even so, two-step verification is an optional feature that adds more security to your WhatsApp account.

### **Set a device code.**

To protect each device, users can use WhatsApp on up to four linked devices at once without the need to keep the phone connected

### **Be aware of who has physical access to mobile phones.**

If someone has physical access to a mobile phone, they can use the WhatsApp account without user permission.

### **Safety and security features**

WhatsApp comes built in with some basic controls that users can adjust to stay safe.

## Conclusion

---

The techniques and tactics used by hackers to steal accounts are constantly evolving over time, as more tools are developed and becoming accessible to anyone in the Web. Internet users need to equip themselves with knowledge on how to be more careful and vigilant to protect and prevent fraud incidents while online.

Guidelines and best practices to safeguard social media accounts and online fraud incidents have been published at in our website:

<https://www.mycert.org.my/portal/details?menu=431fab9c-d24c-4a27-ba93-e92edafdefa5&id=d2ea8e03-0436-4a07-a20f-df98d00e35f1>

## Reference

---

1. <https://www.mycert.org.my/portal/details?menu=431fab9c-d24c-4a27-ba93-e92edafdefa5&id=6fdeca93-313f-48d7-9947-a27e4a11e169>
2. <https://www.mycert.org.my/portal/details?menu=431fab9c-d24c-4a27-ba93-e92edafdefa5&id=4d245fbd-df65-4e64-b1af-53e524a331f0>
3. <https://www.mycert.org.my/portal/details?menu=431fab9c-d24c-4a27-ba93-e92edafdefa5&id=ad40bf86-69c6-4a21-af96-1c980fe35d00>
4. <https://www.mycert.org.my/portal/details?menu=431fab9c-d24c-4a27-ba93-e92edafdefa5&id=e6b9dd94-3209-4a33-b600-8027d32b302a>
5. [https://faq.whatsapp.com/619670298808780/?cms\\_id=619670298808780&published\\_only=true](https://faq.whatsapp.com/619670298808780/?cms_id=619670298808780&published_only=true)
6. <https://www.mycert.org.my/portal/details?menu=431fab9c-d24c-4a27-ba93-e92edafdefa5&id=d2ea8e03-0436-4a07-a20f-df98d00e35f1>
7. [https://faq.whatsapp.com/286438328952313/?locale=en\\_US](https://faq.whatsapp.com/286438328952313/?locale=en_US)
8. [https://faq.whatsapp.com/2976081889094372/?locale=en\\_US](https://faq.whatsapp.com/2976081889094372/?locale=en_US)
9. [https://faq.whatsapp.com/619670298808780/?cms\\_id=619670298808780&published\\_only=true](https://faq.whatsapp.com/619670298808780/?cms_id=619670298808780&published_only=true)



# Digital Signature Application in Malaysia

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

Since the imposition of Movement Control Order (“MCO”) by the Malaysian government to curb the spread of COVID-19 pandemic, businesses have been turning to digital technology to engage and serve their clients remotely. This situation had compelled businesses to resort to digital signature for execution of documents.

Digital signature is a signature generated using an asymmetric cryptosystem and verifiable to a public key listed in a valid certificate issued by a licensed certification authority. The certificate is used to verify the identity of the signer of a message and to ensure the correctness and validity of information in electronic transactions. In Malaysia, digital signatures are governed by the Digital Signature Act 1997 (the “DSA”). The Multimedia and Communication Commission Malaysia (the “MCMC”) is responsible to administer, enforce, and give effect to the provisions under DSA.

Section 2 of the DSA defines digital signature as:

*“transformation of a message using an asymmetric cryptosystem such that a person having the initial message and the signer’s public key can accurately determine -*

- a. whether the transformation was created using the private key that corresponds to the signer’s public key; and*
- b. whether the message had been altered since the transformation was made”*

Digital signatures generated by unlicensed software provider found online are not recognised in Malaysia. Only licensed certification authorities can issue legally binding digital certificates for digital signatures to be valid, enforceable and effective. The licensed certification authorities act as trusted third party in verifying the identity of both the signer and the recipient of digitally signed documents. They are licensed by virtue of Section 4 of the DSA. Currently, there are four licensed certified authorities as follows:

- i. Pos Digicert Sdn Bhd (licence valid until 25 December 2025);
- ii. MSC Trustgate Sdn Bhd (licence valid until 24 July 2025);
- iii. Telekom Applied Business Sdn Bhd (licence

valid until 31 July 2024 ); and

- iv. Rafcomm Technologies Sdn Bhd (licence valid until 30 April 2024).<sup>1</sup>

Section 62 (1) of the DSA provides that a digital signature shall be recognised by the DSA where:

- a. the digital signature is verified by reference to the public key listed in a valid certificate issued by a licensed certification authority;
- b. the digital signature was affixed by the signer with the intention of signing the message or document; and
- c. the recipient has no knowledge or notice that the signer—
  - i. has breached a duty as a subscriber; or
  - ii. does not rightfully hold the private key used to affix the digital signature.

As long as the digital signature created meets the requirements set in the DSA, then it is legally binding, valid, enforceable and effective and a document signed with the digital signature has the same legally binding effect as a document signed with a handwritten signature, an affixed thumbprint or any other mark, as stated under Section 62 (2) of the DSA.

A digital signature satisfies the requirements provided by DSA. Section 64 (1) of the DSA provides that a message shall be as valid, enforceable and effective as if it had been written on paper if -

- a. it bears a digital signature in its entirety; and
- b. that digital signature is verified by the public key listed in a certificate which -
  - i. was issued by a licensed certification authority; and
  - ii. was valid at the time the digital signature was created.

It is also considered as written document created under Sections 91 and 92 of Evidence Act 1950.

Section 65 of the DSA provides that a copy of a digitally signed message shall only be

<sup>1</sup> <https://www.mcmc.gov.my/en/sectors/digital-signature/list-of-licensees>

valid, enforceable and effective as the original message unless it is evident that the signer has designated a specific instance of the digitally signed message to be a unique original, in which case only that instance constitutes the valid, enforceable and effective message. This corresponds with Evidence Act 1950 with regards to Sections 61, 90A, 90B and 90C.

Section 66 of the DSA further provides that a certificate issued by a licensed certification authority shall amount to acknowledgement of a digital signature as verified by reference to the public key listed in the certificate, regardless of whether words of an express acknowledgment appear with the digital signature or whether the signer physically appear before the licensed certification authority when the digital signature was created, provided that the said digital signature is –

- a. verifiable by that certificate; and
- b. affixed when that certificate was valid.

However, despite digital signature being formally recognised and governed statutorily, there are risks and challenges concerning digital documents transmitted over any electronic networks such as interception, tampering, deception, non-repudiation and authenticity. To overcome this, the sender and receiver must be convinced that their electronic record can be authenticated and not forged while in transit unlike traditional signature where a person is required to witness the signature. Meanwhile the digital signature will be verified by a licensed certification authority through a trustworthy system. Furthermore, the type of digital signature under the DSA is restricted to asymmetric cryptography only and excludes other existing technologies such as Escrowed Encryption Standard (EES) and biometric method (fingerprint validation and retinal scans), secure socket layer (SSL) and secure electronic transaction (SET) or others that may be developed in the future. This has raised the concern on the security issue as the hardware and software used to create digital signature may be vulnerable to unauthorised access or unauthorised modification.<sup>2</sup>

It is also worth noting that the DSA only governs within Malaysia only, thus it is limited in its application and may not be effective in the borderless cyber world where digital documents could be transmitted across multiple

jurisdictions.<sup>3</sup> This also hampers cross-border transactions where parties domiciled outside Malaysian jurisdiction are restricted to execute documents digitally.<sup>4</sup> To date, there are no recognised foreign certification authorities in Malaysia. To qualify as a certification authority, certificate issued by foreign certification authority must exhibit equal or more stringent security level than the level of security of a certificate issued by a licensed certification authority in Malaysia.<sup>5</sup>

Unlike traditional or conventional signature which has no validity period, maximum validity of digital signature is three years from the date of issuance under Section 59 (2) of the DSA and no provision of renewal of digital certificates. Subscriber has to reapply and incur additional cost for new certificate using the same process. The DSA is not equipped to deal with criminal elements of hacking such as unauthorised access and unauthorised modification. However, it is presumed that these aspects are governed by the Computer Crimes Act 1997.<sup>6</sup>

There are also issues related to the licensed certificate authority and subscriber. The DSA did not set any qualification for a licensed certification authority, whereby there are no requirements for education or professional qualification nor specialised training to be a licensed certification authority. The only provisions available are those under Regulations 6(h) and 41 of the Digital Signature Regulations 1998. Regulation 6 (h) provides that the certification authority only employs operative personnel who have not been convicted of an offence involving fraud, false statement or deception within the past fifteen years and have demonstrated knowledge and proficiency in following the requirements of the DSA and the Regulations. Section 61 of the DSA also limits the liability of the licensed certification authority. They are not liable, among others, for any loss caused by reliance on a false or forged digital signature of a subscriber, and punitive or exemplary damages or damages for pain or suffering. The DSA also does not provide for certification authority to carry any liability

3 Ibid

4 Julian Hashim & Desmond Lim (2020). Digital and Electronic Signature: Application and Legal Position in Malaysia. <https://www.linkedin.com/pulse/digital-electronic-signature-application-legal-position-julian-hashim/>

5 <https://www.mcmc.gov.my/en/sectors/digital-signature/licensing-application>

6 Tay Eng Siang & Goh Choon Yih (2006). Legal Issues and Technical Aspects on Mechanism of Digital Signature in Malaysia. Proceedings of the International Conference on E-Commerce (ICoEC) 2006.

2 Tay Eng Siang & Goh Choon Yih (2006). Legal Issues and Technical Aspects on Mechanism of Digital Signature in Malaysia. Proceedings of the International Conference on E-Commerce (ICoEC) 2006.

insurance, nor any specific amount required as surety bond.<sup>7</sup>

While the risks in signing of an electronic document through the asymmetric cryptosystem is minimal, transfer risks to the private key could still be there. The problem with the algorithm sequence of a digital signature is that it is stored in computer device such as smart card, and thus the device must be kept in a secure location. The only presumption is that if a document is signed with someone's private key, the receiver may expect that this comes from that person. Section 43 of the DSA only imposes the duty on the subscriber to 'exercise reasonable care' in retaining control of his private key. This standard of care is not sufficient to curb forgery or fraud. Since the private key is the personal property of the subscriber under Section 44 of the DSA, absolute liability should be attached to private key holder to hold and control his own private key.<sup>8</sup>

In conclusion, the usage of digital signature is imminent due to evolving digital trends and more so, it provides convenience. However, the DSA may need to be further improved to cater to new technologies and stay relevant in current times.

---

7 Ibid

8 Ibid

# Endpoint Detection And Response Platform As A Mitigation Strategy For Advanced Security Operation Center In Managing Security Incidents

By | Muhammad Nasim Abdul Aziz, Wira Zanoramy Ansiry Bin Zakaria, Md Sahrom Bin Abu & Fathi Kamil Bin Mohad Zainuddin

## Introduction

Cybersecurity threats are IT-based attacks that can create harm to critical national infrastructures, businesses, and organizational entities. Cyber-attacks are malicious activities that target computer systems through different methods from distributed denial of service (DDOS), malware attacks, phishing, SQL injection to zero-day exploits. Cyber threats can cause disastrous impact on individuals' minds and mental health due to disturbances through online love scams, cyber harassment, online blackmail, and also cyber intimidation. All these cyber-threat activities result in not only monetary losses, insecurity, but also mental dysfunction to a person, and also disruption to organizational operations.

An Advanced Security Operation Center (ASOC) is an IT security entity initiated by professionals who want to protect their stakeholders by addressing compliance and threat management. A nation, business organizations, and the public as a whole can benefit from the creation of ASOC to protect their interests and important data from being stolen and exploited by cyber criminals. ASOC is typically an advanced level of Security Operation Center (SOC), managed by a team of IT security experts, to monitor, detect, analyze, and investigate cyber threats. Through ASOC, dedicated security teams monitor the cyber security environment and alert management of any potential external threats to the organization [1].

As ASOC needs to stop cyber threats before they happen, it needs to access advanced technological system platforms or security tools to deal with security incidents. Certain cyber incidents may not be considered critical or warrant investigation, even though they may cause significant damage if not resolved [2]. It is crucial to be able to monitor, anticipate, and take advanced steps to control potential cyber security threats. An advanced monitoring tool

that proactively detects and prevents endpoint cyber-attacks known as Endpoint Detection and Response (EDR) offers such facilities and thus, is an important tool for ASOC.

EDR combines different ways to protect endpoints by combining real-time continuous monitoring, endpoint data analytics, and automated response based on rules. The goal is to make it harder for people to take advantage of security holes and cause damage to computer systems.

## EDR Functions And Features

As cyber security landscape grows more sophisticated, a lot of features need to be added to make endpoints of IT systems safer and less vulnerable to attacks. EDR does not only focus on monitoring, but also has other features that have the capability to improve security for endpoint activities. Security teams identify cyber-attacks by looking at data from endpoints that EDR solutions send them [3]. EDR also helps review what happened when a cyber security incident happens so that it can be fixed to avoid any future breach.

Among the features and functions of EDR are as follows:

### 1. Threat intelligence

EDR issues warnings to users on any potential risks and threats from its threat intelligence features. EDR generates intelligence that facilitates the elimination of any insider threat by analyzing information on past activities rather than predicting existing risk [4]. It also provides information on threats, collected by EDR's server. This can help users focus on variables that are hard for attackers to change, such as tactics, techniques, and procedures (TTP). By doing this, users can make it more prohibitive for attackers to launch attacks and improve their ability to find and stop cyber threats.

## 2. Continuous monitoring

EDR monitors the endpoints on a regular basis to look for any irregular activities in the computer or network system. If an endpoint is infected, EDR will be notified and the infection isolated right away. Monitoring consistently prevents threats from penetrating an organization's IT system.

## 3. Remediation and cleanup

When a threat has been detected, EDR will perform deep cleaning of the system and continuously monitor the system from a follow-up attack. This results in a safer environment for the system as all threats will be fully removed and remediated.

## 4. Observe without interference

EDR runs in a network's kernel and can be operated by the system administrator. Because it runs in the kernel network, it protects the system entirely within the organization without interfering with the organization's system components or device processes.

## 5. Using machine learning to detect unknown threats

EDR uses artificial intelligence including machine learning to identify threats that are difficult to recognize and thus, helps in recognizing predictive cyber threats such as malware from unknown database. Machine learning also provides the ability to block unfamiliar threats by swiftly identifying threats that have never been encountered. This is one of the reasons cyber security organizations prefer EDR.

EDR is seen as a reliable solution for today's security systems due to its adaptation and improvisation to detect, monitor, and deter severe cyber-attacks from happening. By detecting suspicious events at the endpoint, EDR solutions have been in the spotlight as the market for 5G and the Internet of Things (IoT) matures. [5]. EDR does not wait for an attack to occur. Rather, its continuous monitoring prevents attacks from even surfacing in a system. This helps tremendously in managing risky security situations and eases ASOC in handling security incidents instead of relying a reactive system.

## Comparison Of EDR With Other Security Tools

EDR is just one of the many tools developed by cyber security experts to protect against cyber threats. Other security tools include antivirus

(AV), Extended Detection and Response (XDR), Network Detection and Response (NDR), and Managed Detection and Response (MDR) [6]. All of these security tools offer customised features that can be used across different situations and scenarios, though some of these features are available in EDR are more advanced. Below are some comparisons between main security tools mentioned.

Technology	2021
EDR	<ul style="list-style-type: none"> <li>• Data collection</li> <li>• Detection engine</li> <li>• Data analysis engine</li> <li>• Threat intelligence</li> <li>• Alerts and forensics</li> <li>• Trace back</li> <li>• Automated response</li> </ul>
AV	<ul style="list-style-type: none"> <li>• Security controls</li> <li>• Device controls</li> </ul>
XDR	<ul style="list-style-type: none"> <li>• Device controls</li> <li>• Disk encryption</li> <li>• Firewalls</li> <li>• Orchestration</li> <li>• Machine learning analysis of internal and external traffic</li> </ul>
NDR	<ul style="list-style-type: none"> <li>• Internal network D&amp;R</li> <li>• Behavioral analysis</li> <li>• Security controls</li> <li>• Insider threat detection</li> </ul>
MDR	<ul style="list-style-type: none"> <li>• Managed EDR</li> <li>• Perimeter telemetry</li> <li>• Incident management and response</li> <li>• Contracted service</li> </ul>

Table 1: Security solutions comparisons and features (source: eSecurity Planet)

Based on Table 1 above, it can be seen that EDR has adapted and improvised certain features across other security tools. While EDR focuses on protecting endpoints, other tools only provide security monitoring. Furthermore, EDR provides protection, detection, and response across data sources, while some tools only monitor security within themselves.

## EDR For Advanced Security Operation Center

Since ASOC is tasked to detect, monitor, and respond to cyber threats, it is critical that it maintains and upgrades its capability in combating cyber-attacks. Endpoint Detection and Response (EDR) helps ASOC deal with



cyber threats proactively by preventing attacks from getting into an organization's system and destroying important data.

EDR enables security experts to monitor all potential threats and equips security experts with the ability to effectively trace any source of attack, ensuring proof of criminal activity should a security incident go through legal process. EDR tools help check for vulnerabilities and prevent endpoint penetration, data loss, and system failure [7, 8]. ASOC will provide organizations with advanced security alerts to help secure their IT systems and reduce their vulnerability.

## Conclusion

Organizations that deal with security incidents often set up a security operation center as part of their division. As time goes on, a more advanced SOC (ASOC) is needed to handle the growing number of changes in security threats. Advanced technological tools, systems, and/or platforms need to be developed to counter and prevent future cyber incidents.

## References

1. Jacobs, P., Arnab, A. and Irwin, B. (2013) 'Classification of Security Operation Centers', in 2013 Information Security for South Africa. IEEE, pp. 1-7. doi: 10.1109/ISSA.2013.6641054.
2. Karantzas, G. and Patsakis, C. (2021) 'An Empirical Assessment of Endpoint Detection and Response Systems against Advanced Persistent Threats Attack Vectors', *Journal of Cybersecurity and Privacy*, 1(3), pp. 387-421. doi: 10.3390/jcp1030021.
3. Penziol, P. (2022) EDR vs. EPP: What is the Difference? exabeam.com. Available at: <https://www.exabeam.com/information-security/edr-vs-epp/>
4. Chandel, S. et al. (2019) 'Endpoint Protection: Measuring the Effectiveness of Remediation Technologies and Methodologies for Insider Threat', in 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC). IEEE, pp. 81-89. doi: 10.1109/CyberC.2019.00023.
5. Chanwoong Hwang, Doyeon Kim, and T. L. (2020) 'Semi-supervised based Unknown Attack Detection in EDR Environment', *KSII Transactions on Internet and Information Systems*. doi: 10.3837/tiis.2020.12.016.
6. Kyle Guercio (2020) XDR Emerges as a Key Next-Generation Security Tool, eSecurity Planet. Available at: <https://www.esecurityplanet.com/threats/xdr-emerges-as-a-key-next-generation-security-tool/>.
7. Sjarif, N. N. A. et al. (2019) 'Endpoint Detection and Response: Why Use Machine Learning?', in 2019 International Conference on Information and Communication Technology Convergence (ICTC). IEEE, pp. 283-288. doi: 10.1109/ICTC46691.2019.8939836.

# Memilih Rancangan Kartun Yang Selamat Untuk Kanak-Kanak

By | Nur Haslaily Mohd Nasir & Alifa Ilyana Chong Abdullah

Laman YouTube ibarat taman permainan buat kanak-kanak zaman sekarang. Bagaimanapun, baru-baru ini, warga maya di Malaysia telah dikejutkan dengan perkongsian tular seorang ibu muda apabila anak kecilnya yang berkarektor lemah lembut, tidak pandai marah-marah dan sayangkan adik beradik tiba-tiba telah berubah sikap. Akibat terpengaruh dengan watak kartun *Huggy Wuggy* yang ditonton melalui laman Youtube, anaknya hampir menikam adiknya sendiri dengan gunting. Watak kartun *Huggy Wuggy* yang dipaparkan sebagai pembunuh yang kejam telah menimbulkan kekecohan di kalangan ibu bapa di Malaysia, bahkan perkara yang sama turut dilihat berlaku kepada ibu bapa di negara-negara lain.

*Huggy Wuggy* ini pada mulanya muncul sebagai watak antagonis utama dalam permainan video seram Poppy Playtime pada tahun 2021 dan digambarkan berlaku di sebuah kilang pembuatan permainan yang usang dan telah ditinggalkan terbengkalai. Namun kini, populariti *Huggy Wuggy* sebagai beruang biru yang mempunyai tangan panjang, bermulut merah dengan barisan gigi yang tajam telah melonjak naik di platform perkongsian video/media sosial YouTube dan Tik Tok. Mesej yang dibawa oleh kartun *Huggy Wuggy* ialah tiada orang sayangkan kamu, keluarga harus dibunuh dan tidak wujud rasa kasih sayang di antara ahli keluarga mahupun rakan-rakan. Kartun *Huggy Wuggy* menonjolkan watak dengan nama yang comel, namun sarat dengan paparan unsur-unsur seram dan ganas yang boleh mempengaruhi minda kanak-kanak supaya memiliki sifat-sifat antagonis dan ganas.

Lebih membimbangkan adalah akhir-akhir ini, terlalu banyak rancangan kartun selain *Huggy Wuggy* ditayangkan di kaca televisyen dan laman YouTube. Ibu bapa perlu berwaspada apabila anak-anak menyebut nama-nama rancangan kartun seperti *Kissy Missy*, *Cartoon Cat*, *Among Us*, *Siren Head*, *Five Nights At Freddy's*, *Long Horse*, *Poppy Playtime*, *Happy Tree Friends*, *Rainbow Friends*, *Monica Toy*, *Mommy Long Legs & Daddy Long Legs*. Kesemua rancangan kartun yang disenaraikan ini adalah merupakan contoh-contoh lain rancangan kartun yang dikenal pasti sangat comel karektor dan namanya, tetapi bersifat ganas. Kanak-kanak

boleh terpengaruh menjadi bersikap agresif, ketagihan terhadap perkara yang berunsur kekejaman dan keganasan ataupun menjadi bersikap sebaliknya iaitu penakut, trauma dan murung. Ada juga watak kartun yang membawa mesej orientasi seks dan ekspresi jantina yang bertentangan dengan ajaran Islam, khususnya ataupun bertentangan dengan budaya masyarakat Malaysia, umumnya seperti lesbian, gay, biseksual, dan transeksual (LGBT) dan adegan perilaku seks yang sememangnya tidak bersesuaian buat kanak-kanak.

