CyberSecurity MALAYSIA

www.cybersecurity.my

eSecurity

The First Line of Digital Defense Begins with Knowledge

Vol 55

Data Protection Officer (DPO): A Critical Role to Safeguard Data Privacy in the Organization

Securing The Future: The Safety and Security of Smart Homes

Overview of Insider Threat in Organization

"The best defense against cyber threats is awareness and preparation". ~ Anonymous

ISSN 1985-1995

9 771985 199003

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

Securing Our Cyberspace

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

For more information, please visit
www.cybersecurity.my

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

Stay connected with us on

- CyberSecurityMalaysia
- CyberSecurity Malaysia
- cybersecuritymy
- cybersecurity_my
- cybersecuritymy

MINISTRY OF DIGITAL

CyberSecurity MALAYSIA

CyberSecurity Malaysia
(726630-U)

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

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

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

WELCOME MESSAGE FROM THE CEO OF CYBERSECURITY MALAYSIA

Dear Esteemed Readers,

Welcome to the latest edition of the e-Security Magazine, where we delve into the rapidly evolving and complex digital landscape. The relentless pace of technological advancement has ushered in a new era brimming with both remarkable opportunities and significant risks. In this ever-changing environment, it is crucial that we remain vigilant in protecting our digital assets and ensuring the security of our interconnected world.

In the following pages, we explore into a wide range of essential topics, from the core principles of project management to the latest advancements in cybersecurity. We explore the intersection of these two disciplines, illustrating how effective project management can serve as a bulwark against cyber threats. Additionally, we highlight the crucial role of the Data Protection Officer (DPO) in protecting sensitive information, emphasizing the importance of data masking and other privacy-enhancing technologies.

Furthermore, we examine the constantly evolving threat landscape, where ransomware, phishing attacks, and insider threats remain significant risks. We discuss strategies to strengthen software development practices and improve online security, empowering individuals and organizations with the tools they need to navigate the digital realm with confidence.

As we look to the future, the security implications of emerging technologies, such as smart homes, mobile devices, and cloud computing, demand our attention. We scrutinize the potential risks posed by advancements in artificial intelligence and blockchain, stressing the importance of vigilance and proactive measures to address emerging vulnerabilities.

In this era of rapid technological advancement, staying informed and adaptable is crucial. By embracing the latest trends, best practices, and emerging technologies, we can better protect our organizations and individuals from cyberattacks. We invite you to dive into the insightful articles and thought-provoking discussions within these pages as we work together to build a more secure digital future.

Finally, test your cybersecurity knowledge with our engaging Cybersecurity Crossword Puzzle! It's a fun and educational way to enhance your understanding.

“Cybersecurity isn’t just about protecting your devices. It’s about protecting yourself.”

Thank you for reading. Be Smart, Be Safe.

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

EDITORIAL BOARD

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

The In's & Out's Of Currency Devaluation

By | Tormizi Bin Kasim, Siti Noriah Nordin, Nur Nadira Mohamad Jafar, Shamsul Hairy Haron & Muhammad Faizal A. Rahman

Definition Of Currency Devaluation

Currency devaluation means a reduction in purchasing power of a domestic currency in comparison to a foreign currency. In other words, devaluation amounts to reduction in the value of a currency with respect to goods or other monetary units with which that currency can be exchanged for. To adjust the balance of payment for a country, the government often reduces the exchange rate of its domestic currency against foreign currency rate. This may apply to the case of special drawing rights enjoyed by international agencies such as The World Bank (WB) or The International Monetary Fund (IMF).

As a result of devaluation, more of the currency is required to purchase the same amount in other currencies. For example: If last year, USD1 could purchase RM5.00 but this year, USD1 can only get RM4.50, then the USD has undergone devaluation.

Objective Of Currency Devaluation

Countries often engage in currency devaluation to gain a comparative advantage in international trade. When they devalue their currency, they make their exports less expensive in foreign markets. Among the objectives of currency devaluation are:-

1. **Promoting Export**
   Currency devaluation leads to better export opportunities. Developing countries could stimulate exports through currency devaluation. However, without adequate foreign exchange, no economy can flourish sustainability.

2. **Discouraging Unnecessary Import**
   Currency devaluation puts a stop to unnecessary imports. Through this process, imports of discretionary consumer items can be curbed successfully.

3. **Adjustment of inter country foreign exchange rates**
   Through currency devaluation, inter-country foreign exchange rates are re-adjusted. Such adjustments could foster better relationships between trading countries.

4. **Increasing domestic employment**
   Currency devaluation creates more opportunity for employment as it stimulates exports and curtails imports. The unemployed can be repositioned to export related jobs and productions that meet domestic demand.

5. **Encouraging foreign capital investment**
   When foreign investors find it cost effective to invest in production facilities due to favourable currency exchange, they will commit a vast amount of investment.

6. **Removal of trade balance deficit**
   Through currency devaluation, higher exports will help address trade balance deficits, especially for developing countries.

Reasons For Currency Devaluation

1. **Overvaluation of Domestic Currency**
   Currency devaluation is usually undertaken when the domestic currency is deemed overvalued relative to other currencies. It may be used as a policy tool to relieve an unfavourable balance of trade or to stimulate fledging export industries. Such policies assume that devaluation will make the country's exports more attractive abroad and in turn, make imports from other countries less attractive at home.

2. **Domestic Economic Policies**
   The value of an item is often tied to its supply or availability. For example, a diamond is rare because only so few are in circulation. The same is true with a currency: when too much of currency is circulated throughout the economy, the currency depreciates. An

increase in the money supply occurs when the US prints more money or the Federal Reserve lowers interest rates. When interest rates are lowered, more people take out loans while the issued money increases the amount of money in circulation. If too much money is in circulation, the economy runs the risk of hyperinflation. Harvard economist and professor Greg Mankiw explains Zimbabwe was a country that experienced a rapid increase in prices due to inflation, but curtailed its rapid monetary expansion by pegging its currency to the U.S. dollar.

3. **Selling currency**
   Investors, financial institutions and central banks often purchase foreign currency. Governments hold large reserves of foreign currency as a safeguard and investment. For instance, the "Wall Street Journal" reports that China owns 2.4 trillion U.S. dollars as a means of steadying the country's local currency, the yuan. When countries or investors grow wary of a currency's stability, they often sell their reserves into the open market. Concern arises when a country is deep in debt, experiencing economic hardship or suffers a terrorist attack or major disaster. Releasing a large amount of any currency to the market causes depreciation in its value.

4. **Existence of Rate Controls and Other Government Exchange Rate Policies**
   Technically, the biggest cause of currency devaluation is rate controls and a government's exchange rate policies. Should these mechanisms not exist, there would still be currency depreciation, but there would never be any organized efforts (even if reluctantly) to allow a currency value to fall. However, in the interests of stability, nearly all nations practice some form of rate intervention from time to time, whether by occasional targeted transactions in the open market or by a strict regime of price controls. Hence, currencies most vulnerable to devaluation are those belonging to nations with uncertain economic prospects coupled with active rate control/support policies.

5. **Currency Crisis**
   Developing countries periodically face a currency crisis in which they may need to consider currency devaluation. This can occur when chronic trade deficits, government budget deficits, or other internal weaknesses cause weakened demand for a nation's currency. This was the case during the Asian financial crisis of the late 1990s.

Benefits / Importance Of Currency Devaluation

1. **Foreign Currency**
   As exports increase and imports fall so foreign currency such as USD, Euro and GBP outflows may fall and inflows rise. This causes the accumulation of foreign exchange reserves for the government and strengthens the economy and increases its viability temporarily.

2. **Decrease in Imports and Increase in Exports**
   Devaluation leads to high import prices leading to a reduction in imports. Conversely, devaluation increases exports due to lower export prices.

3. **Industrial Growth and Economic Development**
   Higher exports lead to industrial growth. Export earnings enable producers to seek improved means of production. As a result, more resources are put into the production process. Incomes, profits, and wages could rise and thus, improve living standards and overall wellbeing of society. It is evident that countries which are net exporters are likely to be rich and. Therefore, exports are key to success and development of any economy. Devaluation not only boosts exports; it can also open doors to long term prosperity, growth, and development.

Danger Of Currency Devaluation

1. **A Risky Undertaking**
   There are factors which may diminish the positive effects of a currency devaluation, making it a risky undertaking. Even if domestic conditions are conducive for it, one country's devaluation may trigger a retaliation of competitive devaluations by other countries and thereby undermining the country's initial strategy.

2. **Aggravating Inflation**
   By increasing the price of imports and stimulating greater demand for domestic products, devaluation can trigger inflation. If this happens, the government may have to raise interest rates to control inflation, but at the cost of slower economic growth.

3. **Dampening Investor Confidence**
   To certain extent devaluation is viewed as a sign of economic weakness, jeopardizing the creditworthiness of an economy. Thus, devaluation may dampen investor confidence and hurt the country's ability to secure foreign investment.

4. **Successive Devaluations**
   One possible consequence is a round of successive devaluations. For instance, trading partners may become concerned that devaluation might negatively affect their own export industries. Neighbouring countries might devalue their own currencies to offset the effects of their trading partner's devaluation. Such policies tend to exacerbate economic difficulties by creating instability in broader financial markets.

5. **Raising the Cost of Imports**
   Due to currency devaluation, banks must raise their key lending rates to guard against a surge in inflation which can be a threat to the economy.

6. **Economic Crisis**
   Devaluation could also affect many companies that have heavy debts denominated in foreign currencies. It can slow the economy with lower growth as concerns mount. Exports may fall sharply and the nation is hit with a budget deficit. The stock market may dip, the trade deficit may rise and bad property loans may bring about crisis to financial institutions.

Impact Of Currency Devaluation On Economy

1. **Role of Exchange Rate Policies**
   Ever since concerted efforts by developing countries to increase their growth rates in the early 1950s, a major source of controversy has been the role which exchange role policy played in conditioning the rate of economic growth. Numerous issues were linked to this approach. Many developing countries' exchange rates were maintained through severe quantitative restrictions which restricted purchases from foreigners well below optimum levels. This in turn led to relatively weak incentives for exports and a marked divergence in domestic prices even inclusive of the tariff charges.
   Some "export pessimists" believe that this did not matter because they regarded import substitution as the only feasible means of rapid growth. Others saw the bias against exports as a major impediment to rapid development. In addition to these issues, "stabilization programs" which included currency devaluation and efforts to curtail the government deficit and the growth of the money supply were highly controversial. Critics alleged that devaluation resulted in more rapid inflation and recession with little or no improvements in the balance of payments.

2. **Stimulation of Merchandise Exports**
   Stimulation of merchandise exports discourages merchandise imports and thus, improves terms of trade, increases revenue collection and savings through the repatriation of profits and royalties by existing foreign investors, bringing illegal foreign exchange leakages into official channels and putting an end to gold smuggling. The inflow of foreign capital can only be improved by devaluation if prices do not rise. It is supposed to provide relief from vexatious import controls that prevent the utilization of full industrial capacity and stifle export drives.

3. **Trade and Payments**
   Currency devaluation promotes exports and thus, results in inflow of short-term capital to the domestic economy.

4. **Trade Terms**
   Currency devaluation changes export-import prices and affects trade terms. This impact generally affects many aspects of the economy and determines the course of prospects or risks.

5. **Wages and Prices**
   Currency devaluation results in price hikes, demand for more pay and wages. As inflation increases, purchasing power decreases, forcing consumer to curtail consumption.

6. **Domestic Income and Allocation of Resources**
   Currency devaluation has a negative effect on income but a positive effect on resource allocation. Both these opposing effects could have significant impact on the economy. It is more so in the economy of a developing country.

7. **Capital Inflow**
   Currency devaluation causes a reduction in

resource value when compared to foreign currencies. It results in an inflow of huge foreign capital to the domestic economy. However, it can also cause a reduction in inflow of long-term capital to the domestic economy.

Summary

In the Short Term

- If the local currency appreciates, it is plausible that exports would decrease as they are less competitive. Thus, if a firm manufactures primarily for exports, an appreciation of the local currency has a negative impact on the company sales. However, if the company imports a large part of its raw materials, it will see the price of its imports decrease. The appreciation of the local currency leads to a decrease in expenses. It is necessary to determine if the impact is greater in income rather than expense.

- If the local currency depreciates, local sales will increase as the manufactured products would become more competitive. However, if the company imports a large part of its products, it will see its prices increase. The depreciation of the local currency leads to an increase in the sales and expenses. Again, it is necessary to determine if the impact is greater on the expenses or the takings.

The primary objective of devaluation is to increase exports and decrease imports. Conversely, a revaluation will lead to a decrease in exports and an increase in imports in the country. This policy is ideal to absorb a deficit or a surplus in the balance of payments. In the mid and long term, this cannot remain as it neglects certain secondary effects from the devaluation.

In the Mid and Long Term

Although a country which devalues its currency is importing less, this does not mean imports are not critical. Due to devaluation, the cost of imported products, notably those of raw materials increases. Companies react to such increase in costs by increasing their prices. This unpredictable effect is more prevalent when the economy of the country in question is small and is not possible for companies to substitute national products for imported ones. This is further reinforced when there is a system of automatic indexing of the salaries in the country, in relation to the general price levels.
A devaluation policy led by a government with a view to reabsorbing a deficit in the balance of payments risks being hit with a price increase unless the government applies strict control policy on prices in which case it will prevent from conserving beneficiary margin.

At the same time, the price of imported critical components decreases. The reduction in production costs enables them to suppress their own prices to safeguard their market share which is momentarily threatened by the imported competing finished products being cheaper.

Conversely, with currency revaluation, entrepreneurs would need to purchase locally produced goods at a higher price. Therefore, they foresee their prices increase while the country which is experiencing a drastic drop in production costs can maintain stable prices. Such stabilizing of national prices ends up offsetting the short term advantages that have been derived from revaluation.

A revaluation policy led by a government with a view to re-absorbing a surplus balance of payments risks being mitigated following a general phenomenon of stabilizing local prices relative to an increase in foreign prices.

Reference

1. Wikipedia, the free encyclopedia. Devaluation. Retrieved 1st May 2011 from http:// en. wikipedia.org/wiki/Devaluation
2. Joshua Curtiss, eHow Contributor. What is currency devaluation? Retrieved 1st May 2011 from http://www.chow.com/about_5295910_currency-devaluation.html
3. Why Do Government Devalue Their Currency Rates? Ratrieved 2nd May 2011 from http://www.currencysolutions.co.uk/currency/why-do-goverments-devalue-their-currency-rates
4. Currency devaluation and Revaluation. Retreived 5th May 2011 from http://www.newyorkfed.org/aboutthefed/fedpoint/fed38.html
5. Devaluation (money). Retreived 7th May 2011 for http://www.referenceforbusiness.com./encyclopedia/Dev-Eco/Devaluation-Money.html
6. https://www.investopedia.com/terms/d/devaluation.asp
7. https://www.wallstreetmojo.com/currency-devaluation/
8. https://www.bound.co/blog/what-does-a-currency-devaluation-cost

Navigating Project Management Challenges: Strategies for Success

By | Azrina Binti Md Saad

Most companies believe that a project's success hinges on ample monetary resources, but in reality, such assumption is grossly misplaced. If money alone could guarantee success, then no multimillion-dollar projects should ever fail. According to a Gartner survey, large IT projects are even more susceptible to failure compared to their smaller counterparts. Surprisingly, functionality issues and significant delays accounted for about half of all project failures, irrespective of size. Moreover, it is worth noting that as the business and project budgets expand, the risk of failure also increases. Project management challenges can manifest across projects of varying scale, duration, and scope.