Menurut jurnal dari *U.S. National Institutes of Health*, kanak-kanak secara purata, menonton televisyen selama 10 jam atau lebih setiap minggu. Pernahkah anda terfikir adakah mungkin anak-anak anda telah menonton rancangan kartun yang salah? Sebelum melarat dan memberi kesan kepada perkembangan emosi dan mental mereka, eloklah ibu bapa mengambil tindakan segera dengan memilih rancangan kartun yang sesuai dan selamat untuk tontonan anak-anak.

## Memilih Rancangan Yang Sesuai

### 1. Pilih rancangan berdasarkan umur kanak-kanak.

Kenal pasti umur anak-anak anda. Adakah anak-anak anda berada dalam lingkungan umur bayi, kanak-kanak atau remaja? Kanak-kanak prasekolah tidak wajar menonton rancangan kartun yang memaparkan kandungan untuk kanak-kanak berusia 8 tahun dan ke atas. Manakala bagi golongan remaja, secara umumnya mereka tidak mahu menonton rancangan kartun *Cocomelon*, *Didi & Friends* atau *Pingu* yang kandungannya lebih mesra kepada kanak-kanak prasekolah. Oleh itu, pilihlah rancangan kartun yang bersesuaian dengan umur serta perkembangan minda mereka.

Sebagai contoh, rancangan kartun *BabyBus* sesuai untuk kanak-kanak berumur 2 - 6 tahun kerana penekanan pendidikannya adalah melalui lagu dan animasi untuk mereka mula belajar tentang warna, huruf, kemahiran hidup, tabiat baik dan petua keselamatan dengan

60

cara yang menyeronokkan. Rancangan kartun *BabyBus* pastinya tidak menepati selera dan kurang sesuai bagi perkembangan kecerdasan otak (IQ) remaja.

## **2. Pilih rancangan berdasarkan tahap perhatian kanak-kanak.**

Bayi dan kanak-kanak prasekolah tidak mempunyai tahap perhatian (*attention span*) yang lama. Mereka mungkin mahu bangun dari duduk setiap 5 minit, ataupun mahu melakukan aktiviti fizikal lain. Jangan paksa kanak-kanak kecil untuk duduk diam melebihi tempoh 20 minit.

Kanak-kanak yang lebih besar boleh memberikan fokus, duduk diam dan memberi perhatian untuk jangka masa yang lebih lama. Oleh yang demikian, mereka mungkin boleh menonton rancangan kartun yang berdurasi antara 20 minit sehingga satu jam.

## **3. Pilih bahasa yang baik seperti yang digunakan di rumah setiap hari.**

Kanak-kanak boleh belajar melalui rancangan kartun yang mereka tonton. Sekiranya ibu bapa menemui rancangan kartun yang menggunakan perkataan mahupun bahasa yang tidak sesuai, maka tukar kepada rancangan kartun yang bersesuaian.

Kanak-kanak selalu digambarkan seperti sebuah span kerana mereka cepat menyerap semua maklumat dari persekitaran mereka. Sebagai contoh, jika kanak-kanak dibesarkan dalam persekitaran bahasa yang tidak baik, mereka berkemungkinan besar akan meniru dan juga menggunakan bahasa yang kesat dan buruk.

## **4. Semak rancangan dengan mesej tersembunyi.**

Agak susah untuk mengenal pasti mesej yang tersembunyi selagi tidak menonton keseluruhan rancangan kartun yang ditayangkan. Jadi sebaiknya ibu bapa luangkanlah masa untuk menonton rancangan kartun bersama anak-anak. Ada rancangan kartun yang dieksploitasi dengan unsur yang tidak sihat dan ada juga yang diselitkan dengan aksi dan perilaku yang tidak bermoral.

Sebagai contoh, elakkan menonton rancangan kartun *South Park* yang kerap menggunakan bahasa kesat, sindiran seksual, kontroversi agama dan memperjuangkan hak sama rata antara lelaki dan wanita. Begitu juga dengan rancangan kartun *Family Guy* yang memaparkan mesej tidak senonoh, jenaka perkauman dan aksi keganasan. Rancangan kartun *The Simpsons* juga sarat dengan paparan watak dan senario yang boleh menjadi contoh buruk bagi anak-anak iaitu seperti adegan mabuk-mabuk,

kekerasan, bercakap kasar dan perkahwinan sesama jantina. Rancangan kartun *Jurassic World* dan *Buzz Lightyear* juga ada menyelitkan unsur LGBT yang bertentangan dengan ajaran Islam ataupun unsur tidak bermoral menerusi perilaku yang bertentangan dengan budaya masyarakat Malaysia.

Ini adalah sebahagian dari contoh-contoh rancangan kartun yang mengandungi mesej atau kandungan yang tidak baik untuk kanak-kanak. Harus diingat bahawa pada kebiasaannya tingkah laku kanak-kanak dipengaruhi oleh rancangan kartun sepertimana yang dinyatakan di atas. Sebagai contoh, anak-anak anda mungkin mula menggunakan bahasa kesat ataupun meniru perbuatan tidak bermoral dari rancangan kartun yang mereka telah tonton di sekolah.

## **5. Tentukan sama ada ia akan memberi manfaat atau tidak.**

Adakah rancangan kartun yang ditonton itu membawa apa-apa faedah atau hanya untuk hiburan semata-mata? Tidak mengapa jika anda mahu rancangan kartun itu hanya mengandungi elemen hiburan dan tanpa sebarang elemen pendidikan. Sebagai contoh, rancangan kartun *Baby Shark* amat diminati oleh kanak-kanak kerana lagu dan gerak-geri yang menghiburkan.

Kebanyakan rancangan untuk kanak-kanak yang berumur 3 hingga 6 tahun termasuklah rancangan kartun adalah berbentuk pendidikan oleh kerana kajian membuktikan bahawa mereka paling cepat belajar pada usia emas ini. Kanak-kanak yang berumur 7 hingga 12 tahun sudah boleh menonton rancangan-rancangan yang bertujuan semata-mata hanya untuk hiburan namun memerlukan kawalan dan pemantauan dari ibu bapa.

## **6. Hidupkan kawalan ibu bapa untuk anak yang lebih kecil.**

Tidak semua video yang dipaparkan dalam laman YouTube berfaedah untuk kita semua, khususnya bagi kanak-kanak. Terdapat lambakan video yang tidak bermanfaat iaitu video tersebut tidak patut sama sekali ditonton oleh kanak-kanak kerana boleh mendatangkan kesan negatif kepada mereka. Video-video sedemikian kebiasaannya memaparkan tajuk utama ataupun ilustrasi muka hadapan yang sangat menarik perhatian dan menyemarakkan sifat ingin tahu ataupun mencuba maka kerap kali akhirnya mereka akan klik ikon 'main' (*play*) kerana ingin tahu kandungan lanjut video tersebut.

Dalam senario yang lain, kanak-kanak yang naif ini mungkin tidak berniat langsung untuk menonton video-video tersebut. Namun

sekiranya laman YouTube tersebut berada dalam mod 'Autoplay On' maka adalah tidak mustahil untuk video-video sebegitu ditayangkan dengan secara automatik. Pilihlah untuk lakukan sekatan terhadap rancangan kartun yang tidak sesuai untuk tontonan kanak-kanak agar mereka tidak berpeluang untuk menonton rancangan kartun dengan ciri-ciri seperti yang dinyatakan di atas.

### 7. Lihat dalam talian untuk ulasan yang baik.

Menonton rancangan kartun tidak wajar menerima tanggapan stereotaip bahawa ia membawa kesan negatif semata-mata. Ini adalah kerana rancangan kartun yang mempunyai isi kandungan yang selamat dan membina minda juga sebenarnya boleh meningkatkan darjah IQ kanak-kanak. Carilah maklumat dari sumber-sumber yang boleh dipercayai termasuk ulasan atas talian daripada mereka yang bertaualiah berkenaan dengan kandungan rancangan kartun yang bagus untuk pembinaan diri dan kecerdasan otak kanak-kanak sedari mereka masih kecil.

Ramai berpandangan bahawa rancangan kartun *Sesame Street* amat sesuai untuk kanak-kanak berusia 3 hingga 5 tahun kerana banyak membantu dalam meluaskan perbendaharaan kata kanak-kanak dan menambahkan minat mereka terhadap bidang sains.

Rancangan kartun *Tayo: The Little Bus* pula merupakan salah satu contoh rancangan kartun pendidikan untuk kanak-kanak dengan mesej yang menyenangkan. Rancangan kartun ini memaparkan watak kartun yang comel serta penuh dengan nilai-nilai kebaikan, semangat setia kawan, mengutamakan keselamatan dan mematuhi peraturan jalan raya.

Selain daripada itu, rancangan kartun *Omar & Hana* dan *Alif & Sofia* juga merupakan contoh rancangan kartun yang menampilkan kandungan interaktif, informatif dan menarik khususnya untuk kanak-kanak prasekolah. Siri rancangan kartun ini mengetengahkan nilai-nilai murni ajaran agama Islam bagi menjalani kehidupan seharian bersama ibu bapa, guru-guru dan kawan-kawan.

### 8. Selidik rancangan yang anda mahu anak anda tonton.

Lakukan carian pantas atas talian sama ada bersumberkan maklumat dari dalam negara mahupun luar negara. Ambil perhatian dan pedoman daripada rancangan kartun yang telah dibantah dan disekat tayangannya di luar negara oleh kerana kandungannya yang bercanggah dengan nilai-nilai murni dan terpuji. Sebagai contoh, sekatan tayangan dilakukan kerana rancangan kartun itu tersebut mungkin mengandungi adegan ataupun mesej yang tidak

sesuai bagi perkembangan sosial, minda dan emosi kanak-kanak.

### 9. Ketahui keperluan anak anda.

Kebanyakan kanak-kanak seusia anak anda mungkin gemar menonton rancangan kartun *Upin dan Ipin*, *Paw Patrol*, *Dora The Explorer* ataupun *Papa Zola*. Namun begitu, ia tidak bermakna anak anda juga menyukai kesemua rancangan kartun ini.

Dapatkan maklum balas daripada anak anda tentang sesuatu rancangan kartun. Jika anak anda kelihatan tidak berminat untuk menonton ataupun tidak mahu bercakap mengenainya maka lumrahnya adalah mereka berkemungkinan tidak suka dengan rancangan kartun tersebut. Pilih dan tukarlah kepada rancangan kartun yang lebih membina diri anak anda selagi mereka masih berada dalam jagaan dan pantauan anda selaku ibu bapa.

Kesan negatif terhadap kanak-kanak kerana menonton rancangan kartun yang bersifat ganas dan tidak bermoral termasuk boleh membuatkan mereka memiliki sikap memberontak, tidak suka bergaul, agresif, penakut apabila berada di tempat sunyi ataupun gelap, berfikiran bahawa perbuatan membunuh dan memusnahkan musuh adalah perkara yang dibenarkan, serta menjadikan watak kartun sebagai idola (*role model*) dan kehidupan sebenar mereka. Oleh yang demikian, usah biarkan telefon bimbit ataupun tablet menjadi barang permainan serta teman setia anak-anak tanpa pengawasan ibu bapa ataupun penjaga yang lebih dewasa dan matang. Pantau rancangan kartun yang mereka tonton bermula dari sekarang agar tidak terlewat dan menjadi parah.

## Rujukan

1. Anak Berubah Sikap, Cuba Cederakan Adik Lepas Terpengaruh Kartun *Huggy Wuggy* di You Tube (<https://www.mingguanwanita.my/anak-berubah-sikap-cuba-cederakan-adik-lepas-terpengaruh-kartun-huggy-wuggy-di-you-tube/>)
2. Watching Television By Kids: How Much And Why? (<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4456860/>)
3. "Anak Panjat Tingkap & Cakap Akan Mati" Ibubapa Seluruh Dunia Takut Dengan Watak Pembunuh *Huggy Wuggy* (<https://www.majalahpama.my/anak-panjat-tingkap-cakap-akan-mati-ibu-bapa-seluruh-dunia-takut-dengan-watak-pembunuh-huggy-wuggy/>)
4. Pantau Kartun Tontonan Anak (<https://www.hmetro.com.my/WM/2022/08/872319/pantau-kartun-tontonan-anak>)

# General Data Protection Regulation (GDPR)

## Comparisons: Malaysia's, Singapore's Personal Data Protection Act (PDPA) And California Consumer Privacy Act (CCPA)

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

The European Union (EU) General Data Protection Regulation (GDPR) is the culmination of over 30 years of research, development, and revision. By default, it incorporates personal data protection which corresponds to some of the PDPA's content. The EU GDPR has 11 chapters and 99 articles with some significant differences with Malaysia's PDPA legislation. The objective of these laws, while comparing Malaysia PDPA and GDPR, is to safeguard the rights of data subjects and their personal information. The GDPR, however, gives data subjects more comprehensive rights. The other important differences between the four laws are as follows:

COMPARISON BETWEEN MALAYSIA & SINGAPORE PDPA, GDPR AND CCPA				
	MALAYSIA PDPA	SINGAPORE PDPA	GDPR	CCPA
WHEN DOES THE LAW GO INTO EFFECT?	JUNE, 2010 Gazetted	JULY 2, 2014 Data Protection Obligations	MAY 25, 2018 Enforcement in effect	JANUARY 1, 2020 Enforcement begins July 2020
WHICH INDIVIDUALS OR ORGANIZATIONS ARE WITHIN THE SCOPE?	<ul style="list-style-type: none"> <li>To regulate the processing of personal data in commercial transactions by data users and protect the interest of data subjects.</li> </ul>	<ul style="list-style-type: none"> <li>Collect personal data in a manner which recognises both the right of individuals.</li> <li>Protect personal data and the need for organisations to collect, use and disclose personal data.</li> </ul>	Any organization that: <ul style="list-style-type: none"> <li>Operates inside or outside the European Union (EU) and offers goods or services to consumers or businesses in the union</li> </ul>	<ul style="list-style-type: none"> <li>Collect personal data on 0K+California residents</li> <li>Have annual revenues of over \$25 million</li> <li>Earn 50% + of annual revenue from California residents' data.</li> </ul>
WHO IS AFFECTED?	<ul style="list-style-type: none"> <li>A person who either alone or jointly in common with other persons processes any personal data or has control over or authorizes the processing of any personal data</li> </ul>	<ul style="list-style-type: none"> <li>Covers virtually all businesses in Singapore</li> </ul>	<ul style="list-style-type: none"> <li>EU citizens, businesses, controllers, processors and data subjects</li> </ul>	<ul style="list-style-type: none"> <li>Business, service providers, third parties, and California consumers</li> </ul>
WHAT DATA IS WITHIN SCOPE?	<ul style="list-style-type: none"> <li>Personal data in the context of commercial transactions</li> </ul>	<ul style="list-style-type: none"> <li>Personal data collected, used, or disclosed</li> </ul>	<ul style="list-style-type: none"> <li>Personal data of any type</li> </ul>	<ul style="list-style-type: none"> <li>Personal data that is sold for monetary or other value considerations (releasing, disclosing, transferring, or even renting of the data)</li> </ul>



WHAT ARE THE FINES FOR NON-COMPLIANCE?	<ul style="list-style-type: none"> <li>Penalty for non-compliance RM100 Thousand to RM500 Thousand and or between 1 to 3 years imprisonment</li> </ul>	<ul style="list-style-type: none"> <li>Fines Up to \$5,000 to \$10,000 (depending on the offence) or imprisonment of up to 12 months for person or individuals.</li> <li>Fines up to to \$50,000 to \$100,000 (depending on the offence) for Organizations.</li> </ul>	<ul style="list-style-type: none"> <li>Up to 20 million euros or 4% of total global turnover from the prior fiscal year for the most severe violations</li> <li>Up to 10 million euros or 2% of the worldwide annual revenue of the prior fiscal year for less severe violations</li> </ul>	<ul style="list-style-type: none"> <li>Up to \$7,500 per violation with no ceiling on the number of violations</li> <li>\$100-\$750 per consumer per incident for statutory damages related to breaches</li> </ul>
--	--	--	---	--

## References

1. Rock Content Writer, "CCPA vs GDPR: Similarities And Differences Explained", <https://rockcontent.com/blog/ccpa-vs-gdpr/>
2. Construct Digital, "GDPR and PDPA: What's the Difference?", <https://medium.com/constructdigital/gdpr-and-pdpa-whats-the-difference-198df2405e4e>
3. Zul Rafique & partners, "GDPR and PDPA: What's the Difference?", <https://www.zulrafique.com.my/article-sample.php?id=757>
4. Olivia Tan, et al., Digital Tracing and Malaysia's Personal Data Protection Act 2010 amid the COVID-19 Pandemic, <https://journals.mmupress.com/index.php/ajlp/article/view/86/109>
5. "What You Need To Know? Personal Data Protection Act 2010 (Act 709)", <https://www.pdp.gov.my/jpdpv2/assets/2019/09/WhatYouNeedToKnow.pdf>

# CSM Cyber Range – an Overview

By | Ruhama Bin Mohammed Zain

Cyber range is a platform for the development, delivery and use of interactive simulation environments. A simulated environment is a representation of an organization's ICT, OT, mobile and physical systems, applications, and infrastructures. It facilitates simulation of cyber-attacks on users and their activities as well as any other Internet, public or third-party services. A cyber range leverages a combination of core technologies for the realization and use of the simulation environment as well as any additional components which are required for achieving specific cyber range use cases.

CyberSecurity Malaysia (CSM) is the national technical and specialist center for cybersecurity matters and an agency under the Ministry of Communications and Digital. This article describes how CyberSecurity Malaysia started the development of its own cyber range infrastructure by laying the foundation for required cyber range components.

There are three fundamental use cases for CSM cyber range. The first is for training of cyber security professionals with a red team (offensive) and blue team (defensive) set up. The second use case is to assess the proficiency of security professionals after training. The third is for practical assessment as part of the Global ACE Certification examination.

## Detailed Use Cases

The following is a brief description of detailed use cases for the cyber range.

First and foremost, the CSM cyber range will be used to build cyber security competency through hands-on training. Nothing beats good old-fashioned practical exercises to solidify the theories learned during training lectures. The government's current push for TVET approach in education has also reinforced this use case. In line with this approach, CSM continues to partner with universities and other institutions of higher learning in integrating hands-on module to develop practical experience in graduates where the cyber range plays a key role.

Companies looking to recruit new hires for cyber security positions can also use the cyber range to assess their competency as part of the hiring process. This will eliminate post hiring surprises where candidates were only impressive during the interview but failed to deliver during the actual job due to lack of hands-on capability.

At the national level, the cyber range can be used to develop cyber resiliency against adverse conditions, stresses, attacks, or compromises on systems that impact cyber resources of the country. This will require adding real-world systems such as SCADA (Supervisory Control and Data Acquisition) to add fidelity to the cyber range in order to mimic actual critical physical systems as closely as possible.

The cyber range can be used to hold national and international cybersecurity competitions. This popular approach encourages more participation by cybersecurity enthusiasts in order to generate interest in ethical hacking as part of the broader cybersecurity domain.

A cyber range is an ideal ground for testing of security products and solutions. This is because it provides a safe and realistic environment to conduct tests. In short, it is a general-purpose testbed that can be customized to cater for specific product testing need.

## Cyber Range Required Features

A cyber range with orchestration capabilities can support additional functionalities, which would otherwise require additional manual effort and coordination and hence, additional costs for users.

At its most fundamental level, orchestration entails setting up a virtual environment. At its highest level, orchestration may also be used to automate tasks and interaction across different components of the cyber range such as the ability to schedule attacks and user simulation, events injection to initiate collection of user activities and more, depending on specific use cases.

There is also requirement to automate scoring of completed exercises, tasks and assessments done by the cyber range participants. This is to reduce subjectivity of scoring which is an important aspect of a cyber range.

## Cyber Range Target Users

Cyber range users typically come from diverse organizations and background. Generally, they include private citizens, government staff and private corporations such as financial institutions. More specifically, some users could be security professionals from military agencies, Critical National Information Infrastructures (CNII), Computer Network Operations (CNO), Security Operations Centre (CSOC), educators, students and researchers.

## Architectural Components

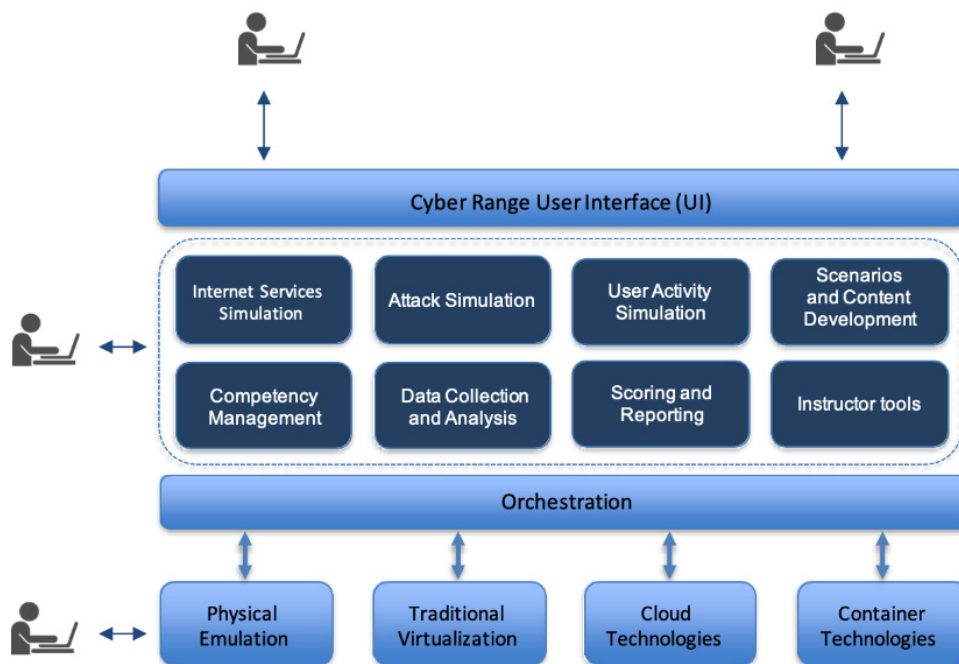


Figure A: Components of the cyber range architecture

The core architectural components of a cyber range are shown in Figure A. The components are modular in nature, so it is not necessary that all components must be present and ready before the cyber range can be used. In fact, a basic infrastructure in the form of hypervisors to create and run virtual machines and sufficient storage space to store the virtual machines are all that is required for the cyber range to start operating.