Project management is an essential framework that ensures specific project objectives and goals are realized. It entails meticulous planning, systematic organization, efficient allocation of resources, and skilled management. By understanding the desired outcomes, devising practical strategies, estimating project duration, fostering collaboration, and ensuring stakeholder alignment, project managers facilitate a seamless execution of tasks and achievement of project objectives.

However, the role of a project manager comes with inherent challenges. It encompasses the responsibilities of initiating, executing, and ultimately delivering a project successfully. According to the 2020 Pulse of the Profession® report, a significant 11.4 percent of investment is wasted due to underperforming projects. This begs the question: What are some of the key factors leading to poor project performance? Prominent factors include communication, unclear project goals and misalignment with business objectives, lack of accountability, scope creep and ever-changing requirements, unrealistic timelines and project schedules, lack of project tracking and monitoring, and poor supplier and vendor management.

Let us now delve into the major challenges often encountered in project management and explore practical tips to overcome them.

1. **Communication**

   Ineffective or poor communication poses one of the most significant risks to any project. As a project manager, how often have you encountered project-related issues caused by “misunderstandings”, “misinterpretations”, or “miscommunication”? It will happen if the project manager does not correctly delegate tasks, provide or clarify roles and responsibilities or "who is doing what." In that case, this will cause enormous confusion among all the stakeholders.

   It is therefore crucial to implement an effective communication plan. A well-crafted communication plan acts as a robust framework, providing project teams with governance systems and clearly outlining the communication methods to be used, such as emails, meetings, phone calls, memos, and more. This plan ensures that specific areas, issues, and milestones are communicated efficiently and effectively throughout the project life cycle.

   Consider a scenario where there is a change in the project's planning, scope, or cost. In such cases, it becomes imperative for the project manager to circulate a change management notice to the project team. The project manager can determine the most effective way to disseminate this crucial information by referring to the communication plan. Additionally, adopting and implementing project management software can greatly assist in keeping project team members and stakeholders up to date while simultaneously increasing transparency. Such software also provides a centralized platform for all project-related correspondence, discussions, and feedback, streamlining communication processes for tasks and milestones.

2. **Unclear project goals and misalignment with business objectives**

   One prevalent project management challenge arises from the lack of clearly defined project goals and alignment with the business, primarily due to inadequate

planning. Companies often neglect to invest sufficient time and resources in planning projects and ensuring coherence with the overarching business strategy and roadmap. Ineffective planning frequently results in unclear project goals and a lack of alignment with the business objectives. To address this, organizations must allocate adequate resources to comprehensive planning and ensure seamless integration of project objectives with the broader business strategy. It is crucial for companies to devote ample time and effort to meticulous planning, emphasizing the connection between project milestones and the overarching business objectives. Poor planning contributes to the common project management challenge of lack of clarity regarding project goals and misalignment with the business. Organizations should therefore prioritize project planning, establish a clear and well-communicated set of goals, and regularly review their alignment with the overall business objectives. By dedicating sufficient time and resources to effective planning, companies can overcome the challenge of unclear project goals and misalignment with the business.

1. **Lack of Accountability**

   Accountability holds significant importance in project execution as each team member contributes to the project's successful outcome. The absence of accountability can negatively impact a project with a cascading impact. Typically, a project kick-off meeting precedes the project's initiation, where the project manager must effectively communicate the roles, responsibilities, and progress communication methods to all team members and stakeholders. The completion of tasks relies on the timely completion of preceding tasks, necessitating clear communication between responsible individuals. The project team comprises of individuals with diverse skill sets, work habits, specialties, and personalities. Successful collaboration on the project necessitates each team member to fulfill their assigned responsibilities and maintain effective communication

2. **Scope creep and changing requirements**

   It is essential to follow a strategy in addressing scope creep and changing requirements. Firstly, conduct a comprehensive scope definition and requirements gathering at the onset of a project. This will ensure a clearer understanding of project boundaries and client expectations. Secondly, establish a change management process that allows for evaluation and effective incorporation of changes. By implementing a structured approach to change, you can assess the impact, feasibility, and risks associated with each requested modification. Thirdly, communicate changes promptly and effectively to the project team and stakeholders. Transparent and timely communication is crucial in maintaining alignment and managing expectations throughout the project. This will help stakeholders understand the rationale behind changes and their potential impact on the project's scope, timeline, and budget.

3. **Unrealistic timelines and project schedules**

   Unrealistic timelines and project schedules refer to setting or committing to project deadlines that are difficult or impossible to achieve within the given resources, constraints, and scope. This can happen for various reasons, such as inadequate planning, inaccurate estimation, external pressures, or an overly optimistic outlook.

   To address the issue of unrealistic timelines and project schedules, several strategies can be implemented. First and foremost, conduct realistic project planning and estimation by considering various factors such as available resources, complexity, and potential risks. Secondly, involve relevant stakeholders in setting project timelines to gain valuable insights and ensure a more accurate project duration assessment. Regular review and adjustment of project schedules are also essential to cater for unforeseen circumstances or changes in project requirements. Additionally, prompt communication of any changes or delays to stakeholders is crucial to manage expectations and maintain transparency throughout the project lifecycle. By implementing these solutions, project managers can improve the likelihood of achieving realistic timelines and schedules that are aligned with project goals and stakeholder needs.

4. **Lack of project tracking and monitoring**

   To overcome the challenge of inadequate project tracking and monitoring, consider implementing several methods. Firstly, establish a robust project tracking system that systematically monitors progress, milestones, and deliverables throughout

the project lifecycle. This includes defining clear metrics and key performance indicators (KPIs) to measure project success. Secondly, ensure regular project status updates and progress reporting to keep all stakeholders informed about the project's current status and any potential issues or risks. This facilitates transparency and enables timely decision-making. Lastly, leverage project management tools and software that offer efficient tracking and monitoring capabilities, thereby allowing real-time visibility into project activities, task assignments, and timelines. By adopting these solutions, project managers can enhance their ability to track and monitor project progress effectively, mitigate risks, and make data-driven decisions for successful project outcomes.

5. Supplier and Vendor Management

Supplier and vendor management plays a pivotal role in a project's success. Challenges in managing suppliers, such as delays, quality issues, or performance monitoring, can significantly impact project timelines and outcomes. However, by establishing effective supplier management practices, organizations can mitigate risks associated with external partners and ensure smooth project execution.

Managing suppliers and vendors can be complex due to the potential for delays, where suppliers or vendors may face obstacles that impede their ability to deliver materials, equipment, or services on time, causing disruptions to project schedules. Mitigating the impact of unexpected delays can be achieved by maintaining contingency plans and alternative supplier options to ensure a smooth flow of materials, equipment, or services.

Another challenge in supplier and vendor management is quality issues, which can result in defects, rework, or unsatisfactory project outcomes due to the provision of poor-quality materials, equipment, or services. Defining quality requirements and expectations in supplier contracts is therefore crucial to tackling this challenge. Conducting thorough due diligence and supplier assessments can help identify reliable partners before engagement. Regular monitoring and evaluation of the quality of supplied goods or services is necessary to ensure adherence to project standards. Establishing feedback channels and fostering collaboration with suppliers enables prompt addressing of any quality concerns that may arise.

A critical aspect of supplier and vendor management is performance monitoring. Failing to monitor and evaluate supplier performance can result in underperformance, missed milestones, or a failure to meet quality standards. To address this challenge, organizations should implement performance monitoring mechanisms. This can be achieved by establishing key performance indicators (KPIs) and conducting regular performance reviews. Metrics should be defined to measure aspects such as on-time delivery, quality, responsiveness, and adherence to contractual obligations. Based on performance evaluations, organizations provide feedback to suppliers and collaborate with them to address any identified shortcomings or areas for improvement.

Executing a project comes with numerous obstacles. However, the above mentioned challenges provide a glimpse into some of the critical areas that project managers commonly encounter.

In conclusion, project management challenges are common obstacles that most project managers often face. From communication issues and inadequate goal alignment to scope creep, unrealistic timelines, and a lack of project tracking, can threaten success and hinder organizational growth. Nevertheless, they can be addressed by implementing effective strategies and best practices.

It is crucial for project managers to prioritize clear and efficient communication, both within the project team and stakeholders. Project managers can enhance collaboration, ensure transparency, and minimize misunderstanding by developing a comprehensive communication plan, utilizing appropriate communication methods, and leveraging project management software.

Proper project planning can also address inadequate goal alignment and scope creep, including thorough scope definition and requirements gathering. By engaging with relevant stakeholders, conducting realistic project estimations, and implementing change management processes, project managers have the means to establish a solid foundation for goal attainment and scope control.

Accurate timelines and project schedules require realistic planning, regular schedule reviews, and effective communication of any changes or delays to stakeholders. By setting achievable deadlines, involving stakeholders in the planning process, and utilizing project management tools, project managers can better manage project timelines and mitigate associated risks.

Lack of project tracking and monitoring can be adressed by establishing robust tracking systems, regular progress reporting, and using project management tools for efficient tracking and visibility. Project managers must ensure project success by monitoring project progress, identifying bottlenecks, and making data-driven decisions.

Finally, effective supplier and vendor management is vital for a project's success. Organizations can enhance project outcomes by addressing challenges related to delays, quality, contracts, communication, and performance. Engaging in proactive supplier and vendor management mitigates potential risks and nurtures enduring partnerships that prioritize trust and collaboration. By prioritizing supplier management practices, organizations can ensure smooth project execution and drive successful project outcomes.

In summary, while project management challenges may seem daunting, they can be effectively addressed through proactive planning, clear communication, stakeholder involvement, and the utilization of appropriate tools and strategies. By adopting these approaches, project managers can navigate challenges, enhance project performance, and achieve successful project outcomes.

References

1. https://cmoe.com/blog/navigating-the-challenges-of-project-management/
2. https://teamdeck.io/project-management/project-management-challenges/
3. https://studyonline.rmit.edu.au/what-are-the-challenges-in-project-management
4. https://www.jmest.org/wp-content/uploads/JMESTN42351894.pdf
5. https://www.academia.edu/6676836/Challenges_faced_by_the_Project_Managers_in_IT_industry
6. https://kissflow.com/project/project-management-challenges/
7. https://www.proofhub.com/articles/project-management-challenges
8. https://www.indeed.com/career-advice/career-development/challenges-in-project

Komunikasi Krisis Di Era Teknologi Digital

By | Mohd Shamil Mohd Yusoff

Evolusi teknologi dan Internet yang dinamik membawa banyak kemudahan dan manfaat dalam kehidupan masa kini. Namun penggunaan teknologi serta kebergantungan terhadap Internet turut mendedahkan organisasi dan pengguna individu kepada pelbagai risiko ancaman serta serangan siber.

Menurut Statista's Key Market Indicators (KMI), pada tahun 2022 terdapat 29.5 juta pengguna Internet di Malaysia dan dianggarkan akan meningkat kepada 32 juta menjelang tahun 2028(1). Pertambahan ini menjadikan rakyat Malaysia tidak terkecuali dari terdedah kepada ancaman dan serangan siber. Ini kerana penjenayah siber sentiasa mencari peluang dan mengambil kesempatan dengan mengeksploitasi kemajuan teknologi yang sama untuk meningkatkan keupayaan mereka.

Natijahnya wujud pelbagai ancaman dan serangan siber seperti penipuan dalam talian, ketirisan data, ancaman dalaman, serangan perisian berniat jahat, penggodaman, manakala terdapat juga unsur-unsur penyalahgunaan internet seperti penyebaran berita palsu, fitnah, buli siber, kecurian identiti dan lain-lain. Situasi ini menyebabkan berlakunya krisis digital yang berupaya menggugat kestabilan, merencat pembangunan sehingga membobrok kesejahteraan sesebuah negara.

Pada tahun 2022, Polis Diraja Malaysia (PDRM) merekodkan 19,034 kes serangan siber dengan nilai kerugian RM593 juta. Manakala, laporan Ancaman Siber 2022 SonicWall pula mencatatkan jumlah serangan siber global seperti Malware sebanyak 5.5 bilion, Malware IoT - 112.3 milion, Percubaan Pencerobohan - 6.3 trillion, Ransomware 493 milion (2). Apa yang pasti setiap serangan siber yang berlaku akan menimbulkan krisis digital.

Krisis Digital

Individu atau organisasi berisiko untuk berdepan dengan krisis kerana sesuatu insiden berupaya untuk terserak dengan pantas merentasi platform media sosial. Dalam situasi tertentu ia mungkin menjadi sukar untuk dikawal sehingga mewujudkan krisis digital.

Krisis digital berlaku secara dalam talian apabila terdapat ancaman dan serangan siber seperti pencerobohan ke atas sistem rangkaian di sesebuah organisasi atau kerenah pekerja yang menabur fitnah tentang syarikat melalui platform media sosial. Krisis digital juga berlaku di luar talian apabila sesuatu insiden tular dan dibincangkan secara meluas di platform digital seperti isu skandal melibatkan selebriti atau figura awam, wabak penyakit, insiden bencana alam seperti banjir, tanah runtuh dan sebagainya. Sesebuah organisasi berisiko mengalami kerugian besar akibat krisis digital.

Mengurus Komunikasi Krisis Digital

Sesuatu krisis yang berlaku perlu diurus secara strategik dan sistematik. Apabila mengurus krisis digital, sesebuah organisasi perlu bertindak secara profesional serta telus mengenai krisis yang dihadapi. Mengurus komunikasi krisis digital memerlukan sesebuah organisasi membuat analisis insiden yang berlaku, bekerjasama dengan pasukan krisis yang ditubuh khas, mempertimbangkan pihak berkepentingan dalaman dan luaran, bersikap membantu dan empati selain perlu berhati-hati dengan komunikasi selepas krisis.

Organisasi yang memahami evolusi teknologi dan kepentingan mengurus krisis digital akan sentiasa bersedia untuk menghadapi sebarang insiden dan sentiasa berusaha meningkatkan tahap bersiapsiagaan mereka dengan mengikuti program latihan serta mewujudkan Pelan Komunikasi Krisis.

Pelan Komunikasi Krisis

Perancangan komunikasi sewaktu krisis adalah sangat penting kerana ia berupaya mengubah persepsi serta mengelak dari berlaku perkara di luar jangka, mengenalpasti kaedah untuk bertindak balas dengan pantas, membawa ketenteraman, mengelak kekeliruan serta dapat memberi gambaran dan penjelasan mengenai insiden yang berlaku.