## Functionality and Use Case Matrix

In clarifying which functionality is required for which use case, Figure B attempts to capture the essence of the various requirements. This helps identify which functionality will be given priority according to the required use cases.

Functionality	Cyber Range Use Cases									
	Security Testing	Security Research	Competence Building	Security Education	Development of Cyber Capabilities	Development of Cyber Resilience	Competence Assessment	Recruitment	Digital Dexterity	National Cyber Security Competitions
Orchestration			D	D	D	D	D	D	D	D
Internet Services Simulation						D			D	
Attack Simulation	D	D	D	D	D	D	D	D		D
User Activity Simulation		D	D	D	D	D	D	D	D	D
Competency Management			D	D	D	D	D	D	D	D
Scenarios and Content Development			D	D	D	D	D	D		D
Data Collection and Analysis		D	D	D	D	D	D	D		D
Scoring and Reporting			D	D	D	D	D	D		D
Instructor Tools			D	D	D	D	D	D		D

Figure B: Cyber range functionality vs use case

## Core Technology of the Cyber Range

Based on the cyber range planning, the first step is to prepare a working virtualization server platform with a large amount of disk storage and RAM, enough to cater for multiple trainings and examination scenarios. For this purpose, a couple of rack mounted servers were installed with hypervisors to host the virtual machines. The rack mounted servers will be connected to a Network Attached Storage (NAS) through fiber channel connection to ensure optimum performance. It is estimated that each virtual machine (VM) will require at least 32GB of disk space on the NAS. Therefore, the NAS needs to hold sufficient disk capacity. Each virtual machine will require a minimum of 2GB of memory which translates to a minimum of 1TB of RAM for the servers which are running the hypervisors.

In terms of user experience, the cyber range features a full-blown User Interface (UI) that can be accessed simply from a web browser such as Google Chrome or Mozilla Firefox via HTML5 features. This will eliminate requirements for specialized client software and reduces compatibility issues.

## Challenges

There are specific challenges in terms of development effort that must be tackled in order to realize the full vision of CSM cyber range. The first challenge is the development of the orchestration component that will become the glue that combines each component and get them to work together seamlessly. The second challenge is to enhance the exercise scenarios and update them regularly so that they remain relevant in the ever-changing cyber security threat landscape.

## Conclusion

This article describes the vision and target of CSM cyber range. The basic groundwork has been done and the actual development of the cyber range is ready to proceed. In future articles, we shall chronicle the progress of CSM cyber range.

# Building Cybersecurity Talent And Capacity Through Global ACE Certification

By | Zafreida Zahrullayali

## Background

With the rapid expansion of data-driven technologies such as convergence of web, cloud, mobile, Internet of Things and the Industry Revolution 4.0, cyber threats have grown in tandem. As these technologies expand in use, so do the risks, making cyber risk management imperative for all organizations today. Protecting against targeted cyber threats without disrupting business growth is increasingly critical from a business, economic and social imperative. The environment of uncertainty coupled with the spectre of potential threats would hinder players in the ecosystem from pursuing cyber-related initiatives thus restricting economic development.

## Cybersecurity Market

According to statistics from Cybersecurity Market Report published in Q4, 2020 by Cybersecurity Ventures, the global cybersecurity market size is estimated to grow by 15 percent per year reaching USD10.5 trillion annually by the year 2025.

Global cybersecurity spending in industrial critical infrastructure sectors such as energy, transport, and water and waste management is projected to hit \$23 billion by year-end, according to a report by ABI Research. Spending is expected to grow at a compound annual growth rate of 10% to reach US\$36.67 billion by 2027.

## Cybersecurity Workforce & Education

A report from (ISC) 2 revealed that the Asia Pacific cybersecurity workforce will have more than 2.72 million unfilled positions. According to a research by the Cybersecurity Ventures, cybersecurity awareness training market size will exceed US\$10 billion globally by 2027.

The above scenario created a vacuum of opportunity in the area of cybersecurity education as evidenced by a paradigm shift of global market focus, accelerating towards a more secure and resilient cyber environment.

Competent cybersecurity personnel are required to address the shift, shape the future pathway and accelerate the adoption among communities of concerns. However, shortage of competent personnel is a global issue as competent personnel are not easily identified while the process of qualifying and accrediting is time consuming. In addition, the holistic framework of cybersecurity qualifying training and examinations have yet to be fully addressed. The above scenario has created a vacuum of opportunity in the area of cybersecurity education.

## CyberSecurity Malaysia (CSM) Workforce Development Initiatives

Guided by the government's vision towards Industry 4.0, CSM is committed towards enhancing the quality of education and knowledge of the public to become experts in the area of cybersecurity.

CSM realizes the need to contribute its expertise and technical know-how in developing the human capital. Towards this end, CSM has established a holistic framework of cybersecurity professional certification via the Global ACE Certification.

At present, there is still no Malaysia-owned version of cybersecurity education scheme in existence. A few international organizations and business entities including SANS, Cisco, Communications – Electronics Security Group (CESG), Institute of Information Security Professional (IISP) and others do run programmes in certifying cyber security skill sets.

However, these certification programmes are quite costly for the majority. In addition, the said programmes do not cater specific requirements in Malaysia.



After conducting research and current analysis on professional certification programmes in the region, CSM opted for an overall approach in professional certification aimed at enhancing the skill sets of practitioners both in technical and soft skill sets, as well as the psychological aspects of a professional.

It is also designed to provide an alternative to the current professional scheme but at a more competitive price in line with Malaysia's requirement and with a wider scope of coverage.

## Collaboration with Strategic Partners in Workforce Development

On 13 December 2016, CSM had attained approval from the Organization of Islamic Cooperation, Computer Emergency Response Team (OIC-CERT) for Global ACE Certification and its implementation in the OIC-CERT member countries. The approval itself has garnered interest from 15 countries to join the scheme as Country Chapters, underscoring their confidence in our home-grown professional certification. There are: Azerbaijan, Oman, Indonesia, Iran, Brunei, Nigeria, Egypt, UAE, Pakistan, Saudi Arabia, Turkmenistan, Kazakhstan, Sudan, France and Bangladesh.

A year after the approval, CSM initiated the Cybersecurity Technology field under the Malaysia Board of Technologists (MBOT) and was later appointed to the Technology Expert Panel (TEP). On 27 July 2017, Malaysia Board of Technologies (MBOT) approved "Cybersecurity" as a new technology field, for which Global ACE Certification will play a pivotal role. MBOT recognized Global ACE Certification as a cybersecurity professional certification pathway that needs to be pursued prior to application as a Professional Technologist or Certified Technician.

On 1 January 2019, CyberSecurity Malaysia was appointed by the Department of Skill Development (JPK) under the Ministry of Human Resources as the Industrial Lead Body (ILB) for cybersecurity sector to lead the development of National Occupational Skills Standard (NOSS). Prior to that, CSM has jointly developed NOSS Level 5 for Advanced Penetration Testing and assessment with JPK and industries. In 2020-2021, CSM developed NOSS Level 3 for Digital Forensics First Response Operation (J620-003-3:2021). In the same year, CSM also developed Occupational Framework for Cybersecurity field.

## Cybersecurity Workforce in Malaysia

Every year, about 500 cybersecurity enthusiasts in Malaysia take up competency programs to qualify themselves, upgrade and improve their knowledge to stay relevant in the sector. As of to date, there are more than 400 personnel who are certified under the Global ACE Certification. This success can be attributed to our training partners under the Global ACE Certification. In total, Malaysia had 14,240 cybersecurity knowledge workers, as of September 2022.

## Cybersecurity Capacity Building Framework

The cybersecurity capacity building framework is illustrated in Figure 1. The framework is designed for continuous appraisal in light of field experiences, aimed at developing and strengthening cybersecurity capabilities through carefully designed programs. It is presented through systematic methodology inculcating professionalism in participants in the cybersecurity practice.

The framework has been designed to achieve the following objectives:

- To nurture cybersecurity knowledge groups and/or individuals who are resilient to cybersecurity incidents;
- To nurture cybersecurity practitioners who are technically capable and proficient in operations; and
- To nurture cybersecurity professionals who are capable in strategizing, planning and executing cybersecurity initiatives.

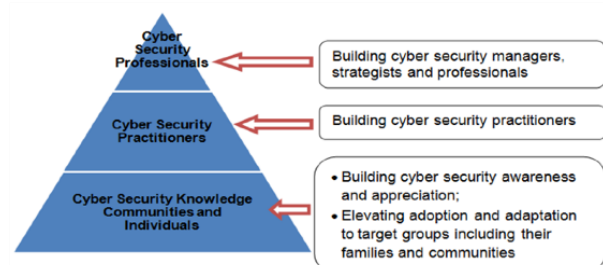


Figure 1: Cybersecurity Capacity Building Framework

## The Global Accredited Cybersecurity Education (ACE) Certification scheme

The cybersecurity capacity building framework is expanded further into the Global Accredited Cybersecurity (ACE) Certification scheme, that holistically and systematically defines the provision for cybersecurity professionals.

The Global Accredited Cybersecurity Education (ACE) Certification scheme is a holistic framework developed in Malaysia for cybersecurity professional certification through collaboration between government, industry and academia. This scheme outlines an overall approach in cybersecurity professional certification, independent assessments, impartiality of examinations, competencies of trainers, identification and classification of cybersecurity domains, and the requirement for professional memberships. This national capacity and capability program in the field of cybersecurity is recognized locally and globally by the Malaysia Board of Technologists (MBOT), Department of Skills Development, Ministry of Human Resources, and the Organization of Islamic Cooperation (OIC).

It has been developed in tandem with international standards such as the ISO/IEC 9000 series on processes, ISO/IEC 17024 on people certifications and ISO/IEC 27001 on security management to:

- Ensure workforce capabilities, ethical conducts, trustworthiness and responsibilities;
- Secure and validate core skills, knowledge, attitude and experience;
- Assure trustworthiness, ethical conducts and responsibilities; and
- Ensure capabilities at par with international standards.

The scheme enhances the knowledge and skill sets of cybersecurity personnel that comply with local and regional requirements; while ensuring a consistent and high-quality service level in its accreditation.

It is also a national project under the Malaysia 11th Plan (2016-2020) mandated from the National Security Council of Malaysia.

While the vision is to create a critical mass of qualified and competent cyber security workforce with shareable expertise across the

member countries, the goal is to establish world class cybersecurity certification programs and propagate its implementation within the region.

## Objectives

The objectives of Global ACE Certification are:

- To establish a professional certification programme that is recognized globally;
- To create world class competent work force in cybersecurity;
- To provide cybersecurity professionals with the right **Knowledge, Skills, Attitude** (KSA) and Experience;
- To be a global cybersecurity training program provider;
- To promote the development of cybersecurity professional programs globally; and
- To ensure accredited personnel are independently assessed and committed to provide a consistent and high-quality service level.

## Global ACE Certification Framework

The heart of Global ACE Scheme is the framework that advocates “**Knowledge, Skills and Attitude**” for our cybersecurity workforce.

The framework provides the base for impartial examinations and guideline on certifications, encompassing two broad categories of domains as shown in Figure 2.

The basis for cybersecurity professional certifications is defined in the Knowledge, Skills and Attitude Descriptor (KSA Descriptor) that determines the required domains and program specifications.

The KSA Descriptor consists of a list of underpinning knowledge, skills and attitudes (KSA) of identified job roles and functions. It enables qualitative and quantitative measurements of professional criteria and serves as the reference guide for the:

- Development of cybersecurity training programs;
- Development of professional examination questions and marking scheme; and
- Development of professional personnel.

The professional membership criteria listed below are used to qualitatively determine the eligibility of each applicant to be admitted as a Professional Member, Associate Member or Student Member. These criteria are:

- Experience and skills
- Cybersecurity professional certificates
- Code of conduct
- Education; and
- Continuous learning

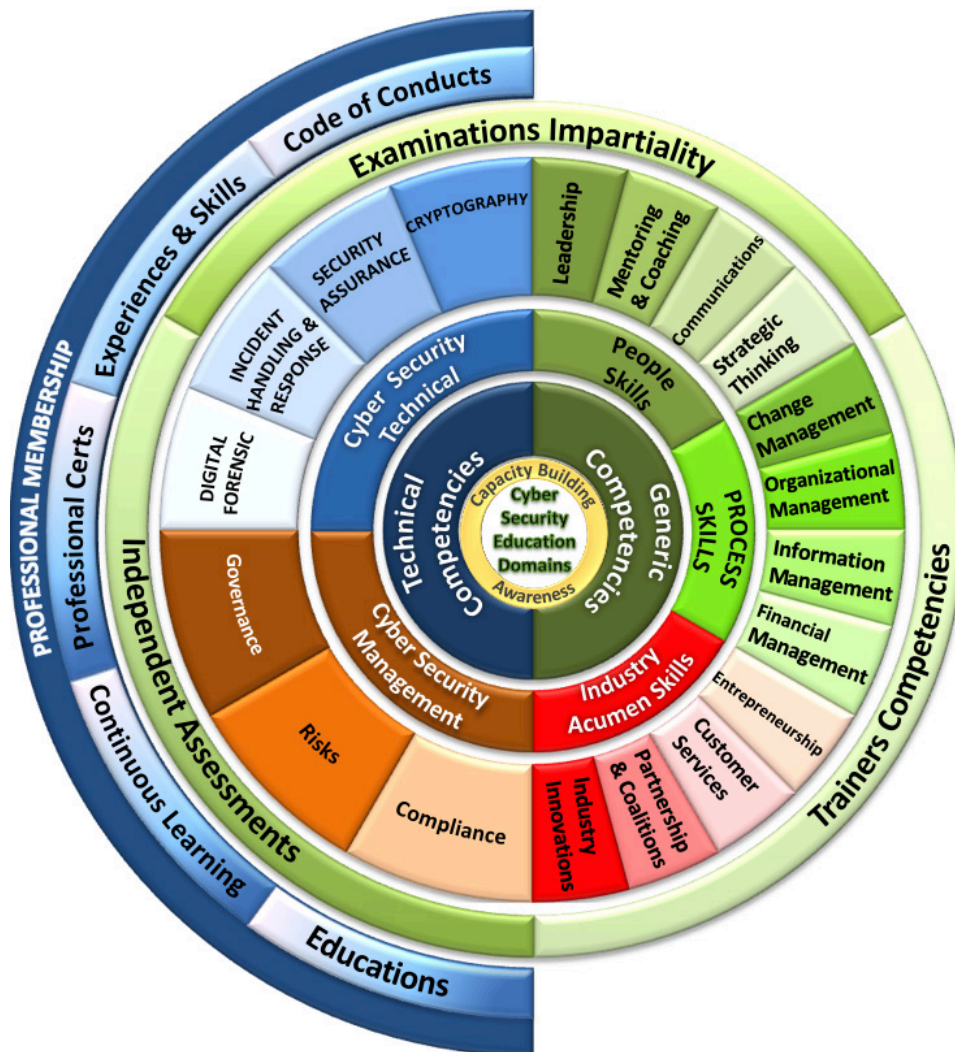


Figure 2: The Global ACE Certification Framework

## Mutual Recognition Through Global ACE Certification Recognition Arrangement

The Global ACE Certification is to be replicated by modelling its operation, products and services through the implementation of Country Chapter. The overall guidance is aligned to the Malaysia Chapter. Periodic audit exercises will be conducted at Country Chapters to ensure alignment and quality of service. All Country Chapters are mutually recognised under the Scheme. This will enable professional training programmes, trainers, professional workforce, cybersecurity products and services to be shared across the country boundaries. Figure 3 below depicts the aspiration of the Global ACE Certification Chapters.



Figure 3: Mutual Recognition Through Global ACE Certification Recognition Arrangement

## Global ACE Certification Progress

To date, CyberSecurity Malaysia (CSM) has established the required building blocks and expertise for the development of the cybersecurity professionals and knowledge workers with in-depth theoretical and technical hands-on know-how.

CSM has accumulated more than 10 years of training experience and assisted Malaysia to be positioned among the top five (5) of the ITU 2020 Global Cybersecurity Index. Based on the ITU 2020 Global Cyber Security Index, Malaysia is highly regarded in terms of cybersecurity and is ranked 5th in the Global Rankings. Going forward, CSM strives to maintain or improve upon its ranking.

So far, eleven (11) certified training programs have been established. These programmes are:

- Certified Secure Application Professional (CSAP)
- Certified Cybersecurity Awareness Educator (CCASe)
- Certified Digital Forensics First Responder (DFFR)
- Certified Penetration Tester (CPT)
- Certified Information Security Awareness Manager (CISAM)
- Certified Information Security Management Systems (CISMS)
- Certified Incident Handling and Network Security (CIHNS)

- Certified Security Operation Centre Analyst (CSOC)
- Certified MyCC Evaluator (CMYCC)
- Certified Data Security Analyst
- Certified IoT Security Analyst (CIOT)

To date, 436 personnel have been certified under the Global ACE Certification.

## Expected Outcome

Global ACE Certification has set the following expected outcomes:

- A global common platform of cybersecurity capacity building and lifelong learning;
- Inclusiveness, equitable and quality cybersecurity education in the region;
- Cybersecurity workforce with the right knowledge, skills, attitude (KSA) and experience; and
- Professional certification programmes that are recognized globally.

## Conclusion

The Global ACE Certification scheme is well on track to establish itself as the premier cybersecurity professional training programme within five years by offering inclusive, equitable and quality cyber security education in the region and globally.



# Pupuk Budaya Integriti Di Sekolah

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

## Pengenalan

Peribahasa Melayu “melentur buluh biarlah dari rebungunya” telah pun berakar umbi di negara kita. ‘Kamus Istimewa Peribahasa Melayu’ terbitan Dewan Bahasa dan Pustaka merakamkan peribahasa “Melentur buluh waktu rebung” dan takrifnya adalah mengajar anak-anak biarlah selagi kecil, apabila telah besar, keraslah hatinya dan tidak dapat diajar lagi. Namun demikian, persoalan yang lebih besar dan lebih penting adalah sejauh mana rakyat Malaysia benar-benar memahami serta mengamalkan peribahasa ini dalam erti kata yang sebenar, dan bukan sekadar menyebut dan menghafal pengertiannya. Persoalan selanjutnya pula adalah bolehkah kita serapkan pengertian peribahasa ini dalam inisiatif memupuk nilai-nilai integriti sehingga integriti menjadi budaya kehidupan seharian rakyat Malaysia.

Apakah pengertian ‘integriti’? Penulis ingin memperkenalkan pemahaman tentang istilah integriti. Kamus Dewan Edisi Keempat mendefinisikan ‘integriti’ sebagai kejujuran, keadaan sempurna dan utuh. Ia selari dengan perkataan asalnya daripada Bahasa Inggeris iaitu *integrity* yang bermaksud berpegang teguh kepada prinsip kejujuran serta mempunyai prinsip moral yang tinggi.

Apakah pula pengertian ‘budaya integriti’? Kamus Dewan Edisi Keempat mendefinisikan istilah ‘budaya’ antara lain sebagai membiasakan sesuatu perilaku (perbuatan dan lain-lain) yang baik supaya berbudi atau beradab. Manakala kebudayaan pula ditakrifkan sebagai keseluruhan cara hidup (yang merangkumi cara bertindak, berkelakuan, dan berfikir) serta segala hasil kegiatan dan penciptaan yang berupa kebendaan atau kerohanian sesuatu masyarakat, tamadun, peradaban, kemajuan (akal budi). Selanjutnya, kamus yang sama juga mendefinisikan istilah ‘masyarakat’ antara lain sebagai kumpulan manusia yang hidup bersama di sesuatu tempat dengan aturan dan cara tertentu.

Oleh yang demikian, istilah ‘budaya integriti’ dapat disimpulkan sebagai membiasakan kejujuran serta keadaan sempurna dan utuh dalam keseluruhan cara hidup merangkumi cara bertindak, berkelakuan, dan berfikir serta

segala hasil kegiatan dan penciptaan berbentuk material dan juga kerohanian sekumpulan manusia yang hidup bersama di sesuatu tempat dengan aturan dan cara tertentu. Contoh kumpulan manusia seumpama ini antara lain adalah penduduk sesebuah negara (atau negeri, bandar dan kawasan), kakitangan sesebuah organisasi, dan ahli sesebuah kumpulan ataupun persatuan.

## Pengamalan nilai-nilai murni bermula di rumah

Mengambil iktibar daripada peribahasa Melayu “melentur buluh biarlah dari rebungunya” maka mendidik anak biarlah bermula dari kecil kerana mereka lebih mudah untuk dibentuk di waktu tersebut disebabkan oleh minda kanak-kanak yang mudah untuk menerima pembelajaran baharu termasuklah teguran dan nasihat. Penerapan amalan nilai murni sewaktu kanak-kanak dapat mempengaruhi diri seseorang itu untuk menjadi insan yang berhati serta berperibadi mulia sehinggalah mereka dewasa. Oleh itu, ibu bapa wajar mengamalkan dan menunjukkan nilai-nilai murni seperti sikap jujur, sayang menyayangi, adil, tolong-menolong dan sikap-sikap murni yang lain ketika membesarkan anak-anak.

## Pemupukan budaya integriti di sekolah

Dalam kesibukan negara kita memfokuskan kepada pembangunan sains, pembangunan maklumat, komunikasi & teknologi (ICT), serta pembangunan perindustrian termasuk Dasar Revolusi Perindustrian Keempat (4IR) Negara, penduduk Malaysia dan pelbagai masyarakat lain di Malaysia turut menjadi ghairah mengejar kemajuan duniawi. Tanpa disedari, persaingan sengit tercetus sehingga mengakibatkan nilai-nilai integriti tidak lagi diutamakan malah kerap kali dilihat seolah-olah telah dipandang sepi dan dikesampingkan sama sekali.

Statistik tangkapan di negara ini yang dilaporkan oleh Suruhanjaya Pencegahan Rasuah Malaysia (SPRM) mencerminkan gejala rasuah masih



berleluasa. Pada tahun 2019, statistik tangkapan memperlihatkan sebanyak 1101 kes. Diikuti pada tahun 2020 iaitu ketika pandemik Covid-19 mula melanda, jumlah tangkapan ialah 998 kes, dan pada tahun 2021, jumlah tangkapan ialah 851 kes. Manakala sehingga Ogos tahun 2022, jumlah tangkapan yang direkodkan ialah 713 kes. Jumlah tangkapan bagi tahun 2022 berbanding tahun 2021 mempamerkan trend penurunan iaitu 83.78%, namun kuantum penurunan sebanyak 16.22% bukanlah sesuatu yang signifikan dan boleh dibanggakan. Lalu timbul persoalan, bagaimana masalah lemah integriti seperti rasuah dan sebagainya dapat dibendung atau diatasi sepenuhnya agar tidak terus menular hingga ke masa hadapan?