Setiap organisasi seharusnya mempunyai Pelan Komunikasi Krisis (Crisis Communication Plan) bagi melancarkan tata kelola serta tadbir urus sesuatu insiden selain mengenalpasti bentuk tindakan yang perlu diambil terutamanya bagi menangani serta mencegah insiden yang sama dari berulang di masa hadapan. Tanpa perancangan mengurus krisis, sesuatu insiden berpotensi untuk menghadapi suasana luar jangka yang memberi impak kepada operasi organisasi, meluntur keyakinan pemegang taruh serta pelanggan selain meninggalkan kesan negatif kepada imej dan mencemar reputasi.

Sememangnya sukar untuk organisasi akui bahawa mereka menghadapi krisis atau menjadi mangsa serangan siber malah ada yang menyembunyikan perkara tersebut kerana dibimbangi akan memberi kesan ke atas perniagaan. Dalam hal ini, organisasi tidak seharusnya berdiam tanpa mengambil sebarang tindakan terhadap krisis yang dialami. Mereka perlu telus dari aspek pengurusan krisis kerana melalui pengurusan krisis secara strategik, ia dapat meyakinkan pemegang taruh serta pelanggan mengenai keupayaan organisasi selain memberi jaminan bahawa organisasi akan terus beroperasi selain menguatkan lagi kedudukan jenama dan reputasi organisasi.

Pengurusan Komunikasi Krisis

Dalam konteks CyberSecurity Malaysia, pengurusan krisis merangkumi aktiviti pemantauan media yang dilaksanakan secara berterusan merentasi saluran media konvensional (TV, radio, akhbar, majalah) dan juga media baharu (platform media dalam talian). Tujuan ia dilakukan adalah untuk memantau, melihat dan mengumpul liputan berita, peristiwa atau insiden semasa berkaitan keselamatan siber termasuk sentimen (positif dan negatif) selain untuk mendapatkan nilai PR liputan media yang diperolehi.

Sekiranya berlaku krisis, aktiviti pemantauan media menjadi fokus utama untuk melihat sejauh mana sebaran berita mengenai krisis tersebut kepada umum. Informasi dari pemantauan media dijadikan rujukan serta panduan untuk mengurus sesuatu krisis, menyepadukan kaedah atau tatacara untuk bertindak balas segera bagi memastikan imej dan reputasi terjamin, membangunkan mesej utama untuk penyediaan input terhadap apa jua pertanyaan media, mengenal pasti sasaran bagi mesej dikongsi serta menjadi sumber kepada pembangunan kaedah atau tatacara menangani isu terlibat agar dapat ditangani di masa akan datang.

Pasukan pengurusan krisis yang turut dianggotai oleh pasukan komunikasi krisis turut memainkan peranan penting dalam mengawal saluran komunikasi dan menyediakan input mengenai insiden yang berlaku, menyokong dari aspek membina keyakinan kepada pihak pengurusan untuk berhadapan dengan pemegang taruh serta membantu memaklumkan kepada kakitangan agar mereka memahami isu atau krisis yang berlaku. Integrasi dalam bertindak balas segera sangat penting bagi tujuan pemulihan serta untuk terus kekal beroperasi semasa dan selepas krisis.

Sementara itu, pasukan pengurusan komunikasi krisis menggalas tugas menyediakan siaran media atau kenyataan media, kemaskini laman web serta media sosial mengenalpasti lokasi termasuk urusan logistik sidang media sekiranya perlu, mengkoordinasi pengurusan media seterusnya melaksanakan sidang media atau edaran kenyataan media selain membuat pemantauan media. Kesemua proses mengurus krisis komunikasi di CyberSecurity Malaysia dibuat berasaskan satu Prosidur Komunikasi Krisis atau Crisis Communications Procedure yang dikemaskini dari masa ke semasa.

Kesimpulan

Di era globalisasi masa kini, krisis digital berlaku dan tersebar dengan amat pantas melalui internet. Situasi ini menimbulkan cabaran baharu bagi sesebuah organisasi untuk menghadapinya. Justeru, kita harus memastikan usaha dan tindakan segera secara berkolaborasi perlu dilaksanakan untuk satu tindak balas secara efektif diambil yang berupaya mengekalkan pengoperasian serta mengekalkan reputasi sesebuah organisasi.

Rujukan

1. https://www.statista.com/statistics/553752/number-of-internet-users-in-malaysia/
2. https://www.sonicwall.com/2023-cyber-threat-report/

ICT Security in Technology Roadmap, Is It a Must?

By | Aiman Aizzat Mohd Yusof, Nor Radziah Jusoh, Mohd Azlan Mohd Nor & Nazri Mohamed

Deconstructing a Technology Roadmap

Before we delve into what a **Technology Roadmap** is all about, let us first understand the definition of a Roadmap. Figure 1.0 below shows an example of an AI Roadmap by MOSTI.

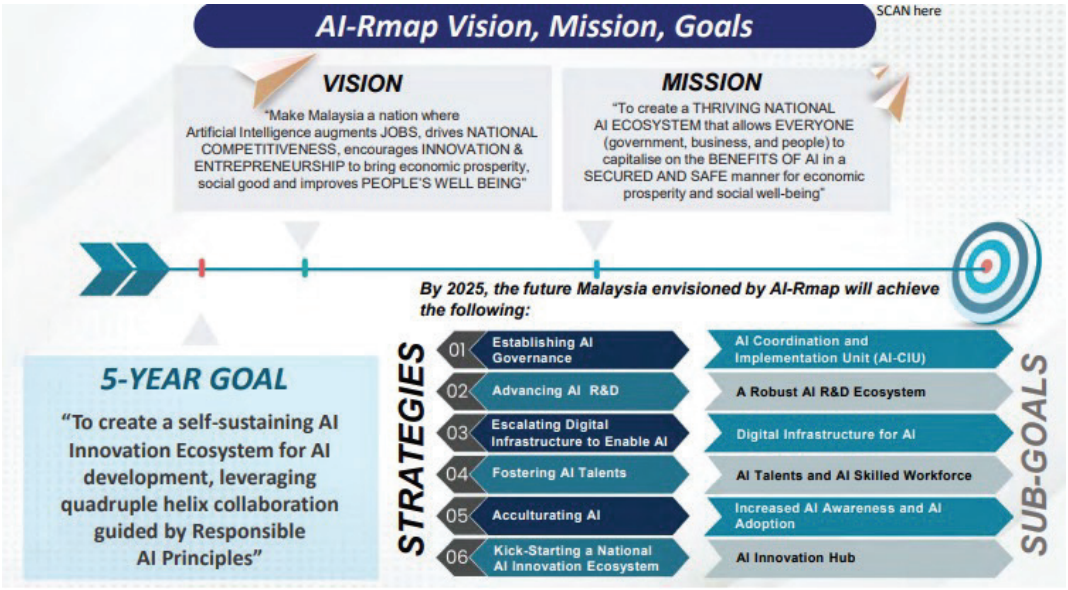


Figure 1.0

Malaysia National Artificial Intelligence Roadmap 2021 - 2025

Simply put, a **Roadmap** is a visual representation of a strategy. The purpose of a roadmap is to ensure everyone in an organization has a common understanding and acts in concert.

A **Technology Roadmap** outlines the long-term strategy of an organization's technology infrastructure. A resource material titled 'Industry 4.0: Managing the Digital Transformation' written by Alp Ustundag and Emre Cevikcan quoted: **"Technology Road mapping is an important method that has become integral to creating and delivering strategy and innovation in many organizations."** It consists of a display or a diagram that shows an organization's technology strategy and its technology adoption plan. The purpose of a Technology Roadmap is to guide the Information Technology (IT) department in making strategic decisions about investments in technology, upgrades, and maintenance regarding its technological infrastructure. However, the illustrated roadmap must be within the organization's budget and realistic in nature. Technology Roadmap plays a significant role in today's business as it outlines what an organization needs in terms of technology to achieve their short-term plans and long-term goals.

Why is it important to have a 'Technology Roadmap'?

A journey consists of a path and a destination. Without any of these two, we are not going to get anywhere. The same applies to a technology roadmap. Without a technology roadmap, everyone in the organization will be in the dark about the direction taken by IT department. Research written by Peiman Alipour Sarvari, Alp Ustundag, Emre Cevikcan, Ihsan Kaya and Selcuk Cebi further validates the importance of a Technology Roadmap, stating that **"In order to achieve success in the digital transformation process, it is necessary to prepare the technology roadmap in the most accurate way".**

However, constructing an accurate technology roadmap without any corresponding security implementations would be very detrimental. Without secure cyber protection, any technology would be rendered useless.

One example of a security feature being implemented in a technology is the use of TAC authentication in online banking. A TAC number is an authentication code received via SMS and used by banks to verify its users through Two-Factor Authentication (2FA). Maybank2u, CIMB Clicks, myBSN and many more online banking sites use Two-Factor Authentication. Currently, most of them have opted to use more advanced authentication method. As technology improves further, the security features become more complex.

These days, banks use SecureTAC that features enhanced encryption that is embedded into its mobile application. This security feature authenticates a user before any online transaction is done. It is an improvement from TAC authentication received particularly for mobile application —both from speed and safety standpoints. A bank will regularly review and update its security measures to ensure the safety and security of its customers' financial transactions and data.

Imagine without any direction or reference, financial institutions might have lost millions if they are forced to rectify security breach on the spot.

Benefits of Security Features in Technology Road Mapping

There are several benefits of incorporating key security features in a Technology Roadmap. These include the following:

Data Protection: With the implementation of encryption, access controls, and secure communication protocols, technology solutions can ensure the confidentiality and integrity of data. Security features will also help safeguard sensitive data, both for businesses and individuals.

Business Continuity: Security features ensure business continuity by reducing interruptions caused by security events. Organisations can sustain operations and prevent costly downtime by recognising possible threats and vulnerabilities early on and executing suitable responses.

Cost Saving: While adopting security features incurs certain initial expenses, it can realize long-term cost savings. Organisations can minimise financial losses associated with data breaches, legal lawsuits, and reputational harm by preventing security incidents.

Key to a successful Technology Roadmap

Against a backdrop of escalating need for data privacy and cybersecurity, it is essential to include security features in a technology roadmap. Apart from planning and determining which technology to adopt into an organization's infrastructure, security should also be taken into consideration during the planning stage for a good roadmap. One misstep could cost a fortune to an organization. Without incorporating proper security features, the technology roadmap could end up being a very expensive exercise for the organization.

First and foremost, it is important for an IT department to assess the current state of its organization's security stance by identifying vulnerabilities that exist in the infrastructure as well as analyzing areas that require improvement. By doing so, it will help determine an organization's security needs and the necessary security features to be included in its technology roadmap.

The next step is to identify and prioritize the

security features that will be incorporated into the technology roadmap. Essential security features that satisfy the pillar of Triad Information Security like the **C(onfidentiality), I(ntegrity) A(vailablity)** must be considered early on. This includes access control, authentication, encryption, backup and recovery, monitoring and other security features. These features will help ensure the security and confidentiality of data and protect the organization against cyber-attacks.

Once the security features have been implemented, the final step is to consistently monitor and evaluate the competency and efficiency of the implemented security features in the technology roadmap. By doing this, any weaknesses or gaps in the infrastructure can be identified early, enabling the IT department to patch up and take action before more damage is done.

Conclusion

In conclusion, security features in a technology roadmap provide numerous benefits, including data protection, risk mitigation, compliance, reputation enhancement, business continuity, competitive advantage, improved user experience, cost savings, and scalability. By prioritizing security, organizations can create robust and trusted technology solutions that meet the needs of users and stakeholders.

Implementing security features in a technology roadmap is essential to protecting an organization's data and infrastructure from cyber-attacks, as well as avoiding big financial losses. IT departments must ensure that the technology roadmap is aligned with the overall organizational goals and objectives. It also needs to provide the necessary security to protect against cyber threats. Last but not least, regular monitoring and evaluation will help ensure that the security features are effective and up-to-date

References

1. https://airmap.my/
2. https://roadmunk.com/guides/roadmap-definition/
3. https://www.lucidchart.com/blog/what-is-a-technology-roadmap
4. https://cisoshare.com/blog/building-security-program-roadmap/
5. https://www.dnv.com/article/the-three-pillar-approach-to-cyber-security-data-and-information-protection-165683#:~:text=The%20CIA%20triad%20refers%20to,fundamental%20objective%20of%20information%20security.
6. https://www.researchgate.net/profile/Emre-Cevikcan/publication/322172971_Industry_40_Managing_The_Digital_Transformation/links/5ce7cd1da6fdccc9ddca7e86/Industry-40-Managing-The-Digital-Transformation.pdf

Secure Shopping: Ensuring Online Safety in the World of E-Commerce

By | Dania Syahirah Zakry, Fatin Nabila Anuar & Siti Nur Fatihah

The growth of e-commerce has revolutionized the retail industry, reshaping the way businesses and consumers operate. With just a few clicks, consumers can browse countless options and purchase from the comfort of their homes and have products delivered right to their doorstep. Meanwhile, businesses can reduce overhead costs associated with physical stores, reach a more extensive customer base, and gather valuable data on consumer behaviour. E-commerce has also significantly transformed the retail sector and opened up opportunities with lower barriers of entry for small businesses and entrepreneurs to enter the market. Today, e-commerce has become an inseparable part of people's daily lives, offering convenience and accessibility. However, knowing the potential risks associated with online shopping is essential.

Online Shopping Risks

Although there are numerous advantages to online shopping such as ease of communication between businesses and consumers, there are cyber security risks that must be considered, such as identity theft. Identity theft is obtaining another person's personal or financial information to commit fraud, such as making unauthorized purchases or transactions online. For example, when buying something via an online or e-commerce system, you must fill in your personal information to proceed with delivery. The personal information you enter when buying online is accessible by anyone. As such, hackers will take this opportunity to steal your information such as name, address, date of birth, social security number, credit card information, and information about your checking account, for their own purpose. There are two methods used by cybercriminals to steal individuals' identities, namely technology-based and social engineering. Typically, technology-based identity theft involves cybercriminals breaking into e-commerce websites and stealing login or credit card information from customers who are users of the system. Meanwhile, social engineering identity theft involves psychological manipulation to trick users into committing security breaches or divulging their private information.

In addition, users also can be tricked into using fake applications or websites. Generally, retailers or brands provide dedicated applications or websites for consumers. Cybercriminals sometimes mimic the brands by creating a fake application version or website URL. For smartphone users, it is risky to download an application through an unofficial application store or link as the said link might be a fake version that cybercriminals created to harvest personal information such as username, password, bank, and credit card details. Conversely, users could also run a risk of being infected by viruses on their devices. These days, many brands sell products through e-commerce platforms such as Shopee and Lazada. Although there is an official brand account on such e-commerce platforms, cybercriminals still create fake accounts to trick users into buying from them instead. They will pretend to sell the same original products as the brand, but in reality are fake items. Cybercriminals also create fake reviews to scam consumers. Reviews which seem too good to be true require further research.