Penulis berpandangan bahawa jalan penyelesaian dan jawapan kepada persoalan di atas terkandung di dalam aspek pendidikan. Dalam hal ini, pendidikan integriti dan pemupukan budaya integriti wajar dijadikan elemen penting di sekolah iaitu nilai-nilai integriti harus dipupuk sejak di bangku sekolah, dan para guru memainkan peranan yang amat penting selain daripada peranan ibu bapa di rumah.

Penerapan nilai-nilai integriti dalam pendidikan telah pun diperkenalkan dalam mata pelajaran seperti Sivik, Pendidikan Agama Islam, serta Pendidikan Moral dan Sejarah. Fakta-fakta sejarah dan cerita-cerita dalam silibus mata pelajaran umpamanya, dapat dibincang dan dikaitkan dengan nilai-nilai murni yang dipegang oleh setiap individu. Zaman penyebaran agama Islam yang dipimpin oleh Nabi Muhammad SAW (Nabi SAW) banyak mengajar umat Islam betapa kukuhnya semangat integriti Baginda. Sabda Nabi SAW, daripada 'Abdullah ('Abdullah bin Mas'ud) daripada Nabi SAW *bahawasanya Baginda pernah berdoa: "Ya Allah! Sesungguhnya aku memohon kepada-Mu petunjuk, ketaqwaan, al-iffah (terhindar daripada perbuatan yang tidak baik) dan kecukupan (tidak meminta-minta)."* (HADITH RIWAYAT MUSLIM, NO. HADITH : 2721)

Dalam kata lain, Nabi SAW adalah ikon integriti. Cara hidup berintegriti Nabi SAW yang kemudiannya diamalkan oleh para sahabat Baginda, khususnya dan umat Islam lain, umumnya adalah budaya integriti yang sepatutnya dicontohi dan diamalkan pada hari ini oleh umat Islam, khususnya dan rakyat Malaysia, amnya. Ketinggian peribadi berintegriti Nabi SAW dapat dihayati apabila Baginda menerima segala bentuk perbuatan jahat, kejam dan penghinaan terhadapnya namun semua itu tidak sedikit pun melunturkan semangat dan kesabaran Baginda untuk

meneruskan perjuangan menyebarkan agama Islam.

Nilai-nilai integriti Nabi SAW seharusnya dijadikan penanda aras serta panduan dalam pendidikan terutama di sekolah. Guru-guru dan kakitangan sekolah merupakan individu yang terlibat secara langsung dalam proses pengajaran dan pembelajaran bersemuka dengan murid pada setiap hari persekolahan. Mereka harus berperanan sebagai contoh (*role model*) pelaksanaan nilai-nilai integriti dalam kehidupan seharian yang boleh diteladani oleh murid-murid. Sebagai contoh, guru-guru dan kakitangan sekolah hendaklah berdisiplin, berbudi bahasa, bersopan santun serta menjaga penampilan diri mengikut peraturan-peraturan perkhidmatan. Selanjutnya, mereka juga harus mempamerkan sikap prihatin, bertimbang rasa dan adil terhadap permintaan dan kebajikan murid-murid tanpa mengira bangsa dan agama. Selain dari itu, guru-guru dan kakitangan sekolah hendaklah bersikap jujur dalam melaksanakan tugas iaitu hanya melakukan tugas hakiki di sepanjang waktu persekolahan dan di sepanjang waktu berada dalam premis bangunan sekolah. Ini bermakna, dalam kedua-dua tempoh masa dan keadaan tersebut, guru-guru dan kakitangan sekolah sama sekali tidak menggunakan peralatan pejabat seperti telefon, mesin fotostat, internet, faksimili, komputer dan lain-lain peralatan sekolah untuk kegunaan peribadi dan kepentingan diri sendiri. Dalam hal ini, guru besar ataupun pengetua sekolah mesti bersikap tegas dalam menerapkan nilai-nilai integriti yang dinyatakan di atas di kalangan guru-guru dan kakitangan sekolah bagi memastikan mereka menjalankan tugas dengan penuh integriti, amanah, bersih dan cekap.

Guru, sebagai contoh (*role model*) juga sinonim dengan peranan sebagai mentor kepada murid. Dalam konteks ini, guru sebagai pembimbing dan penasihat yang berpengalaman dalam bidang pendidikan mempunyai tanggungjawab besar dan komitmen tinggi dalam usaha berterusan untuk meningkatkan kualiti pendidikan supaya dapat membangunkan modal insan dan masyarakat Malaysia yang maju, berakhlak mulia dan berintegriti. Sesungguhnya, tugas guru bukan sahaja mengajar dan menyampaikan ilmu, tetapi juga mendidik, membentuk sikap, nilai dan akhlak anak murid agar bertanggungjawab, berintegriti dan amanah dalam erti kata sebenar.

Selain daripada kaedah pengajaran dan pembelajaran di dalam bilik darjah, kokurikulum juga membantu dalam memupuk nilai-nilai integriti dalam diri murid-murid. Kokurikulum

di sekolah telah menjadi sebahagian daripada elemen sokongan dalam sistem pendidikan di Malaysia. Ianya telah menjadi satu kegiatan yang diwajibkan kepada setiap murid di semua sekolah menengah dan sekolah rendah. Setiap murid perlu menyertai satu badan beruniform, satu sukan atau permainan dan satu kelab atau persatuan di sekolah. Kegiatan kokurikulum dapat mengukuhkan interaksi antara pelajar dan sekaligus memupuk integrasi antara kaum di samping memupuk sifat kesopanan, berdikari, berkerjasama, berdisiplin ketika melakukan aktiviti bersama dalam kumpulan.

## Kepentingan Amalan Integriti Pada Murid Dalam Dunia Digital

Dalam kepesatan dunia digital sekarang, murid tidak hanya tertumpu kepada sesi pelajaran bersama guru di dalam kelas sahaja, malah mampu mendapatkan ilmu tambahan daripada pelbagai sumber lain termasuklah daripada internet. Penggunaan internet di seluruh dunia, amnya dan di Malaysia, khususnya telah mengalami peningkatan mendadak sehingga ke hari ini. Pelbagai video pendidikan telah dimuat naik atas talian seperti di laman YouTube dan kandungan video sebegini telah memberi banyak kemudahan kepada murid-murid untuk mendapatkan bahan-bahan rujukan dan pembelajaran atau dengan lain-lain perkataan, maklumat di hujung jari. Begitu juga dengan sesi pembelajaran atas talian dengan pelbagai platform lain seperti Zoom, Google Meet, Google Classroom, Microsoft Team, Webex dan sebagainya. Tidak dapat dinafikan bahawa internet merupakan sumber maklumat yang penting pada masakini kerana para pengguna hanya perlu layari laman carian Google untuk memperolehi apa sahaja maklumat yang dimahukan.

Sehubungan itu, kesedaran tentang penggunaan internet dengan secara berintegriti kepada murid adalah amat penting dan harus diutamakan. Amalan penggunaan internet secara berintegriti dan berhemah dapat mengelakkan berlakunya salah guna rangkaian, buli siber ataupun kesalahan yang lebih besar iaitu jenayah siber seperti penipuan (*scam*), penggodaman (*hacking*), pancingan data (*phishing*) dan sebagainya.

Didikan serta amalan budaya integriti di peringkat sekolah dapat membantu pembentukan generasi rakyat Malaysia yang mampu menggunakan internet secara berintegriti iaitu beretika, hormat-menghormati

serta mempunyai kawalan sendiri mengikut keperluan kerana nilai integriti yang sudah terbentuk dan menjadi amalan lantas bakal melahirkan generasi muda Malaysia yang menggunakan internet dan ICT secara lebih sihat dan selamat.

## Kesimpulan

Nilai-nilai integriti hendaklah diterapkan, dihayati, diamalkan, dan dibudayakan bermula dari fasa pendidikan paling asas iaitu di rumah dan di semua peringkat persekolahan/ pendidikan. Dengan adanya nilai-nilai integriti yang wujud di dalam diri segenap lapisan rakyat Malaysia sebagai budaya dan cara hidup maka dapat disimpulkan bahawa ia secara tidak langsung mampu memberi kesan positif kepada para murid dalam konteks pencapaian akademik, pertumbuhan akhlak dan cara hidup mereka.

## Rujukan

1. Definisi Integriti : <https://prpm.dbp.gov.my/cari1?keyword=integriti>
2. Nilai-nilai Murni Dalam Pendidikan <https://www.slideshare.net/JalaludinIbrahim/47283032-nilainilaimurnidalampendidikan>
3. Integriti Dalam Pendidikan [https://www.academia.edu/31995144/INTEGRITI\\_DALAM\\_PENDIDIKAN\\_IPG\\_5897fb1b5112a](https://www.academia.edu/31995144/INTEGRITI_DALAM_PENDIDIKAN_IPG_5897fb1b5112a)
4. Pemupukan Integriti Dalam Pendidikan <https://www.moe.gov.my/muat-turun/informasi-integriti-1/buletin-integriti-1/2018-8/2228-siri-3-tahun-2018-pemupukan-integriti-dalam-pendidikan/file>
5. Statistik Keseluruhan Tahun [https://www.sprm.gov.my/index.php?id=21&page\\_id=120&year=2022](https://www.sprm.gov.my/index.php?id=21&page_id=120&year=2022)

# Pengaruh Penggunaan Internet Terhadap Kanak-Kanak

By | Wan Nur Ariffa Binti Wan Abu Bakar Sidek

Di zaman serba moden ini, masyarakat pelbagai lapisan umur telah dipengaruhi oleh teknologi moden, internet, dan perkembangan media sosial yang seterusnya membentuk satu revolusi yang mengubah kehidupan sejagat. Berbeza dengan zaman dahulu, di mana asuhan serta nilai moral terutama dalam kalangan kanak-kanak kebanyakannya diterapkan oleh didikan ibu bapa, guru, dan masyarakat setempat. Sebelum adanya Internet, kanak-kanak menghabiskan masa bersama rakan-rakan bermain permainan seperti baling selipar, berbasikal, bermain guli, *police and thief*, dan sebagainya yang secara tidak langsung aktiviti sebegini merangsang perkembangan fizikal, sosial, dan emosi mereka.

Kini, hasil kemajuan teknologi digital, segala maklumat, pendidikan, dan hiburan boleh dicapai dengan hujung jari sekali gus menjadikan teknologi ini satu keperluan dalam masyarakat moden. Kanak-kanak juga tidak terkecuali di mana banyak masa diluangkan dengan melayari Internet, menonton televisyen, bermain game dan sebagainya.

Sejak kebelakangan ini, penggunaan internet dalam kalangan kanak-kanak meningkat berdasarkan statistik peratusan penggunaan internet dalam kalangan kanak-kanak mencapai 47% pada tahun 2021. Ini berikutan penularan wabak Covid-19 dan pelaksanaan Perintah Kawalan Pergerakan (PKP) sejak Mac tahun 2020 menyebabkan masyarakat perlu berada di dalam rumah, yang menyumbang kepada peningkatan penggunaan internet di kalangan kanak-kanak.

Menurut Kajian Pengguna Internet 2020 (IUS 2020), 56.3% kanak-kanak melayari internet menggunakan peranti digital secara bersendirian, tanpa pengawasan ibu bapa. Ini meningkatkan risiko kanak-kanak menjadi mangsa kepada jenayah siber, buli siber, dan pengaruh media sosial. Walaupun penggunaan peranti dan internet memberi peluang kepada mereka untuk belajar dan menonjolkan kreativiti, peralatan itu juga mendedahkan mereka kepada risiko kesihatan mental dan kesejahteraan keluarga. Sebagai contoh, kini terdapat video kartun yang di tonton melalui aplikasi Youtube antaranya *Huggy Wuggy*, *Kissy Missy*, *Siren Head*, *Mommy Long Legs*, *Poppy Playtime*, dan *Happy Tree Friends* yang

mengandungi unsur ganas yang mempengaruhi mental kanak-kanak. Ini dibuktikan oleh satu kes terbaru yang dilaporkan di Mingguan Wanita di mana seorang kanak-kanak yang bersikap lembut, sabar, dan penyayang hampir menikam adiknya dengan gunting.

Berikut adalah antara beberapa ancaman siber dan risiko terhadap kanak-kanak:

1. **Berhubungan dengan individu yang tidak dikenali.** Contohnya dalam mesej di media sosial atau ruang sembang permainan interaktif yang mendedahkan kanak-kanak kepada ancaman seksual seperti Sexting.
2. **Buli siber.** Kanak-kanak boleh menjadi sasaran dalam talian yang mempengaruhi kehidupan sebenar seperti komen negatif yang dibuat dalam talian boleh memberi kesan terhadap kesihatan mental kanak-kanak.
3. **Penipuan dalam talian seperti kecurian data peribadi.** Kanak-kanak mudah dimanipulasi dan ditipu untuk mendapatkan maklumat peribadi mereka dan keluarga.
4. **Kandungan yang tidak sesuai.** Melayari internet tanpa pengawasan ibu bapa mendedahkan kanak-kanak kepada kandungan seksual eksplisit terutamanya gambar dan video pornografi, kandungan atau grafik ganas seperti menyerang pihak lain walaupun di dalam video kartun, penggunaan bahasa lucah atau penglibatan dadah dan alkohol, termasuk memuat turun dan menyebarkan bahan cetak rompak.

Ibu bapa perlu berperanan aktif terhadap anak mereka. Ibu bapa merupakan agen yang paling dekat dan berpengaruh kepada anak dan harus membantu membimbing anak mengendalikan media dan teknologi secara positif. Antara garis panduan asas yang boleh dikongsikan adalah:

1. Mengingatkan anak supaya tidak memberikan maklumat peribadi diri tanpa kebenaran, seperti nama penuh, alamat rumah, nama sekolah, atau nombor telefon
2. Tidak berkongsi kata laluan dengan individu lain kecuali ibu bapa. Pastikan diri log keluar daripada akaun selepas penggunaan komputer awam

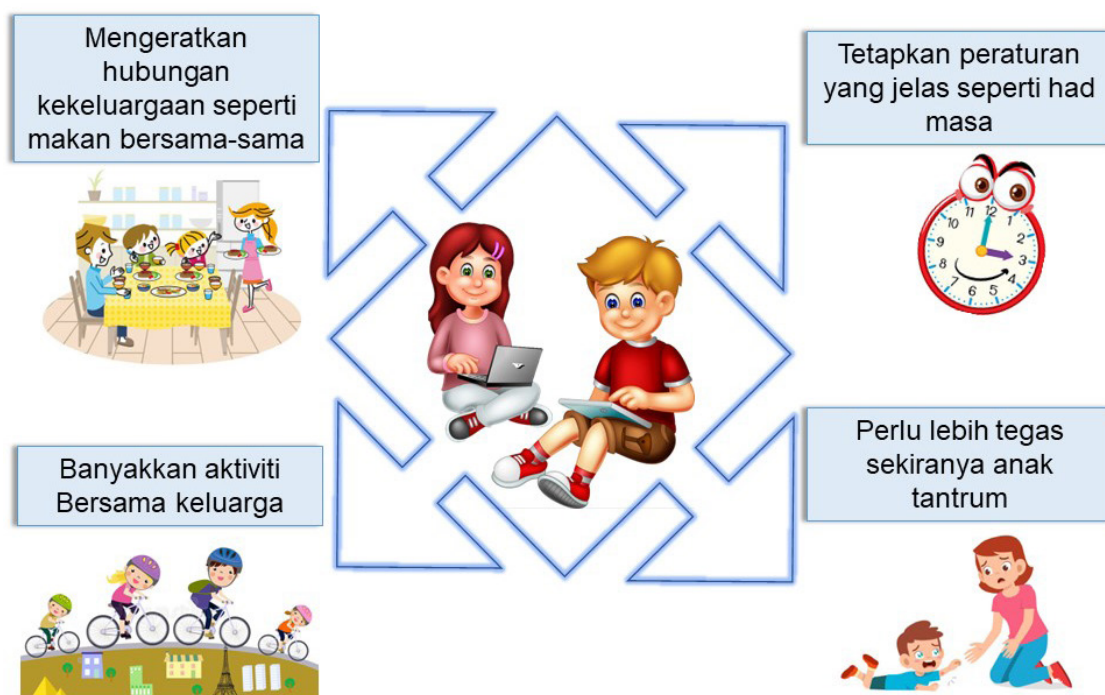
3. Nama skrin yang tidak mengandungi maklumat peribadi seperti nama penuh atau tarikh lahir
4. Mendapatkan kebenaran ibu bapa sekiranya ingin berjumpa rakan dalam talian. Ini kerana ada kalanya watak tersebut mungkin sekadar rekaan
5. Mengingatkan anak supaya tidak melayan atau membalas emel, hantaran, dan teks yang berbaur ancaman atau seksual
6. Memberitahu ibu bapa sekiranya menerima komunikasi atau perbualan yang tidak selesa seperti ancaman atau gangguan seksual.

Tidak dinafikan bahawa kanak-kanak suka melayari internet dan menggunakan peranti kerana daya tarikan kandungan yang tinggi beserta visual dan suara yang menarik. Ibu bapa merasa kagum dan bangga sekiranya anak yang baru berusia 2 tahun sudah pandai membaca ABC dan mengira 123 dengan lancar. Namun tidak dinafikan hal sebegini boleh membawa kepada ketagihan yang akan memberi kesan negatif kepada kanak-kanak. Antara kesan negatif ketagihan internet adalah:

1. **Perubahan sikap dan perkembangan otak kanak-kanak.** Ketagihan melayari internet dan penggunaan peranti boleh memberi kesan negatif kepada perkembangan otak kanak-kanak. Mereka akan mengalami masalah seperti *speech delay*, masalah kognitif, gangguan pembelajaran, peningkatan impulsif, dan kesukaran mengawal emosi.

2. **Masalah penglihatan.** Kajian menunjukkan bahawa ketagihan yang tinggi dalam melayari dan menonton video untuk jangka waktu yang lama boleh mengganggu kesihatan mata, seperti mata merah atau berair dan daya penglihatan yang semakin merosot.
3. **Obesiti.** Kanak-kanak lebih leka bermain atau menonton video daripada melakukan aktiviti fizikal seperti berjalan, berlari, melompat, dan sebagainya. Ini menyebabkan gangguan kepada perkembangan fizikal mereka.
4. **Hilang fokus dan kurang bersosial.** Kajian mendapati kanak-kanak yang mengalami ketagihan internet mempunyai kadar masa fokus yang singkat iaitu lebih kurang 4 saat berbanding 13 minit. Kanak-kanak yang ketagihan internet juga sukar untuk berkomunikasi.
5. **Tantrum.** Kanak-kanak akan tantrum jika tidak dibenarkan menonton video. Tantrum adalah tindakan agresif di kalangan kanak-kanak di mana mereka akan menangis, mengamuk dan meronta-ronta apabila keinginan mereka tidak dipenuhi.

Perkara ini sangat merisaukan memandangkan generasi kanak-kanak hari ini adalah penentu kepada pembangunan negara pada masa depan. Antara tindakan yang boleh diambil bagi mengurangkan ketagihan internet di kalangan kanak-kanak adalah:



Ibu bapa perlu memainkan peranan penting serta mewujudkan hubungan erat dengan anak-anak. Ibu bapa juga perlu mengajak anak-anak untuk selalu berkomunikasi dengan baik dan berbincang ketika membicarakan sesuatu masalah atau peraturan yang dibuat di rumah. Selain itu ibu bapa juga perlu berpengetahuan dan memiliki ilmu berkaitan dengan teknologi internet terutamanya penggunaan telefon pintar dan komputer riba untuk membolehkan mereka memantau aktiviti melayari internet oleh anak-anak.

## Rujukan

---

1. <https://www.hmetro.com.my/mutakhir/2021/03/689557/penggunaan-internet-tanpa-had-risiko-kepada-kanak-kanak>
2. [https://www.researchgate.net/publication/306256070\\_PENGARUH\\_PERANTI\\_TEKNOLOGI\\_KEPADA\\_PERKEMBANGAN\\_SOSIAL\\_DAN\\_PERMASALAHAN\\_KESIHATAN\\_KANAK-KANAK](https://www.researchgate.net/publication/306256070_PENGARUH_PERANTI_TEKNOLOGI_KEPADA_PERKEMBANGAN_SOSIAL_DAN_PERMASALAHAN_KESIHATAN_KANAK-KANAK)
3. <https://www.astroawani.com/gaya-hidup/internet-dan-media-sosial-risiko-keselamatan-terhadap-kanakkanak-326266>
4. <https://tzkrh.com/20163932/>
5. <https://www.usim.edu.my/ms/berita/in-our-words-ms/pendedahan-teknologi-media-baharu-terhadap-kanak-kanak-peranan-ibu-bapa/>
6. <https://www.bharian.com.my/berita/nasional/2017/10/340635/remaja-kanak-kanak-ketagihan-internet-serius>
7. <https://harakahdaily.net/index.php/2021/10/26/56-3-peratus-kanak-kanak-layari-internet-sendirian/>
8. <https://ms.wikipedia.org/wiki/Internet>
9. <https://theinspirasi.my/teknologi-membawa-kesan-yang-buruk-dalam-kalangan-kanak-kanak/>
10. <https://www.mingguanwanita.my/anak-berubah-sikap-cuba-cederakan-adik-lepas-terpengaruh-kartun-huggy-wuggy-di-you-tube/>



# How To Enhance Information Gathering Results With Alternative Search Engines

By | Mohd Adlan Bin Ahmad

## Introduction

It is widely known that Google is the most popular search engine in the world, as well as in Malaysia, with a usage of over 96%<sup>[1]</sup>. The statistics are shown in Figure 1 below.

search_engine-MY-monthly-202108-202208									
Date	Google	bing	Yahoo!	Petal Search	DuckDuckGo	Ecosia	YANDEX	Baidu	Other
2021-08	98.15	1.11	0.52	0.12	0.06	0.01	0.01	0.01	0.01
2021-09	98.02	1.24	0.54	0.09	0.06	0.01	0.01	0.01	0.01
2021-10	97.7	1.45	0.63	0.09	0.07	0.01	0.01	0.01	0.01
2021-11	97.5	1.56	0.71	0.09	0.08	0.02	0.02	0.01	0.01
2021-12	97.61	1.52	0.65	0.09	0.07	0.01	0.02	0.01	0.01
2022-01	97.74	1.41	0.62	0.09	0.08	0.01	0.02	0.01	0.01
2022-02	97.86	1.38	0.57	0.07	0.07	0.01	0.02	0.02	0.01
2022-03	97.58	1.6	0.57	0.12	0.07	0.01	0.02	0.02	0.01
2022-04	97.26	1.74	0.64	0.16	0.08	0.07	0.02	0.02	0.01
2022-05	97.62	1.52	0.56	0.12	0.08	0.04	0.03	0.02	0.01
2022-06	97.25	1.81	0.65	0.11	0.09	0.03	0.03	0.02	0.01
2022-07	97.16	1.87	0.69	0.12	0.09	0.03	0.03	0.01	0.01
2022-08	96.91	2.05	0.73	0.14	0.09	0.02	0.03	0.01	0.01

Figure 1: Percentage of Search Engine used in Malaysia (August 2021 – August 2022)

However, other search engines have started to gain increasing popularity and could prove to be an alternative for users to gather information. The article intends to focus on unique and specific functions (or better) of several alternative search engines apart from Google.

## Microsoft Bing Enhanced Search Function <sup>[2]</sup>

### i. Search Function “contains:”

*\*without the “*

Results: Finds pages that contains the particular types of files being searched (eg: pdf, doc, xls)

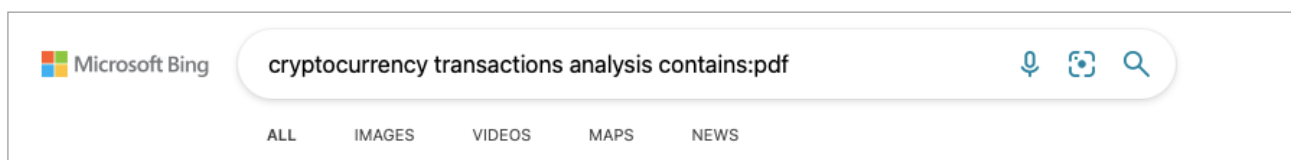


Figure 2: Contains Search Function on Bing being implemented



Figure 3: First result on Bing. The result is a Journal on March 2022



Figure 4: First result from Google, a Journal from June 2022.

In short, the search result from Bing produces the latest article using this search function.

## ii. Search Function “info:”

Results: Bing provides other information on a webpage such as related pages, external pages mentioning about the page and related results.

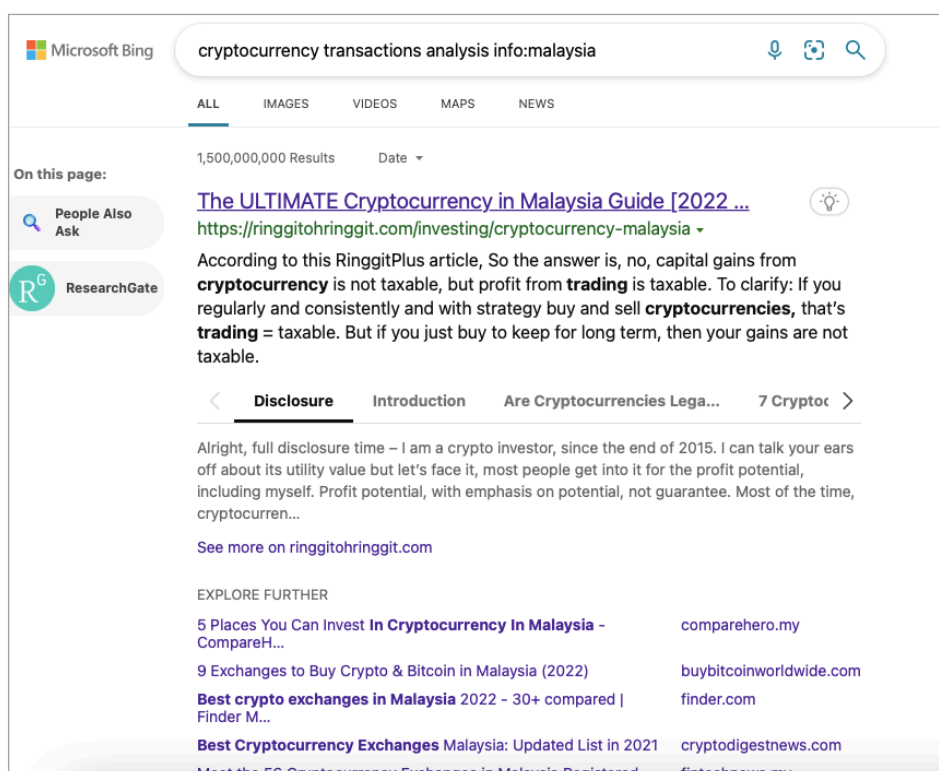


Figure 5: Results from Bing

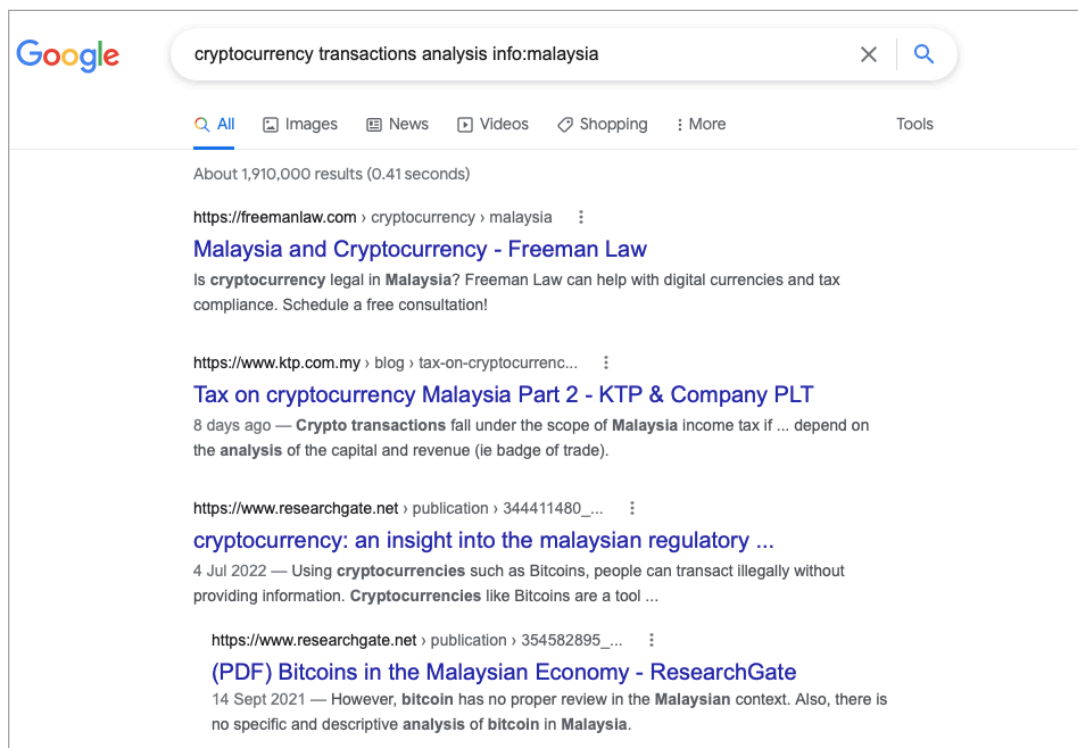


Figure 6: Results from Google

### iii. Search Function "inanchor:"

Results: Finds pages that use a specified keyword as anchor text in a link from the page.

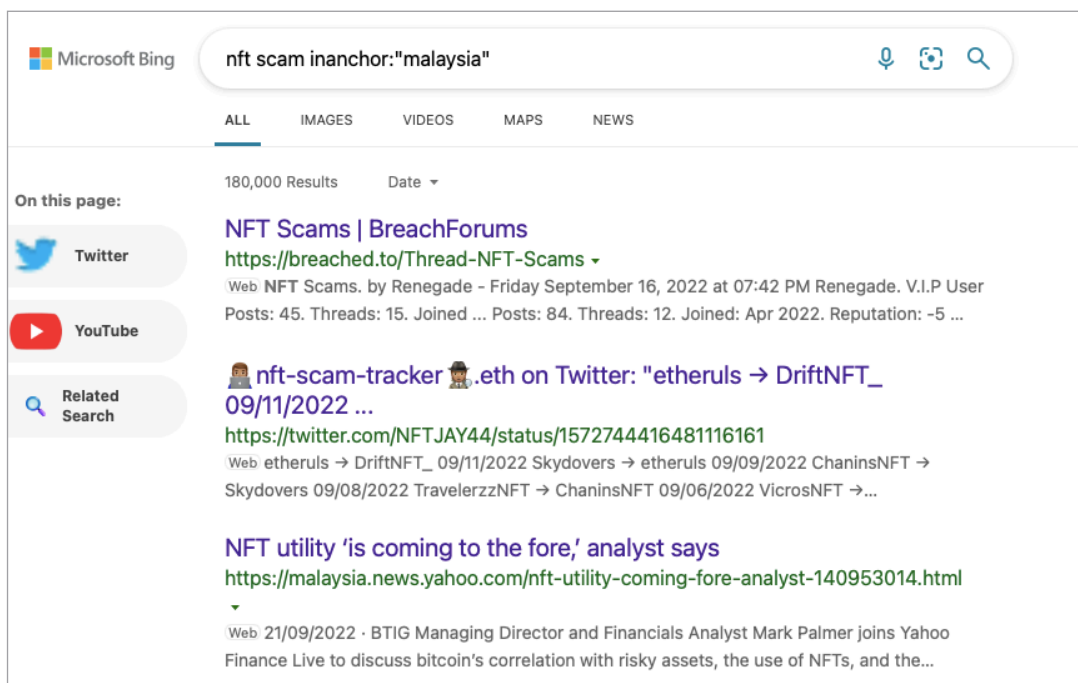


Figure 7: Results from Bing

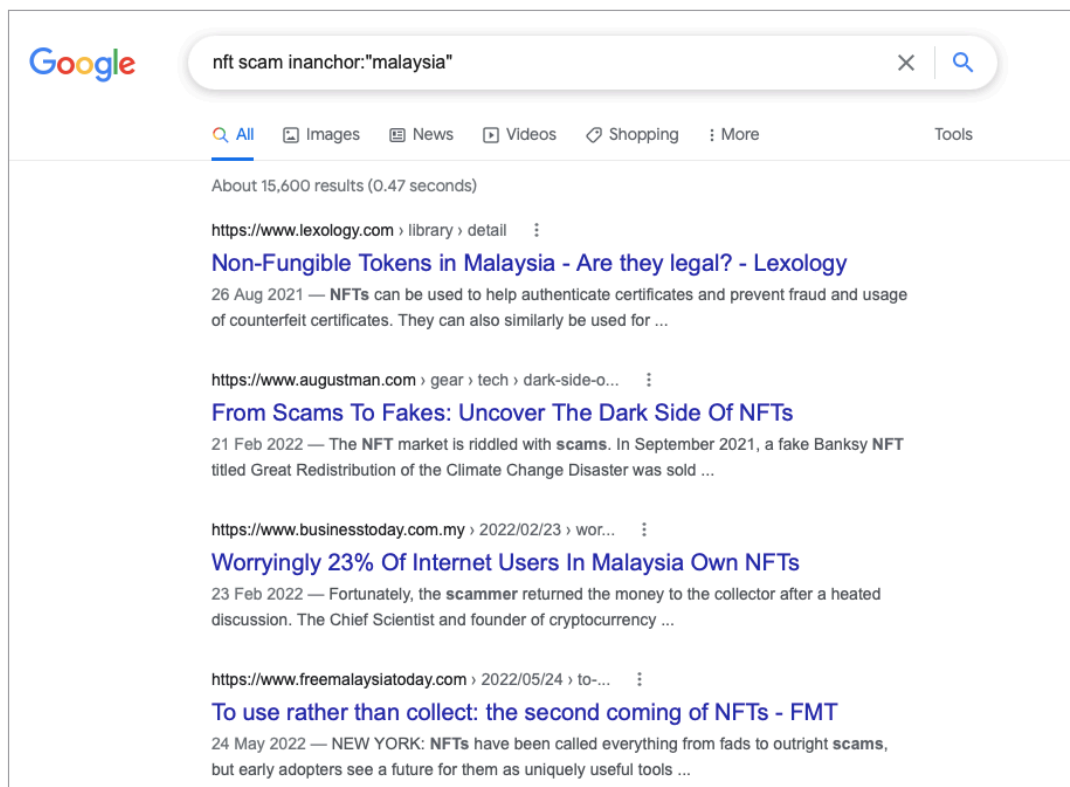


Figure 8: Results from Google

As 'inanchor' is most probably rarely used, the results are less accurate as various websites seem to display different top results. A user could use own due diligence to find relevant information.

### iii. Search Function "inbody:"

Results: Finds pages that use a specific keyword in the body section of the page.

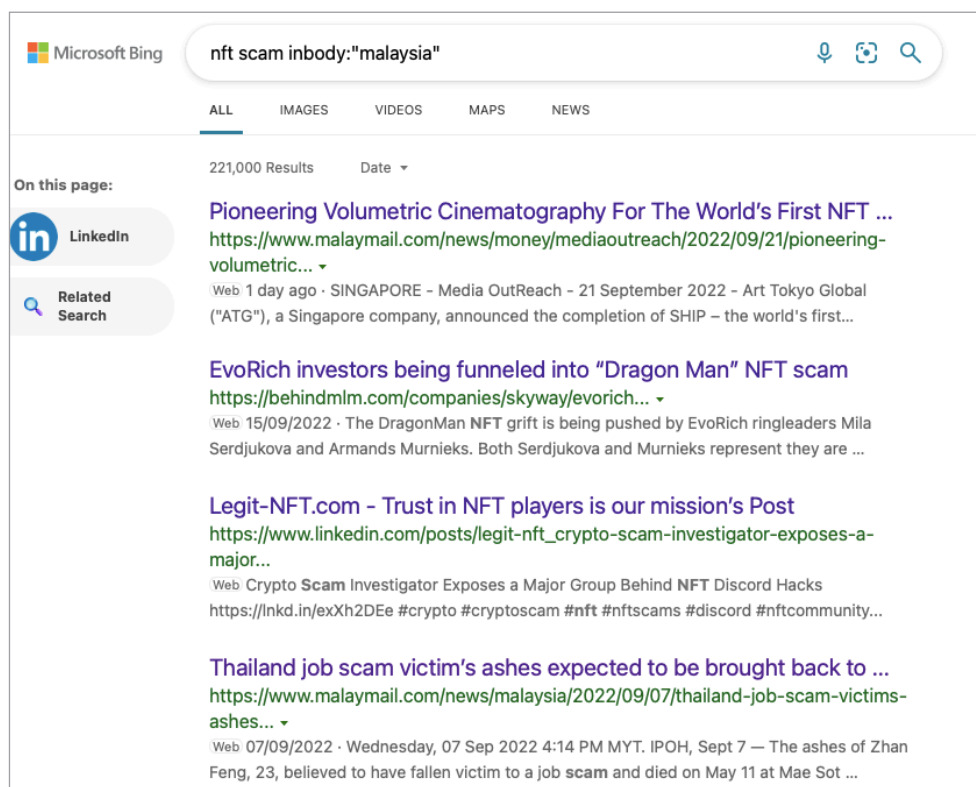


Figure 9: Results from Bing

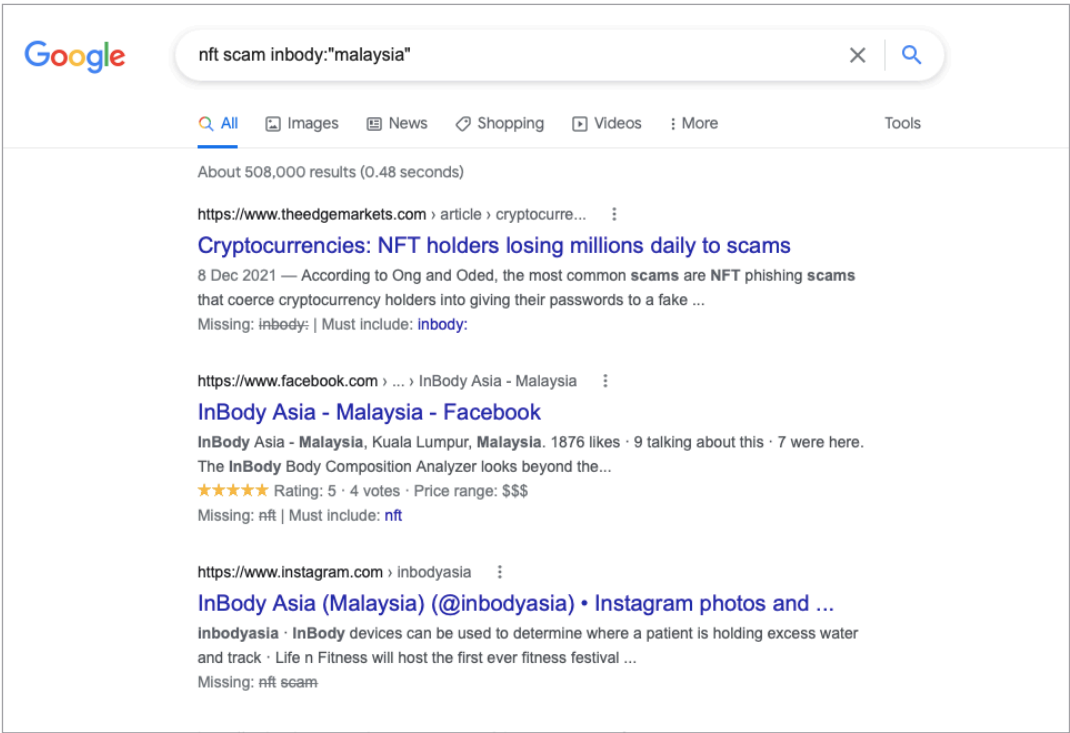


Figure 10: Results from Google

## DuckDuckGo Enhanced Function [3]

For Search Engine DuckDuckGo (DDG), we highlight the unique functions rather than its search capabilities.

### i. Search Function “lowercase”

Function: Changes the Uppercase to lowercase, comes in particularly handy in the absence of any word processing software.

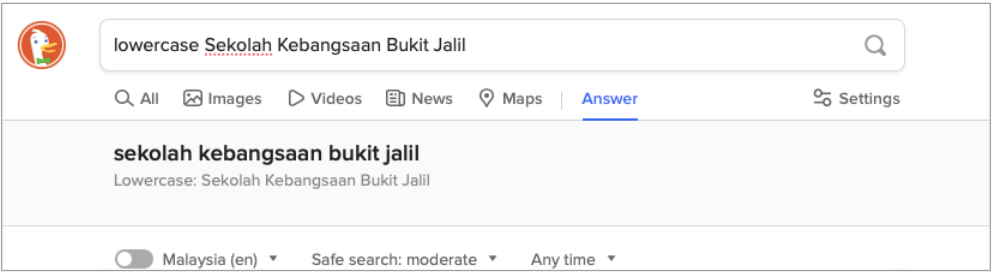


Figure 11: DDG’s search function lowercase changes the Uppercase to lowercase

### ii. Search Function “qr”

Function: Searches for a QR code of each page

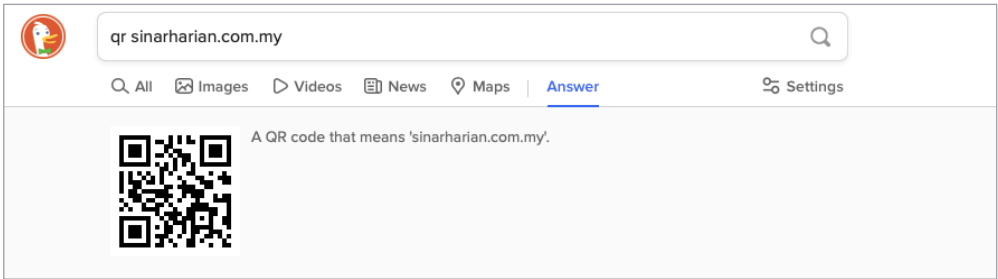


Figure 12: DDG’s qr function searches for QR code of sinarharian.com.my



### iii. Search Function “alternative to”

Function: Lists the result for the alternative answer/product/software of the search subject.

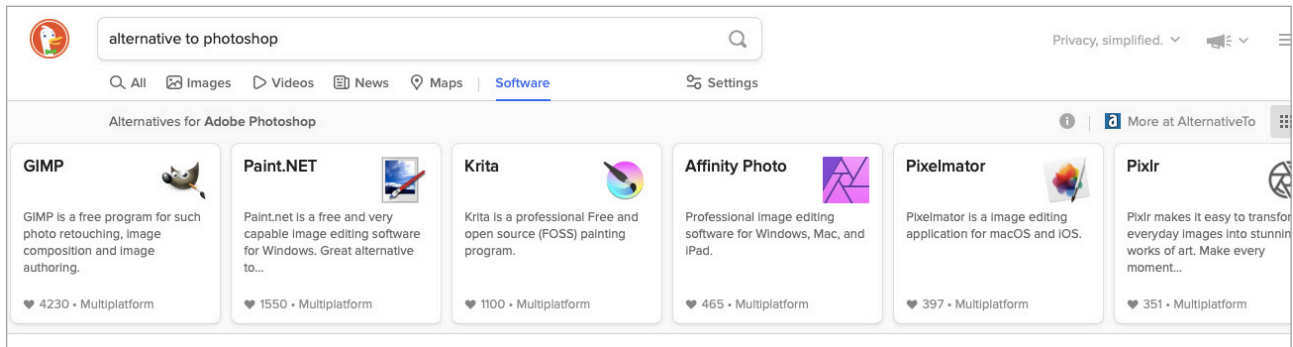


Figure 13: DDG’s ‘alternative to’ function searches for the alternative of Photoshop application

## Conclusion

There are many different approaches and techniques to gather information from the Internet. A combination of existing and unique syntax of a particular search engine could ensure that the required information is found. This article also discusses an introductory approach to alternative search engine for comparative results, as well as backup in case Google is unavailable.

## References

1. <https://gs.statcounter.com/search-engine-market-share/all/malaysia>
2. <https://www.bruceclay.com/blog/bing-google-advanced-search-operators/>
3. <https://www.makeuseof.com/tag/8-search-tricks-work-duckduckgo-not-google/>

# Human Resource Factors In Information Security

By | Sharifah Sajidah Bt Syed Noor Mohammad

Information is an organization's most valuable asset and hence, any data leakage will have disastrous and serious effects on the organization's finances and reputation. Information security is a set of practices intended to keep data secure from unauthorized access or alterations. To effectively manage information security, a business must integrate its people, procedures, and technology. Doing so will lower the likelihood of financial loss due to cyberattacks and enhance the organization's value to all stakeholders.