Another common threat of online shopping is phishing attack. Phishing is a technique used by cybercriminals to trick individuals into providing sensitive information, such as passwords or credit card details, by disguising themselves as a trustworthy entity. This involves scammers sending fake emails which appear to be from a genuine retailer. The emails usually contain an attachment, or a link designed to trick the receiver into clicking so that cybercriminals can launch a malware infection or hacking. Clicking on these malicious elements can initiate download and installation of malware onto the user's device. Once infected, the malware can steal sensitive information like credit card details, login credentials, and personal data, posing a severe threat to an individual's privacy and financial security.

Online Shopping Guide to Protect Yourself Against Cyber Crime

1. Use A Dedicated Email Address for Online Shopping

Although a human can only have one fixed identity associated with them, such identity can be manifested across multiple email addresses, accounts, credentials, and passwords. Hence, to secure your identity, creating alternative personal email addresses is advisable. It is recommended to create one dedicated email address for online shopping. This will help lessen the chance of opening emails that are harmful. For instance, if you use a dedicated email for Lazada but also receive a message from Lazada in your primary email account advising you of a problem with an order of your Lazada account, you will realize that the message is most likely fake or malicious and was sent by cybercriminals.

2. Manage And Protect Your Online Password

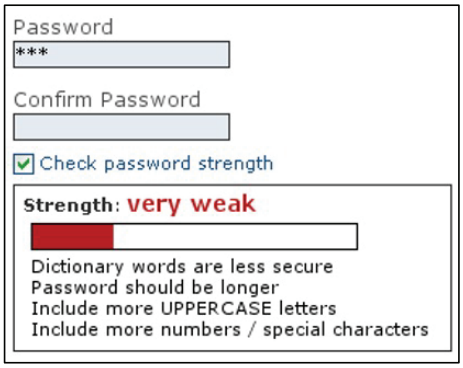


Figure 1: Create a strong password for the online shopping platform

It is advisable to use different passwords for different online shopping platforms. Also, ensure a unique and strong password is used for online shopping. A minimum of twelve characters, combined with upper and lower cases, numbers, and symbols, make up a strong password. Additionally, one should avoid revealing information related to you that is obvious or well-known, such as your birth date or family member's name. This helps to reduce the chances of cybercriminals guessing your login password and doing illegal activities using your account.

3. Check SSL Certificate and URL

Figure 2: URL with SSL certificate

SSL stands for 'Secure Sockets Layer' and indicates that an e-commerce website is secured for shopping. Websites that ask for sensitive or personal information, such as credit card details and addresses, should have SSL certificates. To check that an online shopping website has an up-to-date SSL certificate, look for a padlock icon in the URL bar of your web browser, or check that the URL starts with HTTPS, not HTTP. Next, as a good online shopper, you should always consider the URL you visit. Ensure that the website's spelling is correct with no additional characters.

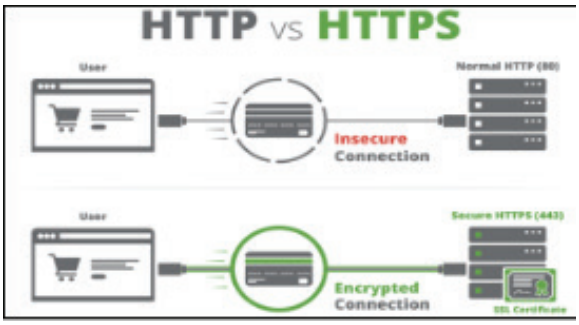


Figure 3: The comparison function between HTTP and HTTPS when dealing with financial transactions on an e-commerce website

4. Avoid Using Public Wi-Fi

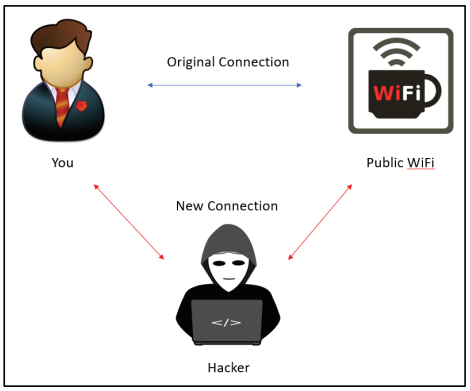


Figure 4: A hacker intercepts the Internet connection to steal the session

Most public areas, such as coffee shops, restaurants, and hotels, offer free Wi-Fi to customers. This enables them to perform online tasks such as checking email and browsing the Internet. Uninformed users may be tricked into believing that a malicious Wi-Fi hotspot is a secure connection. Hackers will use public Wi-Fi to track you, steal your password and personal data, or even take control of your online shopping accounts. The user may unwittingly join a cybercriminal's network without knowing that the hacker now has access to everything you do on your laptop or mobile device. In other words, the hacker will get the username and password if you enter an online merchant or banking account. Phishing attacks can be easily targeted at those who are unaware of security precautions when using free Wi-Fi.

5. Use Secure Payment Gateway

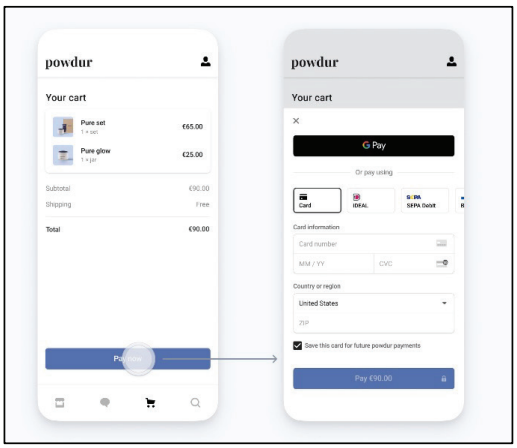


Figure 5: A secure payment gateway from Stripe

Since data breaches have become more rampant and terrifying than ever, users should use a secure, trusted payment gateway platform. A transaction on a shopping website should always start with "HTTPS." This shows that communication is encrypted between your device and the shopping site. Additionally, you might want to reconsider keeping your credit card information and other confidential information on your online store accounts because, in case of a data breach, your information might fall into the hands of cybercriminals. Next, never share your payment information, such as your TAC number, with anyone else. Be suspicious when someone asks for your payment information. Always keep an eye on your account and bank account activity. If you see any charges to the bank account you do not recognize, contact the bank immediately to block the card. Following and adhering to the steps can help keep your payment information safe while using a payment request link.

Conclusion

With the advancement of technology and increasing popularity of online shopping, e-commerce platforms have become convenient for consumers to purchase goods and services. However, this convenience also comes with potential risks of cybercrime. As a consumer, we always need to be aware of the possibility of cybercrime when using an e-commerce platform and always practise safe online shopping.

References

1. https://talwork.net/how-strong-is-your-password
2. https://www.myhostingbubble.com/blog/wp-content/uploads/2017/05/letse.png
3. https://www.cloudways.com/blog/wp-content/uploads/HTTP-vs-HTTPS-1.png
4. https://stripe.com/docs/payments/accept-a-payment?platform=android&ui=payment-sheet

Project Management Frameworks: PMBOK & PRINCE2

By | Nur Athirah Abdullah, Atikah Baharudin & Ahmad Hisyamudin Salleh

Introduction

A project is a unique, transient enterprise that is set up to achieve defined objectives, outputs, outcomes, or benefits. A project is usually deemed to be a success if it achieves the objectives according to its acceptance criteria, within an agreed timescale and budget. Organizations typically utilize perspective of project management for either internal operations or projects engagement. At times, these two may overlap. A project can be defined in terms of its distinctive characteristics — it is a temporary endeavor undertaken to create a unique product or service. Temporary in a way that every project has a definite duration. Operations, however entails ongoing, routine activities undertaken as part of an organization's primary business. They follow organizational procedures to produce consistent result and are permanent in nature. Nevertheless, despite the differences in meaning, operations and projects still share some common characteristics; namely:

- Performed by people.
- Constrained by limited resources.
- Planned, executed, and controlled.