Cyber threats are a growing problem for companies of all sizes across all industries. Securing information has become more difficult due to increased quantity and diversity of information security threats. When it comes to information security, employees whether current or former, are typically cited as the weakest link. Information Security is defined as preventing unauthorized access, use, disclosure, interruption, alteration, inspection, recording, or damage to information.

Avoiding unauthorized access, use, disclosure, interruption, alteration, inspection, recording, or damage to information is the essence of information security. Management and protection are two key and necessary components in ensuring an organization's operation continues smoothly and uninterrupted. If these cyber threats are not prevented, it will damage an organization's reputation and financial position. Numerous organizations have made significant efforts to manage and handle the security of their data by having a systematic information security management. To ensure effectiveness of information security management, organizations should focus on both technical and non-technical aspects of Information Security Management. If organizations overlook the human component, they will not be able to safeguard the integrity, confidentiality, and availability of information assets.

Information breach can be caused by an insider threat either intentionally or unintentionally. Organizations often need to incur billions of dollars in expenditures should a security breach occur, including costs for knowledge loss, liability, and loss of customer confidence. The

implementation of safeguards is to prevent data loss and intelligence theft.

ISO/IEC 27001 is a well-known international standard for information security management (ISMS). It contains the requirements for planning, implementing, operating, and improving an ISMS. Organizations utilize this industry standard to safeguard sensitive information and manage any risks of intrusion brought on by the disclosure of confidential company information. Additionally, inadequate management on accessibility, integrity, and confidentiality of critical assets has led to information security breaches.

ISMS comprises guidelines, practices, and safeguards that are intended to achieve the following key information security goals: confidentiality, integrity and availability. By ensuring only authorized individuals can access data, it enhances confidentiality. Integrity is the maintenance of accurate and comprehensive facts. Availability entails making sure data is accessible when needed. ISMS has the ability to influence employee behaviour and offers guidance on how to behave in a way that preserves ethical standards and information security. It has a structured method for promoting and curtailing employee misbehaviour as well as managing security concerns within the company. One of the ISMS. Annex A Security Controls in ISO 27001 focuses on human resource or better known as Human Resource Security.

Human Resources Security covers three stages of employment—prior, during, and post. Each of these three components contains essential information, security controls and safeguards. This aids management in assessing and implementing crucial controls across three phases of an employee life cycle.

The goal of human resources security is to make sure that all employees (including contractors and anybody using sensitive data) are qualified for and understand their roles and responsibilities, and that access is restricted once an employment ends. The possibility of unintentional or intentional threats can be reduced by implementing effective and proportionate Human Resource security controls

at all employment phases. Details of the three phases are as follows:

- a. **Prior to Employment.** Human resources pre-screening of personnel is one of the most effective security procedures to stop any potential theft of sensitive corporate data and assets. The scope of a background check should cover the risks involved, requirements of the business, and classification of information that will be accessed. Besides that, information security obligations for both the company and its personnel must be stated in the contracts with contractors and employees. These agreements, which carry legal weight, or supported by the law, should clearly spell out the responsibilities and duties of the position. Defining contract terms and defining information security responsibilities for both the employer and the employee in an employment contract should be done at this stage.
- b. **During Employment:** In order to lower the risk of human error, it is important to make sure that all employees, contractors, and third-party users are knowledgeable about information security threats and concerns, their responsibilities and obligations, and the methods necessary to support organizational security policy during the course of their daily work. Employees, and other users who are not well-informed about their security duties could seriously harm a company. An organization's assets could be mishandled or security may well be overlooked as a result of poor management. Therefore, to ensure that security is applied throughout an employee's tenure at the organization, his or her management duties need be clearly defined. To lessen potential security threats, all employees, contractors, and third-party users should also be given regular training and informed about ongoing updates in its policies and procedures, security processes and the proper use of information processing facilities. Security breaches must be handled through a structured disciplinary procedure.
- c. **End of Employment.** To ensure proper security protocols when employees, independent contractors, and other third parties leave the organization or change positions in a controlled manner, their access to the company's information system should be removed immediately. They should also be held accountable for returning all equipment previously issued to them. If this is not well managed, there is a high risk that employees could gain remote access to corporate

data or use the company email account for illegal acts, with damaging consequences. Hence, Human Resource Security aids in protecting the organization from incompetent individuals who may breach data and harm the business' reputation. Any ongoing contractual obligations, security requirements, and if applicable, commitments outlined in any confidentiality agreements, as well as any terms and conditions of employment that will continue for a set amount of time post-termination should be included in the communication of termination responsibilities. Examples include maintaining confidentiality and refraining from removing any corporate data.

The success of ISMS hinges on human activities, such as information security awareness, senior management support, security knowledge and skill sets, as well as ISMS deployment. The implementation of policy deterrent controls from Human Resources' has benefitted information security. Deterrence reduces the likelihood that someone will break the law. The Human Resource should be in charge of making sure that every employee is aware of rules, security policies, and processes, as well as the disciplinary measures that will be applied in the event of a violation. Additionally, it means that the Human Resources team will be entrusted with collaborating with management to investigate and correct any irregularities in the event of an incident and enforcing disciplinary actions as required. This is to protect companies from legal liability and deter other employees from breaking the rules.

Human Resource Security empowers a leader to accomplish his goals on information security. To help with the systematic and cost-effective security of their information, the staff could use ISO 27001 to learn how to conduct internal ISMS audits. The staff could be simultaneously trained in ISMS improvement techniques. An enhanced system and data security and dependability will help elevate consumer and business partner's trust. Employee adherence to ISO 27001 will ensure that information security is ingrained in corporate culture and increases resilience against cyberthreats.

By giving clear instructions, leading by example in terms of information security, and devoting proper budget to ISMS programmes, the management could consistently commit to and support the organization's security goals and objectives.

## Conclusion

The ISMS Team should be led by a select few employees who has regularly participated in most ISMS operations. The ISMS team's expertise, abilities, dedication, willingness, and cooperation is crucial to successfully executing ISMS processes. The staff should have extensive Information Security knowledge and should always be kept up to date on security-related concerns. They must also be skilled, work well together, and be dedicated to their tasks.

Human Resources Security is a crucial aspect of every organization's overall information security posture. Almost all businesses depend on their employees to succeed, but at the same time, they are also a major source of risk. Before employees begin working for an organization, they need to be made aware of their duties and responsibilities on information security. By implementing controls in critical areas, an organization could ensure that those who are under its authority are recruited, managed, and trained in a secure manner.

## References

1. Alavi, R., Islam, S. & Mouratidis, H., (2014). A Conceptual Framework to Analyze Human Factors of Information Security Management System (ISMS) in Organizations. LNCS, 8533, 297-305.
2. Alexei, A. (2021). Ensuring Information Security In Public Organizations In The Republic Of Moldova Through The ISO 27001 Standard . Journal of Social Sciences, 84-94.
3. Balch, S. (2015, March 3). Employee security screening procedures: What employers need to know. Retrieved from Phoenix Business Journal: <https://www.bizjournals.com/phoenix/blog/business/2015/03/employee-security-screening-procedures-what.html>
4. Carolina. (2018, May 27). Cola-Cola breach: ex-employee stole hard drive with 8,000 workers' data. Retrieved from Hackread: <https://www.hackread.com/cola-cola-breach-ex-employee-stole-hard-drive-with-8000-workers-data/>
5. Casper, W. J., & Harris, C. M. (2008). Work-life benefits and organizational attachment: Self-interest utility and signaling theory models. J. Vocat. Behav., 72(1), pp. 95-109.
6. Chaudhary, Shivang. (2018). Interpretation of p value in a model with lack of fit?. Retrieved from [https:// www.researchgate.net/post/Interpretation\\_of\\_p\\_value\\_in\\_a\\_model\\_with\\_lack\\_of\\_fit4/5b3707bdeb8703286733cc11/citation/download](https://www.researchgate.net/post/Interpretation_of_p_value_in_a_model_with_lack_of_fit4/5b3707bdeb8703286733cc11/citation/download)
7. Chiang, A., & Toelle, E. (2022, March 1). Microsoft shares 4 challenges of protecting sensitive data and how to overcome them. Retrieved from Microsoft Security: <https://www.microsoft.com/security/blog/2022/03/01/microsoft-shares-4-challenges-of-protecting-sensitive-data-and-how-to-overcome-them/>
8. Chronchio, J. (2018, May 31). HR and IT Collaborate: Tech, Cyber Security and Employee Experience. Retrieved from Motus: <https://www.motus.com/hr-and-it-collaborate-cyber-security/>
9. Cundle, S. (2021, February 18). 8 Best Practice Guidelines for Human Resource Security. Retrieved from enbordero: <https://blog.enbordero.com/index.php/2021/02/18/8-best-practice-guidelines-for-human-resource-security/>
10. Dataprise. (2021, July 14). Preventing Remote Workforce Cybersecurity Threats for Hybrid Teams. Retrieved from DATAPRISE: <https://www.dataprise.com/resources/blog/preventing-cybersecurity-threats-hybrid-workforce>
11. Garska, K. (2017, October 10). Why You Need to Immediately Cut Data Access When Employees Leave. Retrieved from Identity Lifecycle Management, Cybersecurity: <https://blog.identityautomation.com/why-you-need-to-immediately-cut-data-access-when-employees-leave>
12. Georgescu, E. (2021, February 8). Internal Threats: A Major Risk to Any Business.
13. Halim, H., & Yusof, M. M. (2019). Framework for Digital Data Access Control from Internal Threat in the Public Sector. International Journal of Advanced Computer Science and Applications (IJACSA), 61-67.
14. HiComply. (2021, November 30). ISO 27001 Annex A.7: Human Resource Security. Retrieved from hicomply: <https://hicomply.com/resource-hub/iso-27001-annex-a-7-human-resource-security>
15. Humaidi, N., & Balakrishnan, V. (2012). The Influence of Security Awareness and Security Technology on Users' Behavior towards the Implementation of Health Information System: A Conceptual Framework.
16. Humphreys, T., & Angelika Plate (2006). Measuring the effectiveness of your ISMS implementations based on ISO/IEC 27001.

Human Resources for Information Security. (2020). y

17. Irwin, L. (2022, March 21). Guide to ISO 27001 Human Resource Security.

18. ISO/IEC 27001:2005 Information technology - Security techniques - Information Security Management Systems - Requirements  
2. ISO/IEC 27002:2005 Information technology - Security techniques - Code of practice for information security management

19. Khachatoorian, A. (2015, February 13). Data Breaches and Security in Human Resources.

20. Kumah, P. (2020). The Role of Human Resource Management in Enhancing Organizational Information Systems Security. In S. Misra & A. Adewumi (Eds.), Handbook of Research on the Role of Human Factors in IT Project Management (pp. 278-303).

21. M, E. E. (2003). Information Security Management – A New Paradigm. Information Security Management – A New Paradigm , 130 –136.

22. Machado, H. (2021). 5 Critical Security Threats to Monitor in Your New Hybrid Work Environment.

23. Marchant, K. (2021, February 12). Disciplinary Procedures: step-by-step guide managers.

24. Marshall, S. (2019, September 16). The Importance of Security in Human Resources.

25. MITSDE. (2018, February 27). Three Important Phases of Human Resource Management.

26. Nagele-Piazza, L. (2018, March 14). 6 Ways HR Can Help Prevent a Data Breach.

27. Nasir, A., Arshah, R. A., Hamid, M. R. A., & Fahmy, S. (2019). An analysis on the dimensions of information security culture concept: A review. Journal of Information Security and Applications, 44, 12-22.

28. Nasir, A., R.A Arshah & M.R.A Hamid et. al (2020). Information Security Culture for guiding employee's security behaviour: A pilot. The 6th IEEE International Conference on Information Management Study.

29. Nasir, M. Rashid, & A. Hamid, (2018). Conceptualizing and Validating Information Security Culture as a Multidimensional Second-Order Formative Construct, In The Thirteenth International Multi- Conference on Computing in the Global Information Technology (pp. 1-8).

30. Pahnla, S., Siponen, M., & Mahmood, A. (2007). Employees' behavior towards IS security

policy compliance. In System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on (pp. 156b-156b). IEEE.

31. Rasmussen, S. (2020, February 11). Limit access to data to prevent breaches.

32. Remote Work Security: 12 Best Practices for Employers. (2021). Retrieved from Time Doctor: <https://www.timedoctor.com/blog/remote-work-security/>

33. Rossi, B. (2015, June 9). The top five data admin errors costing companies millions – and how to fix them.

34. Talamantes, J. (n.d.). Danger In Your Ranks: 7 Times Employees Caused Damaging Data Breaches.

35. Tunggal, A. T. (2022, August 8). What is Information Security. Retrieved from UpGuard: <https://www.upguard.com/blog/information-security#>



# DNA Techniques In DNA Based Cryptography

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

## Introduction

There are currently many cryptographic algorithms available in the market ranging from Symmetric Block Cipher, Symmetric Stream Cipher, Asymmetric Cryptographic to Hash Function and so on. With the continuous advancement in technology, there are now more ways than ever to crack cryptography. The security of most cryptographic algorithms and the infrastructure or platform they are stored have now become more vulnerable to attacks. It is getting easier to break these algorithms. Conventional cryptographic algorithms implemented in binary computers have various physical constraints, especially in data storage and computational processes. It is a common approach for a cryptographic algorithm to have a large keyspace and complicated algorithm to strengthen its security. However, the cryptographic key generation, key retrieval, data encryption and data decryption process becomes more time consuming. The quality of the algorithms also continues to be a cause of concern. Therefore, as conventional cryptography has severe security problems, those in the field of information security will need to find new ways of protecting confidential information.

Over the years, there have been many studies by researchers and cryptographers to improve the security and performance of cryptographic technology. Among them are quantum cryptography and DNA cryptography. DNA cryptography is a new cryptographic method that is inspired from DNA computing by using DNA molecules as information carrier and DNA techniques to replace the operations and mathematical computations which exist in conventional cryptography. Due to DNA's natural properties of massive parallelism and huge storage capacity, sustainable solution to support cybersecurity and privacy can be achieved using DNA cryptography.

## DNA Computing And DNA Based Cryptography

DNA computing is an inter-disciplinary area in bio-computing which is concerned with the use of DNA molecules for the implementation

of computational processes. It is an emerging branch of computing technology which is able to solve problems beyond the scope of what a traditional electronic computing can resolve. In DNA computing, performing logical and arithmetic computations are done using biological molecules properties of DNA instead of using the traditional carbon/silicon chips.

The preliminary idea of using molecules and atoms for computations was first introduced by Richard Feynman way back in 1959. Many years later, in 1994, Prof. Leonard Adleman, a computer scientist from University of Southern California, who represents the 'A' in RSA algorithm described the capability of biological molecular computation to solve complex computational problem. Prof. Leonard Adleman is then known as the pioneer of DNA computing. He built the first DNA based computer to solve a mathematical and computer science problem, the directed Hamiltonian Path Problem also known as the Travelling Salesman Problem.

DNA computing technology has many advantages compared to the traditional electronic computing. Among the most important advantage that DNA computing has to offer is the massive parallelism property. This unique property is achieved from the binding properties between nucleotides bases (A binds with T and C binds with G) that offers the possibility of creating self-assembly structures. With a considerable amount of self-replicating DNA, computation will be a lot more efficient compared to the traditional computer which requires a lot more hardware. Because of this massive parallelism property, complex mathematical equations or computational problems can potentially be solved more efficiently at a much lesser time.  $10^{18}$  processors working in parallel can easily be handled, which means huge problems can potentially be solved by parallel search.

Another important advantage of DNA computing is its huge storage capacity property. Each DNA molecule or group of molecules can store up to a billion times data which exceeds the capacity of any traditional storage such as magnetic media, optical media, electronic and physical. One gram of DNA contains  $10^{21}$  DNA bases, which can store nearly equal to  $10^8$  terabytes of data. A single gram of DNA may have the potential of storing the same amount of information that

could fit in one trillion CDs. In other words, a few grams of DNA molecules have the capacity to contain all the data stored in the world. DNA stores memory at a density of about 1 bit/nm<sup>3</sup>, whereas conventional storage media requires up to 10<sup>12</sup> nm<sup>3</sup>/bit.

Besides the two above advantages, DNA computing is highly energy efficient. DNA computing does not require much power efficiency during computational, and therefore the consumption of power is low, which is around 2 × 10<sup>19</sup> operations per joule. This technology is clean as no toxic materials are used. It is also inexpensive because readily available materials are used, and it is smaller in size than any existing computers.

DNA cryptography, a relatively new field of cryptology has emerged from the outstanding development of DNA computing. It is a technique of hiding data in the form of DNA and combining it with any conventional cryptographic algorithm to enhance security of cryptographic algorithms. The massive parallelism and huge storage capacity properties of DNA are important elements which can be implemented for all kind of cryptographic purposes such as encryption / decryption, authentication, signature / verification and others. In this DNA cryptographic field, DNA chemistry is used to replace the mathematical aspect of cryptography, therefore it is immune to the attack from super computers. DNA cryptography was first established by Gehani, LaBean and Reif in 2004 when they published a paper entitled DNA-based Cryptography.

## Basic DNA Concepts And Techniques Implemented In DNA Cryptography

1. Watson-Crick Complementary Rules
2. DNA Encoding / Decoding Rules
3. DNA Operation Rules: DNA XOR, DNA Addition, DNA Subtraction
4. DNA Triple Codon Code
5. DNA Hybridization (DNA Annealing)
6. DNA Transcription and DNA Replication

Six DNA concepts and techniques will be discussed in this section. However, there are many more which is not discussed in this paper.

### 1. Watson-Crick Complementary Rules

A DNA sequence consists of four nitrogenous bases: Adenine (A), Guanine (G), Cytosine (C)

and Thymine (T). In total, there would be 4! = 24 possible types of combinations of these DNA bases. These combinations are as follows:

CTAG	CTGA	CATG	CAGT	CGTA	CGAT
TCAG	TCGA	TACG	TAGC	TGAC	TGCA
ATCG	ATGC	ACTG	ACGT	AGCT	AGTC
GTAC	GTCA	GATC	GACT	GCTA	GCAT

According to Watson-Crick complementary rule, A and T are complementary, and G and C are complementary. Therefore, to fulfil this complementary relationship between DNA nitrogenous bases, only eight types of DNA combinations are considered suitable:

For pair A and T:	CTAG	CATG	GTAC	GATC
For pair G and C:	TCGA	TGCA	ACGT	AGCT

Either one from these eight DNA combinations can be used in the implementation of DNA cryptography.

### 2. DNA Encoding / Decoding Rules

DNA encoding / decoding is the process of mapping two binary bits to DNA representation, and vice versa. The eight encoding / decoding rules of the above DNA combinations are as shown in Table 1 below. In this paper, Rule 1 is considered; 00 – C, 01 – T, 10 – A, 11 – G.

	Rule 1	Rule 2	Rule 3	Rule 4	Rule 5	Rule 6	Rule 7	Rule 8
00	C	C	G	G	T	T	A	A
01	T	A	T	A	C	G	C	G
10	A	T	A	T	G	C	G	C
11	G	G	C	C	A	A	T	T

Table 1: DNA Encoding / Decoding Rules.

### 3. DNA Operation Rules: DNA XOR, DNA Addition, DNA Subtraction

DNA operation rules such as DNA XOR, DNA addition and DNA subtraction are manipulated using traditional binary XOR, binary addition and binary subtraction respectively. If DNA addition rule is implemented in the encryption algorithm, DNA subtraction rule needs to be implemented in the decryption algorithm, and vice versa. Table 2 shows the DNA XOR, DNA addition and DNA subtraction rules.

DNA XOR rule					DNA Addition rule					DNA Subtraction rule				
C	T	A	G		C	T	A	G		C	T	A	G	
C	C	T	A	G	C	C	T	A	G	C	C	G	A	T
T	T	C	G	A	T	T	A	G	C	T	T	C	G	A
A	A	G	C	T	A	A	G	C	T	A	A	T	C	G
G	G	A	T	C	G	G	C	T	A	G	G	A	T	C

Table 2: DNA Operation Rules.

#### 4. DNA Triple Codon Code

A codon is made up of three consecutive nucleotides sequence, or called trinucleotide sequence. These codons correspond to a specific amino acid, and the combination of different amino acids makes protein. In DNA cryptography, triple codon code is used as a substitution method. A random lookup table that contains DNA triple codon code and their corresponding equivalent alphabet or value is used.

#### 5. DNA Hybridization (DNA Annealing)

As described above, DNA structure is presented in a double helix structure with two DNA strands; the sense strand and the antisense strand. These individual two strands are known as single stranded DNA (ssDNA). DNA hybridization or also known as DNA annealing is the process of combining two antiparallel ssDNA to form one double stranded DNA (dsDNA). The combining process must satisfy Watson-Crick complementary rule where A always pairs with T and G always pairs with C. In DNA cryptography, hybridization or annealing is performed by concatenating the antisense strand after the sense strand to form a larger DNA sequence.

#### 6. DNA Transcription and DNA Replication

These two are the operations of converting DNA sequence to protein sequence in Central Dogma process. Transcription of dsDNA sequence to single stranded RNA (Ribonucleic Acid) sequence is by swapping the Thymine (T) nitrogenous base in DNA to Uracil (U) base. Translation is the process of converting the RNA sequence to its protein form. In this process, RNA is read in three letters codon formed from four RNA bases, which gives a combination of 64 codons. These codons form 20 different amino acids. Combination of amino acids in sequence forms protein.

### Conclusion

Cryptography has been extensively employed in the field of information security for protecting and providing security to confidential data. In recent

years, the field of cryptography has emerged to consider a hybrid cryptographic implementation which combines conventional cryptographic techniques with the knowledge of DNA technologies to formulate DNA cryptography. DNA based cryptography is considered as one branch of sustainability science as it combines a transdisciplinary structure of natural sciences and technological sciences. This article discussed various DNA techniques implemented in recent DNA cryptographic algorithms. Among them are Watson-Crick Complementary Rules, DNA Encoding / Decoding Rules, DNA Operation Rules, DNA Triple Codon Code, DNA Segmentation, DNA Hybridization (DNA Annealing), and DNA Transcription and DNA Replication from the Central Dogma Molecular Biology process.

### Reference

- Gupta, R. & Jain, A. (2014). A New Image Encryption Algorithm based on DNA Approach. *International Journal of Computer Applications*, 85(18), 27-31.
- Jayakumar, A. (2020, August 5). Introduction to DNA Computing and its Applications.
- Karimi, M. & Haider, W. (2017). Cryptography using DNA Nucleotides. *International Journal of Computer Applications*, 168(7), 16-18.
- Kaur, M. (2012). DNA Computing: Its Advantages and Future. *Journal of Teaching and Education*, 1(7), 51-59.
- Kolate, V. & Joshi, R.B. (2021). An Information Security Using DNA Cryptography along with AES Algorithm. *Turkish Journal of Computer and Mathematics Education*, 12(1), 183-192.
- Loeffier, J. (2019, March 11). What is DNA Computing, How Does It Work, and Why It's Such a Big Deal.
- Martyn, A. (2019, February 11). DNA Computing. *Encyclopaedia Britannica*.
- Mondal, M. & Ray, K.S. (2019). Review on DNA Cryptography. *ArXiv*(1904.05528v1).
- Nafea, S.S. & Ibrahim, M.K. (2018). Cryptographic Algorithm based on DNA and RNA Properties. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, 7(11), 804-811.
- Patnala, B.D. & Kumar, R.K. (2019). A Novel Level-Based DNA Security Algorithm Using DNA Codons. *SpringerBriefs in Forensic and Medical Bioinformatics*.
- Raj, B.B, Vijay J.F. & Mahalakshmi, T. (2016). Secure Data Transfer through DNA Cryptography using Symmetric Algorithm. *International Journal of Computer Applications*, 133(2), 19-23.
- Zhang, X., Zhou, Z. & Niu, Y. (2018). An Image Encryption Method Based on the Feistel Network and Dynamic DNA Encoding. *IEEE Photonics Journal*.

# Challenges In Patch Deployment

By | Siti Fatimah Abidin & Nurul Syahirah Aspawi

## Introduction to Patch Management

Patch management is a lifecycle process that includes the activities of identifying, acquiring, deploying, and verifying patches for systems and devices. There are several types of patches such as bug fixes, system feature updates, and security patches. From security point of view, patches are applied to mitigate software flaw and vulnerabilities which can reduce the probability or opportunity of exploitation and introduce new security capabilities. However, there are several challenges in implementing patch management which may lead to compromises that are supposed to be preventable. Study indicates that 60% of breaches in 2019 were due to unapplied patches, which most of them were readily available but not deployed.

## Challenges in Patch Deployment

Patch deployment is a process that involves the deployment of patches or hotfixes that are released from time to time. The process seems like a straightforward activity but in a real world it is a tough implementation. Some of the main challenges in patch deployment include lack of asset control and inventory management. If one organisation has a complete asset list or implemented endpoint manager software, they can keep track of all the system/devices to ensure that the patch deployment process is done efficiently and prevent overlooking issues. Other than that, from this asset list, they can prioritise patch activities to specific type of asset according to the impact and risk, especially when the resources; including people and time, are limited. For example, the systems or devices that have higher attack surface such as web-based system that is opened to public should be prioritised compared to devices located in isolated network.

The second challenge in patch deployment is when there are two different teams; one team that finds the vulnerabilities and the other one that patches the product or systems, and both have their own processes. For example, when there are changes required in the system, the IT

development/operations team must follow their change management process. This process may include reviewing, testing, versioning the system, securing approval from several level of superior, and so on. It may sound tedious, but it is very important to ensure that the patch will not cause any disruption to system functionality or compatibility issues to the existing system's operational environment. It is acceptable if the patch is a routine or a scheduled patch. However, when it concerns publicly-known-exploited-vulnerabilities, such process will delay the critical patch deployment. This scenario happens when there are no collaborative action/process and lack of mutual understanding between both teams. The segregation of work for both teams without a well-planned alliance may cause a delay to the devices/systems that have critical issues despite patch availability.

One other challenge in patch deployment is that different teams may have different KPIs which contradicts each other. For example, the IT teams may want to maintain the availability of their system services according to SLA, but others may prefer to reduce the frequency of system downtime as much as possible. Thus, several patches especially the critical ones, need to be bundled and deployed simultaneously, even though the said critical vulnerability has been flagged earlier by the security team. In this case, the organisation fails to categorise the patch priority according to risk and impact. As such, this will cause an attacker to have a longer window of opportunity for exploitation while waiting for the system to be patched.

Another challenge in patch deployment is when an organisation still uses manual approach in applying patch. Updating a single patch for a single workstation may sound simple, but when it comes to hundreds of workstations, it will be strenuous and labour intensive. When no automation process or patch management software tool are used, deploying patch activity becomes more complicated and takes a longer time to be implemented. Manual method may still be needed for some cases such as system / workstations which have unusual configurations. However, the automated tools will definitely benefit an organization as they ensure the patching process is done effectively. In conclusion, to overcome these challenges,

92

vulnerability management and patch management must be strategized properly. Referring to publicly available patch management guidelines such as NIST will also help an organisation to develop the proper processes and choice of tools, techniques and/or methods for patch deployment activities.

## References

---

1. Souppaya, M., & Scarfone, K. (2013). Guide to enterprise patch management technologies. NIST Special Publication, 800, 40.
2. Shailesh Athalye, 2021, The patch management challenge - why is this still so difficult to achieve? (<https://www.enterprisetimes.co.uk/2021/12/01/the-patch-management-challenge-why-is-this-still-so-difficult-to-achieve/>)



# QR Code: Scan Me Or Scam Me?

By | Yuzida Md Yazid



QR codes are not as safe as you might think

## QR - "Quick Response"

A QR code is an image that is represented by a square with a series of black squares on a white background. Users' mobile devices can scan this image, which typically redirects them to a webpage or download. QR codes have gained popularity in a variety of fields of application due to their high information density and robustness. Despite their numerous advantages, QR codes pose significant security risks. Attackers can encode malicious links that lead to phishing sites (QRishing). QR code usage has increased exponentially during the pandemic, leading many scammers to use it for malicious purposes. It seems as though QR codes are the perfect invention that could deter phishing. There's no need to enter a link and unintentionally misspelling, which may send the user to a fake website designed to look like the real page they intended to visit. Just scan the QR code and you'll be taken to the website you intended to go to. However, as with most new and growing technologies, scammers have found a way to weaponize QR codes as well.

## Can hackers get through a QR code?

Can hackers get through a QR code? Unfortunately, the answer is yes. Hackers have recently latched on the QR code trend and have started using fraudulent and infected codes to directly infect phones and access personal devices.

There are several security risks associated with QR code payments:

1. **Phishing:** Hackers can create a fake QR code that appears to be from a legitimate

merchant, but when scanned, it directs the user to a phishing website that is designed to steal personal information.

2. **Malware:** QR codes can be used to deliver malware to a device by redirecting the user to a website that automatically downloads malware onto the device.
3. **Man-in-the-middle attacks:** The attacker intercepts communication between the user and the merchant's payment system and can change the payment details such as amount or recipient.
4. **Replay Attack:** An attacker can intercept the QR code and use it again to make another transaction.
5. **Lack of security standard:** As QR code payment is relatively new, there isn't a standard security protocol that all merchants must follow.

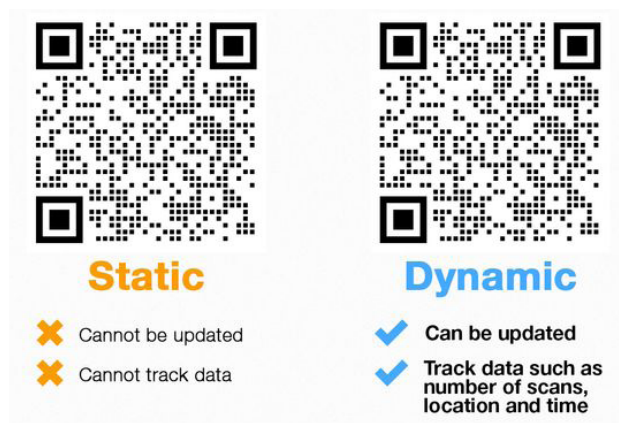
## What makes a QR Code good?

So, how can you stay safe from malicious QR codes while still enjoy the convenience that QR codes provide? The key is to stay alert and watch out for signs if a QR code is not legitimate or has been tampered with. A good QR code should have the following features:

1. **High-resolution:** A good QR code should come in high resolution to ensure that it can be easily scanned and read by QR code readers.
2. **Error correction:** A good QR code should have built-in error correction to ensure that it can still be read even if it is partially damaged or obscured.
3. **Dynamic:** Some QR codes are dynamic, meaning that the encoded information changes with each transaction, making it harder to reuse. This feature is important for security.
4. **Customizable:** A good QR code should be customizable, meaning that it can be branded with a company's logo or colors.
5. **Short URL:** A good QR code url link should be short and easy to read, to avoid any confusion or errors when scanning it.
6. **Encryption:** A good QR code should have

an encryption feature so that the data is protected during transmission, providing an extra layer of security.

7. **Testable:** A good QR code should be testable, meaning it can be scanned and the encoded information verified.
8. **Available in different formats:** A good QR code should be available in different formats, such as static and dynamic, to accommodate different use cases and security needs.



Keep in mind that security should be a top priority when using QR codes, thus a good QR code should have features that can enhance security.

## QRishing

QRishing is a form of phishing attack where hackers exploit QR codes to steal private information, install malicious software on a device, or direct a person to an unsafe website. The purpose of such QRishing scams could range from stealing personal information to clickbait and monetary fraud. This form of phishing is relatively less common than other types of phishing because an attacker would need to invest some effort into distributing the malicious QR code. QRishing works by hiding malicious software or fraudulent websites in the QR code. Users who scan these codes may not immediately recognize the content of the QR code with potentially dangerous consequences. For example, the attacker could place a QR Code in an area dedicated to advertising a product or brand. Once a user falls for the trap and scans the code, he is usually redirected to a fraudulent link, which can aim to trick the user into entering his credentials in order to steal his identity or infect his device with trojans and ransomware.

## Why do people fall for QRishing scams

Curiosity is the biggest motivating factor that leads us to scan QR codes. Each user is led to scan them without fear and consideration about the potential consequences that this could have on their sensitive data, device, or personal computer.

There are several reasons why people fall for QR code phishing scams:

1. **Lack of awareness:** Many people may not be aware of the potential risks associated with scanning QR codes or familiar with the signs of a phishing scam.
2. **Trust in source:** People may trust the source of the QR code, such as a reputable company or brand, and may not suspect that the code could be malicious.
3. **Urgency:** Scammers often create a sense of urgency to get people to quickly scan a QR code, which can prevent people from taking time to verify the legitimacy of the code.
4. **Lack of security measures:** Some people may not have the most updated security measures in place on their devices such as the latest anti-virus or anti-malware software. As a result, it makes them more vulnerable to phishing scams.
5. **Social engineering:** Scammers may use sophisticated tactics such as impersonating a known contact or using a sense of urgency to trick people into scanning a QR code.
6. **Lack of education:** People may not have enough knowledge about QR code, how it works, and the associated risks. This lack of education can make them more susceptible to phishing scams.



It is important to be aware of the potential risks associated with scanning QR codes and to take steps in protecting yourself. Be cautious when scanning QR codes, and only scan codes from trusted sources. Additionally, educate yourself about the signs of a phishing scam and take steps to secure your device.

## QR Code Payment Best Practice

Here are some steps you can take to ensure that your QR code payments are safe:

- Use a secure device: Make sure your device is up-to-date with the latest security updates and good antivirus software installed.
- Only scan QR codes from trusted sources: Be cautious when scanning QR codes, especially if you are unsure of the source.
- Use two-factor authentication: Use a second layer of security such as a fingerprint, password, or a one-time code sent to your phone to confirm the payment.
- Check your account regularly: Keep an eye on your account for any unauthorized transactions and report any suspicious activity immediately.
- Use verified QR code payment app: Use QR code payment apps that are verified and recommended by your bank or financial institution.
- Use QR code with dynamic values: Some payment systems like dynamic QR codes, change with each transaction, making it harder to reuse.
- Be cautious when sharing personal information: Be careful when sharing personal information such as your name, address, or credit card details. Only provide this information to trusted sources.
- Look Carefully: Never Scan a Sticker: Examine the code carefully before scanning. Check for a faint outline surrounding the dotted square. Do not scan if the QR code appears to have been pasted on as a sticker. Never scan any QR code that appears to be a sticker and added after the original document or sign was printed.
- Compare the QR code with others nearby. If the size or design of one or some QR codes is different from most, they may have been tampered with.
- Examine the Link Before You Swipe: Most phones will allow you to approve a QR action before it is completed. Examine the approval page carefully. Does the link's domain name match what you expected to see? Is it the same as the company's official website domain? Is the action being requested what you need to find? If the action is not as expected, cancel the code and do not approve-swipe.
- Don't Scan Random QR Flyers and Stickers: Be selective about which QR codes you scan. Avoid scanning random flyers or stickers that you come across. Be cautious about what you scan.
- Inform a venue if their QR codes have been compromised: If you suspect a business' QR codes have been compromised, please let them know. This can help protect other customers. The business operator will be grateful and you will get a legitimate code to scan the next time you visit.
- If You Suspect Infection, Clean Your Phone: Finally, if you suspect you have scanned a questionable QR code, do have your phone cleaned of malware and infections.

### Remember!

Curiosity often pushes us to take reckless actions, but it is never too late to learn to recognize where dangers, that can undermine our cybersecurity, are hidden! Take note that QR code scanning especially on payment is still a vulnerable technology, so it's important to stay vigilant and cautious to ensure the security of your personal information. QR code security is a new type of personal cybersecurity that we must all be aware of.

### References

1. Krombholz, Katharina, et al. "QR Code Security: A Survey of Attacks and Challenges for Usable Security." Human Aspects of Information Security, Privacy, and Trust, 2014, pp. 79-90. Crossref, [https://doi.org/10.1007/978-3-319-07620-1\\_8](https://doi.org/10.1007/978-3-319-07620-1_8).
2. Vidas, Timothy, et al. "QRishing: The susceptibility of smartphone users to QR code phishing attacks." Financial Cryptography and Data Security: FC 2013 Workshops, USEC and WAHC 2013, Okinawa, Japan, April 1, 2013, Revised Selected Papers 17. Springer Berlin Heidelberg, 2013.
3. QR Codes and Hackers | Pt 1: How QR Codes Get Hacked <https://insureyourcompany.com/blog/qr-codes-and-hackers-pt-1-how-qr-codes-get-hacked/>
4. QR Codes and Hackers | Pt 2: How to Protect Yourself <https://insureyourcompany.com/blog/qr-codes-and-hackers-pt-2-how-to-protect-yourself/>
5. Beware the QR code scams <https://sea.mashable.com/tech/18987/beware-the-qr-code-scams>

# Cloud As A New Media Storage

By | Muhammad Ikhwan bin Mohammad Faisal, Muhammad Anis Farhan bin Yahaya & Muhammad Izwadee Bin Hamzah

Cloud storage is undeniably popular as it is estimated that 95% of IT professionals have adopted cloud storage, according to market researcher Gartner. This trend is definitely here to stay, and it is anticipated to grow even faster. By 2020, 2.3 billion individuals are expected to be using cloud storage, and this figure is expected to increase further. The entire amount spent by end user on cloud services was \$270 billion in 2020. This is projected to rise to a startling US\$332.3 billion in 2021, notching up a 23.1 percent increase. Other industry estimates predict that this amount will reach \$397.5 billion by 2022, and Malaysia is also following the same trend. The question is, why is everyone migrating to this new type of media storage?

We usually store files in our computer's hard drive or another type of external storage medium, such as flash drives or external hard drives. Cloud storage functions by transmitting our files over the Internet and storing them on remote computers that are set up to host them (called servers). What we commonly refer to as "the cloud" is actually a physical server network. We can use an Internet connection to access the data that is stored on these servers. According to Cybercrime Magazine, over 100 zettabytes of data will be stored on the cloud by 2025. To put this in proper perspective, a zettabyte is equal to one billion terabytes (or a trillion gigabytes). Cloud computing is incredibly convenient for both corporate and personal use because all that is needed is an Internet connection. Cloud storage can be thought of simply as having a virtual hard drive that is accessible whenever and anywhere, as needed. One is likely to confuse cloud storage with other kinds of cloud-based technologies as the term "cloud" is frequently used in the digital world.

With cloud storage, we are able to work lot more efficiently. We can access our files remotely from any location via the Internet even in the middle of a desert. The practise of sending large email attachments is quickly becoming obsolete. File uploading is inconvenient and uses a lot of bandwidth and time. You can avoid that by using cloud storage and just send a link instead. The issue of running out of disk space on our computer or mobile device is also addressed

by cloud storage. As files size for videos, programmes, and even operating systems get bigger, your flash solid state drive will be filled up in no time. Cloud storage makes it possible to move files from our hard drive to the cloud to overcome storage space limits. Even though they are not stored on our hard drive, we could still access these files whenever we need to. A broken hard drive can cause the loss of all of our data; which we could avoid with cloud storage. Your files are safe and retrievable even if our hard disk malfunctions. We can save backups of our important files on a remote storage service of our choice, so we don't have to be concerned about local data loss.

By using cloud storage, we will have a secure, yet simple data back-up options. It is incredibly dangerous to keep all of our data on one server. We might lose everything instantly if the server doesn't work for whatever reason. By using Cloud, we are more prepared for any sorts of unknown, unplanned incidents that could corrupt or erase our data, such as natural disasters like floods, fires, or tornadoes or accidental loss of data, including an employee accidentally deleting a critical folder. The majority of the largest cloud service companies have redundancy in place. This means that they make numerous copies of your data and store it across multiple data centres. In this way, you can access your files from a backup server in the event that one server fails. Compared to conventional external backups, which are tied to a single physical place and are exposed to loss or damage, cloud backups offer the necessary redundancy and more effective archiving. Having trustworthy backups helps minimise any downtime and financial losses. Being able to quickly get back online results in fewer frustrated or lost consumers. When data from cloud backups can be retrieved promptly, business continuity is improved as hardware rebuilding and rebooting take less time (as opposed to traditional backup methods like disks, which needs reinstalling everything from scratch, and then testing).

Furthermore, one of the reasons people prefer the cloud to other forms of media storage is that it offers automatic updates. These updates often contain tools designed to protect your devices from the latest viruses or malware. When



we store our data in the cloud, the companies overseeing the servers are consistently updating their security measures so that we need not worry about running an update. A cloud service provider will also regularly update its security measures. Cloud storage is extremely helpful for collaboration. In the cloud, files can be edited simultaneously by multiple users, who can all see the changes as they happen. On the other hand, if we make changes to a file on a desktop, we could only reflect those changes on our own devices. With cloud storage, sharing data with your friends, family, and co-workers become seamless. We can transfer a link to our files, which the recipient can access from another location, using services like Sync.com and One Drive. If we wish to limit who can change the files, we can simply specify permissions, or even password-protect them for more security.

One of the key reasons why people are moving from the old storage media to cloud is to secure against cyberattacks. According to Fortinet, Malaysia recorded a total of 57.8 million virus attacks during the first quarter of 2022, which accounted for 1.14 per cent of the total cyberattacks around the globe. The security of our data when it is kept on a cloud platform is therefore critical. After all, cloud servers where our files, pictures, and movies are kept are outside of our control. You might be concerned about how susceptible these servers are to cyber theft. The data stored with cloud service providers could actually be safer than the data we have saved on our computer's hard disk. The reason is that hackers might be able to access the data stored on own devices via malware and phishing emails. As a result, they could lock up our computer and demand a ransom to unlock our files and data. On the other hand, cloud servers are usually located in warehouses that are not easily accessible to. Secondly, the files stored on cloud servers are encrypted. This means that they are scrambled, which makes it far harder for cybercriminals to access. Artificial intelligence, or AI, is also being used by cloud providers to help safeguard your data due to shortage of qualified security experts. With AI, cloud service providers can at least perform the initial security assessment. These apps use built-in algorithms to look for and pinpoint potential security measure vulnerabilities. Firewalls too are used by cloud providers to protect our files. As the name implies, this technology functions somewhat like a wall to protect our data. All of the traffic entering a network is restricted by restriction criteria applied by firewalls, which can be either hardware or software-based. These regulations are made to block suspicious traffic. As a result, it is more challenging for hackers

to get malware or viruses past the cloud service provider's security procedures.

Cloud-related technology adoption is still relatively new in Malaysia. Malaysia is placed eighth by the Asia Cloud Computing Association (ACCA), after Singapore, which dominates the Asia-Pacific area. Cloud computing requires an initiative to drive the business and develop its implementation. For government's initiatives to be accepted by users, it is crucial to conduct studies on the factors affecting cloud computing readiness and adoption. The Malaysian government introduced MyGovUC, a unified communication and collaboration service that uses cloud computing and overseen by the government. By unifying communications networks across all public sectors in Malaysia, the government is trying to reduce the amount of money spent on data centre. Collaboration and communication between government sectors can be realised in this method, which will benefit the public and more so, the nation. However, an assessment conducted by MyGovUC on the impact of application use revealed certain flaws. These include inconsistent use of applications and a lack of infrastructure that can support some applications which need a lot of bandwidth. In addition, there is a lack of IT expertise as well as number of cloud service providers that disrupt the smooth implementation of cloud services. There are only four major cloud service providers (CSP) in Malaysia namely Amazon Web Services Malaysia Sdn. Bhd., Google Cloud Malaysia Sdn. Bhd., Microsoft (Malaysia) Sdn. Bhd. and Telekom Malaysia Bhd. The government has announced a Cloud Framework Agreement (CFA) with the CSP businesses requiring them to collaborate with identified Managed Service Providers (MSP) to further strengthen MyGovCloud and focus to roll out public cloud services. It is estimated that participation of CSP and MSP firms will result in potential investments between RM12 billion to RM15 billion by 2025

In summary, our nation's ability to utilize technology is attributed to the power of the cloud, which was not readily available 20 or even ten years ago. We can now easily store data remotely and access it from anywhere, ideal for corporations with many locations or employees that work remotely.

Since there are no restrictions on the amount of information stored in the cloud, we can avoid committing too much investment in physical hardware. Eventually, most of the SMEs that joined Cybersecurity Health Check Programme, or so called as (PGPKS), are also using cloud for



98

storing their data. By doing so, the maintenance and security expenses can be reduced and more building space will be freed up, according to Mr. Izwadee Hamzah from CyberSecurity Malaysia. The cloud storage industry is one that is continuously evolving. Because of this, users have access to a wider variety of providers. However, before selecting a cloud service provider, it is crucial to consider not only the above factors but also the precise location and method of data storage, as well as the level of security that will be offered.

## References

---

1. Bourgeios, G. (n.d.). Hubstor. Retrieved from Why Cloud Storage Security is Important: <https://www.hubstor.net/blog/cloud-storage-security-important/#:~:text=Cloud%20storage%20is%20not%20only,a%20considerable%20about%20of%20money>.
2. Gartner Forecasts Worldwide Public Cloud End-User Spending to Grow 23% in 2021. (21 April, 2021). Retrieved from Gartner: <https://www.gartner.com/en/newsroom/press-releases/2021-04-21-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-grow-23-percent-in-2021>
3. Hamzah, E. I. (18 8, 2022). RMK22 - Program Galakan Pemerkasaan Siber kepada Perusahaan Kecil & Sederhana. (Ikhwan, Interviewer)
4. malaymail. (7 June, 2022). Malaysia experienced 57.8 million virus cyber attacks in Q1, says US cybersecurity firm Fortinet. Retrieved from malaymail: <https://www.malaymail.com/news/malaysia/2022/06/07/malaysia-experienced-578-million-virus-cyber-attacks-in-q1-says-us-cybersecurity-firm-fortinet/11070>
5. Mohd Talmizie Amron, R. I. (2019 June , 2019). Acceptance of cloud computing in the Malaysian public sector: A proposed model. pp. 2-3.
6. Rafter, D. (2022). Norton. Retrieved from Cloud Security: How Secure is Cloud Data?: <https://us.norton.com/internetsecurity-privacy-cloud-data-security.html#>
7. Raj, A. (22 May, 2022). Techwire Asia. Retrieved from Malaysia has a new government hybrid cloud service: <https://techwireasia.com/2022/05/theres-a-new-government-hybrid-cloud-service-in-malaysia/>
8. Seagate. (n.d.). Retrieved from What Is Cloud Backup Storage? Benefits and Why Your Business Needs It: <https://www.seagate.com/as/en/blog/what-is-cloud-backup-storage/>
9. Stockon, B. (2022 July , 2022). Cloudwards . Retrieved from How Does Cloud Storage Work? A 2022 Guide for the Uninitiated: <https://www.cloudwards.net/how-cloud-storage-works/>
10. Sumina, V. (7 June, 2022). Cloudwards, Articles. Retrieved from 26 Cloud Computing Statistics, Facts & Trends for 2022: <https://www.cloudwards.net/cloud-computing-statistics/#:~:text=In%202020%2C%20the%20combined%20end,will%20rise%20to%20%24397.5%20billion>.

# Two-Factor Authentication: What Is It And How It Works.

By | Mohammad Zailani Bin Shato, Amieruddin Afiq Bin Rahmat, Mohd Masri bin Abd Kamad, Mohd Azlan Bin Mohd Nor, Nazri Bin Mohamed

## Introduction

Passwords are a vital part of information and network security, serving to protect user accounts. If poorly chosen, the consequences could put an organisation's entire network at risk. Passwords provide the first line of defence against cyber crime. The more unique password are, the more protected data will be from hackers and malicious software.

## Are my passwords not secure enough anymore?

Single passwords are not as secure as they used to be. Hackers can find tons of ways to crack a password, using tactics like password spraying, keylogging or brute force attacks. While strong, complex passwords or passphrases are recommended, they may not always be enough to keep an account secure.



Illustration of the password problem.

## Two-factor authentication: Understanding it

A two-factor authentication (also known as 2FA) is a security system that requires two distinct forms of identification in order to access something.



Combination of 2FA.

2FA can be used to strengthen the security of an online account, a smartphone, or even a door. 2FA does this by requiring two types of information i) the user - a password or personal identification number (PIN), ii) a code sent to the user's smartphone, or a fingerprint - before the secured site can be accessed.



Simplistic diagram of the 2FA process.

2FA also enables businesses and public institutions to be more productive and efficient, allowing employees to perform remote tasks with far less security concerns.

2FA is designed to prevent unauthorized users from accessing accounts based solely on a stolen password. Furthermore, users may be at greater risk of compromised passwords than they realize, particularly if they use the same password on more than one website. Downloading software and clicking on links in emails can also expose an individual to password theft.

2FA combines two of the following:

- Something we know (your password)
- Something we have (such as a text with a code sent to a smartphone or other device, or a smartphone authenticator application)
- Something that we are (biometric using fingerprint, face or retina)

## Why do we need 2FA?

---

2FA is a far more effective way to control access than keeping personal data protected with only a password. If someone hacks into an account that is protected by 2FA, one still needs to know the second access factor, like an SMS verification code or fingerprint.

## How does 2FA work?

---

2FA works by using two unrelated authentication methods to secure an account. The second authentication method usually needs to be verified through a personal possession, such as a phone in addition to the normal username and password.

## Is 2FA actually secure?

---

Yes, 2FA is very secure. Although no login method is completely foolproof, two-factor authentication is much safer against data leaks and hacking attempts. If hackers find that 2FA has been enabled, they will likely move on to another victim, as the potential for success is low.

## Three factors to be addressed

---

2FA is a reliable and effective system for blocking unauthorized access. However, there are still some issues that need to be addressed.

These include:

- i. **Increased login time** – Users need to go one step further to log into an application, which adds time to the login process.
- ii. **Integration** – 2FA usually depends on services or equipment provided by third parties, e.g., a mobile service provider issuing verification code. This creates an out-of-control dependency issue to an external service if a fault occurs.
- iii. **Maintenance** – Ongoing maintenance of a 2FA system could be difficult and if there is a lack of competency in managing requirements and burden of additional cost.

## References

---

1. What Is Two-Factor Authentication (2FA)?, <https://www.investopedia.com/terms/t/twofactor-authentication-2fa.asp>
2. What is two-factor authentication and why is it used?, <https://www.techtarget.com/searchsecurity/definition/two-factor-authentication>
3. Why is password security important, <https://assuredigitaltech.com/news/why-is-password-security-important/>
4. 2FA explained: How to enable it and how it works, <https://www.csoononline.com/article/3239144/2fa-explained-how-to-enable-it-and-how-it-works.html>
5. Two Factor Authentication (2FA) <https://www.imperva.com/learn/application-security/2fa-two-factor-authentication/>

# Kebocoran Maklumat Peribadi Dalam Kalangan Pengguna Internet

By | Ridzwan Ahmad Mohd Fathil

Di era kemajuan teknologi masa kini, pelbagai jenis peranti digital dengan pelbagai fungsi canggih dikeluarkan oleh syarikat pengeluar telekomunikasi. Selain itu, promosi pelbagai pakej telefon pintar bersama data jalur lebar yang menarik turut memberi kesan kepada pertambahan pengguna internet di Malaysia.

Menurut kaji selidik penggunaan dan capaian ICT oleh individu dan isi rumah 2021 yang dikeluarkan oleh Jabatan Perangkaan Malaysia, capaian isi rumah terhadap internet pada tahun 2021 adalah sebanyak 95.5 peratus berbanding 91.7 peratus pada tahun 2020. Pada tahun yang sama juga terdapat peningkatan kepada capaian oleh isi rumah terhadap telefon bimbit dan komputer iaitu sebanyak 99.6 peratus berbanding 88.3 peratus pada tahun sebelumnya.

Peningkatan ini adalah kesan dari penularan pandemik Covid-19 yang melanda negara pada tahun 2020, di mana situasi ini telah memberi ruang kepada lebih ramai pengguna internet untuk kekal berhubung serta melaksanakan pelbagai urusan secara dalam talian seperti bekerja, belajar, berniaga dan sebagainya.

Melihat kepada trend tersebut, pengguna internet kini lebih terdedah kepada pelbagai ancaman dan serangan siber di mana setiap aktiviti yang dilakukan secara dalam talian adalah berisiko termasuk transaksi kewangan bagi tujuan pembelian barangan dan juga perbankan.

Menurut Astro Awani pada 29 Mac 2022, kerugian sebanyak RM2.23 bilion dicatatkan bagi tempoh lima tahun bermula 2017 hingga Jun 2021 akibat jenayah siber di negara ini. Jenayah siber yang direkodkan ini antaranya buli siber, pemalsuan identiti, penggodaman, pancingan data dan penipuan e-mel yang semakin meningkat setiap tahun.

Kes-kes yang melibatkan kebocoran dan penjualan data peribadi juga bukan suatu perkara baharu dan ianya tidak seharusnya dipandang remeh. Isu ketirisan maklumat dan data peribadi masyarakat awam melalui laman sesawang Lembaga Hasil Dalam Negeri (LHDN), kecurian data iPay 88 dan sebagainya

menunjukkan bahawa serangan siber bukan sahaja mampu menggugat data kerajaan malah berupaya memberi kesan dan impak kepada pengguna internet.

Dalam hal ini pengguna internet perlu berhati-hati sewaktu berkongsi maklumat peribadi terutama melalui media sosial. Sikap gemar berkongsi maklumat secara berlebihan berupaya mendedahkan mereka kepada ancaman siber seterusnya menjadi punca kebocoran maklumat peribadi.

Memuat naik informasi dan maklumat seperti nama, tarikh lahir, nombor kad pengenalan dan juga nombor akaun bank secara terbuka di media sosial membolehkan pihak tidak bertanggungjawab mengambil kesempatan menyalahgunakannya. Ada juga yang berkongsi gambar di media sosial tanpa menyedari bahawa maklumat tersebut boleh dilihat secara umum oleh pengguna internet yang lain.

Bagi mengurangkan risiko pendedahan data dan maklumat peribadi, berikut adalah beberapa tips dan amalan terbaik yang boleh membantu pengguna internet menjaga dan melindungi maklumat mereka sekali gus menghindari dari terjerumus menjadi mangsa kepada jenayah siber:

- Pengguna hendaklah sentiasa melihat dengan teliti paparan nama pengirim apabila menyemak kesahihan sesuatu e-mel yang diterima. Sebagai peraturan umum, pengguna tidak seharusnya klik kepada pautan atau memuat turun fail walaupun ianya datang daripada sumber yang kelihatan "boleh dipercayai";
- Pengguna hendaklah sentiasa memerhatikan sebarang kesalahan tata bahasa dan kesalahan ejaan. Syarikat yang sah selalunya menggunakan khidmat penyunting yang berperanan untuk memastikan bahan yang mereka hantar adalah bebas daripada sebarang kesalahan tersebut;
- Aktiviti memancing data direka untuk dihantar secara besar-besaran secara umum. Sebagai contoh "Tuan/Puan yang dihormati, anda telah memenangi sejumlah wang bernilai RM500,000.00". Sekiranya

pengguna mendapati kandungan emel mempunyai ayat yang umum, ia merupakan salah satu cubaan jenayah pancingan data;

- Walaupun tidak semua pengguna internet mempunyai capaian atau menggunakan perisian anti pancingan data, mereka masih boleh menggunakan ciri-ciri yang terdapat pada emel mereka untuk menyekat semua fail dan menapis sebarang emel yang mengandungi kandungan yang tidak sah. Contohnya, pengguna perlu menetapkan e-mel untuk menyekat kandungan sehinggalah disahkan oleh penerima;
- Kebanyakan organisasi tidak akan menghantar emel pengesahan kepada pelanggan mereka melainkan organisasi tersebut ingin menghantar makluman, berita atau iklan;
- Pengguna hendaklah sentiasa berwaspada apabila menerima mesej atau e-mel daripada platform dalam talian. Sebagai contoh, kebanyakan akaun dalam talian seperti KWSP tidak menunjukkan nombor keahlian. Seharusnya pengguna perlu berhati-hati sekiranya mereka menerima e-mel yang mengandungi nombor keahlian palsu yang digunakan oleh penjenayah;
- Jika pengguna merasa sangsi dengan kandungan mesej yang diterima melalui aplikasi WhatsApp, Telegram, e-mel dan sebagainya, maka mesej tersebut perlu disemak terlebih dahulu. Pengguna haruslah berwaspada apabila memberi maklumat peribadi melalui mesej atau e-mel;
- Bagi kejadian yang melibatkan kerugian wang ringgit, orang ramai dinasihatkan supaya melaporkan segera kepada Pusat Pencegahan Jenayah Kewangan Nasional (NSRC) dalam tempoh 24 jam di saluran hotline 997 (Waktu Operasi: 8 pagi - 8 malam).
- Failkan laporan tersebut kepada Jabatan Data Perlindungan Peribadi (JPDP) jika pengguna menerima panggilan sedemikian yang meminta maklumat peribadi mereka di:

Jabatan Data Perlindungan Peribadi  
 Aras 6, Kompleks Kementerian Komunikasi Digital  
 Lot 4G9, Persiaran Perdana, Presint 4  
 Pusat Pentadbiran Kerajaan Persekutuan  
 62100, Putrajaya  
 Telefon : 03 8000 8000  
 Fax : 03 8911 7959  
 Emel : aduan@pdp.gov.my

Dengan perkongsian tips dan amalan terbaik ini diharap ia dapat membantu pengguna internet untuk menjaga maklumat peribadi dan tidak berkongsi dengan mudah agar tidak disalah guna oleh orang yang tidak bertanggungjawab. Isu ini bukan suatu perkara yang perlu dipandang remeh.

Justeru, usaha mencegah harus dilakukan secara berterusan terutamanya oleh pengguna internet itu sendiri selain pihak berkuasa yang melaksanakan pelbagai kempen kesedaran, agar pengguna internet lebih berhati-hati supaya tidak menjadi mangsa kepada jenayah siber seterusnya dapat menjaga kerahsiaan data peribadi.

## Rujukan

1. <https://www.mycert.org.my/portal/advisory?id=MA-893.112022>
2. <https://nfcc.jpm.gov.my/index.php/soalan/mengenainsrc>
3. <https://www.astroawani.com/berita-malaysia/dsa-2022-rm223-bilion-kerugian-direkodkan-akibat-jenayah-siber-ketua-setiausaha-kdn-354169>
4. [https://www.pdp.gov.my/jpdpv2/keratan\\_akhbar/harian-metro-ketirisan-wujud-apabila-integriti-maklumat-tidak-dikawal-selia/?lang=en](https://www.pdp.gov.my/jpdpv2/keratan_akhbar/harian-metro-ketirisan-wujud-apabila-integriti-maklumat-tidak-dikawal-selia/?lang=en)
5. [https://www.dosm.gov.my/v1/uploads/files/5\\_Gallery/2\\_Media/4\\_Stats%40media/4\\_Press\\_Statement/2022/04.%20APRIL/PENGGUNAAN%20DAN%20CAPAIAN%20ICT%20OLEH%20INDIVIDU%20DAN%20ISI%20RUMAH%202021.pdf](https://www.dosm.gov.my/v1/uploads/files/5_Gallery/2_Media/4_Stats%40media/4_Press_Statement/2022/04.%20APRIL/PENGGUNAAN%20DAN%20CAPAIAN%20ICT%20OLEH%20INDIVIDU%20DAN%20ISI%20RUMAH%202021.pdf)



# The Necessity Of Conducting Cyber Security Drills For Organisations

By | Mohammad Fahdzli bin Abdul Rauf

There is one definite outcome from the COVID-19 Pandemic that struck the world during the years 2019 to 2021. The pandemic has fundamentally transformed how people work over the past two years. It shows the importance of digitalization of company operations and infrastructure to accommodate the needs of remote work. Most organisations and companies have embarked on their own digitalization journey, but some have not considered the aspect of cyber security while laying down the framework and planning toward digitalization.

In CyberSecurity Malaysia, we consistently advocate the three most important aspects, or pillars, for a holistic approach towards cyber security implementation. The three pillars are cyber security responsive capabilities, cyber security proactive activities, and people awareness, including capacity building. Cyber security responsive capabilities refer to the readiness to respond to any cyber-attacks in the most effective manner to minimise the impact of any cyber-attacks, while cyber security proactive activities are the actions or steps taken to minimise the risks of cyber incidents from happening in the first place. People awareness and capacity building are the bedrock or foundation for any organization, particularly in cyber security, to ensure that everyone is aware of cyber security in day-to-day situations and that qualified professionals are available to handle all related matters.

In this article we will focus on one key exercise in the first pillar, which is the cyber security responsive capabilities, that is the cyber security drill exercise.

Cyber-attacks in Malaysia have increased dramatically over the past decade. In 2021 alone, CyberSecurity Malaysia has received 10,016 reports on cyber-related incidents<sup>1</sup>. This figure does not include cases that go unreported almost daily. These cyberattacks have leaked sensitive personal and business information, disrupted critical operations, and inflicted immense costs on the economy. Unlike before, today's cybercriminals have the persistence, the technology, and the skills to launch highly successful attacks on

businesses and governments. Their efforts have turned cybercrime into a big global business resulting in valuable private and sensitive data stolen on a massive scale. Daring cyber-attacks on government IT infrastructures in several parts of the world is already a major concern for most countries. The risk will undoubtedly be higher since our government recently launched the Malaysia Digital Economy Blueprint or MyDIGITAL, which outlines the plans to accelerate Malaysia's progress as a technologically advanced economy.

Furthermore, other references also indicate that such cases of cyber-attacks on organisations and businesses have increased recently, in tandem with an acceleration in the digitalization of businesses across Malaysia. An independent survey conducted by Cisco Systems Inc. shows that 50% of small and medium businesses (SMBs) in Malaysia suffered a cyber incident in 2012, and that 67% of Malaysian businesses also lost their customer information to the hands of malicious actors because of these incidents<sup>2</sup>. This will affect consumer perception of your business and it is proven by a recent study published by Forbes Insight which stated that 46% of organisations suffered reputational damage as a result of a data breach and another 19% of organisations suffered reputation and brand damage as a result of a third-party security breach<sup>3</sup>.

Therefore, it is of utmost importance that all organisations (big, small, and medium) be well prepared to handle such cyber incidents when they happen. All organisations should at least have a computer security incident response team (CSIRT), either in-house or through an outsourced arrangement to a third party. A computer security incident response team, or CSIRT, is a group of IT professionals that provides an organisation with services and support surrounding the assessment, management, and prevention of cybersecurity-related emergencies, as well as coordination of incident response efforts.

For a better grasp on the importance of cyber drill let us compare it with another common drill that most of us are aware of, the fire drill.

104

In Malaysia, according to the Fire Services Act 1988 (Act 341)<sup>4</sup>, fire drills for buildings such as libraries, hospitals, hotels, hostels, offices, and government buildings must be held at least once a year. The main objective is to ensure that each occupant of that building is aware of what to do in case of fire to prevent any unnecessary loss of life.

People's lives are invaluable, and thus the need for such regulation is warranted. But what is important too is people's personal data, their personal identifiable information (PII), intellectual property information, key business strategy, and other sensitive data that has been stored digitally in any information technology infrastructure for most organizations. For example, keeping PII private and secure is important to ensure the integrity of your identity. With just a few bits of your personal information, cyber threat perpetrators can create false accounts in your name, start racking up debt, or even create a falsified passport and sell your identity to a criminal<sup>5</sup>.

But having established or outsourced a CSIRT is not enough. This is where the analogy to the fire drill is applicable. Do you know what to do in case of fire, and do you know where to assemble and the safest path to exit your office? With an annual fire drill exercise, everyone will be aware of what to do, and this will minimise the risks and impact of fire on assets and people's lives. Similarly, the objective of a cyber drill is to ensure the readiness and feasibility of an organisation as a whole, and particularly the CSIRT team, to rapidly detect and respond to any real-time cyber incidents. Through this cyber drill exercise, shortcomings in existing policies, procedures, and guidelines can be identified and improved upon further. This drill should be performed at least once a year to ensure that the policies, procedures, and guidelines are still applicable with the current configuration of your IT infrastructure and that the team and the entire organisation are always prepared for any cyber-attacks.

There are two categories of cyber drill exercises, and both are equally important. It is the test of policy adherence and the technical capabilities of the CSIRT team. Each organization's SOP for responding to critical incidents is verified through the policy adherence category. This activity aims to familiarise the participants with the process and prepare them based on their SOP for handling real-life critical cybersecurity incidents in the future. The organisation is

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

The technical assessment category is to appraise the CSIRT performance and technical capability in handling the drill incidents. Upon first identification of an incident, the CSIRT needs to verify and validate the root cause of the incident. Once the cause is found, the CSIRT applies a solution by patching, updating some configurations, etc. to essentially prevent the same cybersecurity incident from hitting the organisation again.

Cyber drill exercises are a necessity to be better equipped to handle real cyber security incidents. Carrying out periodic cyber drill exercises within organisations will ensure that cybersecurity incidents are better addressed and remediated. Cyber drill exercises are also significant as they establish the requirement for proper contingency plans and instill familiarity with relevant policies, procedures, guidelines, and tools to manage incidents.

As the national technical specialist in cyber security, CyberSecurity Malaysia can assist your organisation in providing cyber drill services. We have more than 25 years of experience in managing cyber incidents via MyCERT and experience in collaborating with industry players such as the Securities Commission in conducting sector-wide cyber drills encompassing both categories (policy adherence and technical assessment) for more than 100 capital market organisations (big, medium, and small) from 2017 until 2022.

Other than that, CyberSecurity Malaysia offers various other services to organisations to ensure the security of cyberspace. We can provide the role of facilitator, technical consultant, training, and certifications to stakeholders to address concerns in various facets of the cybersecurity industry and develop action plans to stimulate the growth and development of the local industry. Eventually, this will create opportunities for greater alliances within the local and regional ICT industry to gain a competitive advantage and propel the industry into the future.

## References

---

1. MyCERT Reported Incidents based on General Incident Classification Statistics 2021 <https://www.mycert.org.my/portal/statistics-content?menu=b75e037d-6ee3-4d11-8169-66677d694932&id=77be547e-7a17-444b-9698-8c267427936c>
2. Cisco: 50% of M'sian businesses suffered cyberattacks last year. <https://themalaysianreserve.com/2021/12/02/cisco-50-of-msian-businesses-suffered-cyberattacks-last-year/>
3. The Reputational Impact of IT Risk [https://www.forbes.com/forbesinsights/ibm\\_reputational\\_IT\\_risk/index.html](https://www.forbes.com/forbesinsights/ibm_reputational_IT_risk/index.html)
4. Malaysia Fire Services Act (Act 341) – [https://www.bomba.gov.my/wp-content/uploads/2021/07/Act\\_341\\_Fire\\_services\\_act\\_1988.pdf](https://www.bomba.gov.my/wp-content/uploads/2021/07/Act_341_Fire_services_act_1988.pdf)
5. What is PII and Why Is Protecting It Important? <https://www.shrednations.com/2018/08/what-is-pii-why-protect-it/>

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](mailto:info@cybersecurity.my)

**[www.cybersecurity.my](http://www.cybersecurity.my)**

 @cybersecuritymy

 CyberSecurityMalaysia

 cybersecurity\_malaysia

 CyberSecurityMy

© CyberSecurity Malaysia 2022 – All Rights Reserved



MINISTRY OF  
COMMUNICATIONS AND DIGITAL



ISSN 1985-1995



9 771985 199003