Projects are often undertaken at all levels of an organization. They may involve a single person or hundreds and even thousands. Some may require less time to complete or over a long term horizon. Projects may involve a single unit of one organization or could cut cross organizational boundaries such as joint ventures and partnership. Projects are often critical components of an organization's business strategy performance. Examples of projects include:

- Developing a new product or service
- Effecting a change in the structure, staffing, or style of an organization
- Designing a new transportation vehicle
- Developing or acquiring a new or modified information system
- Constructing a building or facility
- Running a campaign for political office
- Implementing a new business procedure or process

Project management entails application of knowledge, skills, tools, and techniques to manage project activities in order to meet or exceed stakeholder needs and expectations. This invariably involves balancing competing demands among:

- Scope, time, cost, and quality.
- Stakeholders with differing needs and expectations.
- Identified requirements (needs) and unidentified requirements (expectations).

The term project management is also sometimes used to describe an organizational approach to the management of ongoing operations. This approach, more properly called management by projects, treats many aspects of ongoing operations as projects in order to apply project management. Although an understanding of project management is obviously critical to an organization, a detailed discussion of the approach itself is outside the scope of this paper.

Knowledge about project management can be organized in many ways. Effective and successful project management ensures that risks are identified at an early stage and managed appropriately, while objectives and benefits are achieved within budget, time and to the required quality. It gives staff and managers control over their project, ensuring that everyone involved in a project knows what is expected of them, and provides an appropriate level of reporting chain.

This paper aims to study two different project management approaches, namely PMBOK (Project management Body of Knowledge) and PRINCE2. Both have their own pros and cons and identity, depending on what kind of project one is working on. MySEF leverages hybrid approaches, incorporating both the PMBOK and PRINCE2 methodologies as needed. The PMBOK framework enables MySEF to adhere to best practices and effectively manage project processes and knowledge areas within the Common Criteria (CC) lab environment. Meanwhile, PRINCE2 provides a structured methodology throughout a project lifecycle, ensuring transparent processes and principles are followed. By combining the strengths of

both approaches, MySEF maintains flexibility while implementing a systematic and controlled approach to its CC lab operations, ensuring efficient project management and compliance with industry standards.

Summary Of Key Findings

PMBOK provides a framework of important guidelines, rules, and characteristics of projects spanning all industries. Through the acceptance and constant application of PMBOK standards, an organization is assured of achieving professional excellence. The principles framed in PMBOK guide can also be used to manage projects across multiple industry verticals. PMBOK serves to promote and establish a common vocabulary for the project management profession by prescribing tools and techniques for each process and defining inputs and outputs as well. It describes the basic concepts of Project, Project Management, the Role of the Project Manager in different organizational structures, Project Management Phases, and the Project Lifecycle.

The guide provides a comprehensive approach to balancing project constraints. PMBOK can be summarized as an approach that provides information on what a project manager needs to know whereas PRINCE2 methodology demonstrates how to apply this knowledge in a structured and consistent manner. PRINCE2's principles are guiding doctrines which must be followed by all projects. It is considered a "constitution" for which all projects must abide by its philosophies. While PMBOK discusses the importance of defining roles and responsibilities in a project, PRINCE2 provides a model on how to set up a project team and standard role descriptions suitable for each project type. Overall, PMBOK is essentially a guide and a collection of good project management principles, techniques and guidelines that help manage projects. PRINCE2 is a methodology on roles, responsibilities, and deliverables.

Analysis Of Review

Created by the Project Management Institute (PMI), PMBOK stands for Project Management Body of Knowledge, which breaks down project management into five phases: conception and initiation, planning, execution, performance and monitoring, and closing. It follows a "waterfall" or cascading methodology through phases from start to finish. PMBOK is considered a direct 'competitor' to PRINCE2 because of the strengtheners. PMBOK applies universal standards to its waterfall method and is a very thorough approach in managing large-scale projects. It can also be helpful for large enterprises that want all departments, or even companies, to work in one standardized way, using the same vocabulary and best practices. Users of PMBOK find that it has more substantial frameworks for contract management, scope management and other aspects which are arguably less robust in PRINCE2. However, many users of PMBOK find that they are not entirely satisfied with the way the system limits decision-making solely to project managers, making it difficult for handing over aspects of the management to other parties and senior managers. With PMBOK, the project manager is invariably the primary decision maker, planner, problem solver, human resource manager and much more. In contrast to PMBOK, PRINCE2 is a project management program that shares more functional and financial authority with senior management, not just the project manager. This program focuses more on aiding a project manager to oversee projects on behalf of an organization's senior management. On a positive side, PRINCE2 provides a single standard approach to managing projects, which is why many governments and global organizations prefer this option. It is also favoured because of its ease of use, which makes it easy to learn, even for those with limited experience. However, on the downside, there are users who feel that PRINCE2 neglects the importance of soft skills that a project manager should focus on. Like the waterfall method, PRINCE2 is a very rigid and highly controlled methodology. It is not the right fit for small projects or smaller teams or agencies, who do not have time or resources to go through a lengthy certification course. Below are knowledge areas and principles that are applied by these two frameworks:

Knowledge Areas	Principle
PMBOK	PRINCE2
· Project Integration Management · Project Scope Management · Project Time Management · Project Cost Management · Project Quality Management · Project Human Resource Management · Project Communication Management · Project Risk Management · Project Procurement Management · Project Stakeholder Management	· Continued Business Justification · Learn from Experience · Defined Roles and Responsibilities · Manage by Stages · Manage by Exception · Focus on Products · Tailor to Suit the Project

Discussion On The Reviews

In conclusion, there is no one-size-fits-all method. What will work for any organization really depends on their industry, workload, and personal preferences. But there are a few questions we can ask ourselves that might be helpful:

- Is my project complex or is it relatively straightforward?
- Do I work in a flexible, dynamic environment like a startup?
- Am I open to taking risks?
- Am I willing to let the workflow change or evolve?
- If working with clients, what are they like? How do they work best?

Some project management methodologies will immediately yield result (either positively or negatively), but others will require experimentation and time to see what works best. In summary, a skilled project manager is one who can apply the right project management methodology based on knowledge areas. For example, those of PMBOK with the aid of a structured methodology such as PRINCE2. A highly skilled project manager should also have the 'know-how' to apply project management controls that are appropriate to the scale, complexity and nature of a project. Each of these has its distinct differences. If a project manager needs to be the sole decision maker, then PMBOK could be the preferred method. However, if the project manager wants to follow a methodology comprehensively, then PRINCE2 is a better choice because it acts as a guide rather than a methodology like PMBOK. Still, each project manager will form different opinions and may even interchange both methodologies based on nature of each project.

To achieve optimal results in project management, a project manager can consider combining both methods.

References

1. AMO. (2017, November 24). Agile Management Office AMO. Retrieved from What is Agile, PMBOK and PRINCE2?: https://agilemanagementoffice.com/what-is-agile-pmbok-and-prince2/
2. Bangor University. (2017). Project Management Framework. North Wales, UK: Bangor University. Retrieved from https://www.bangor.ac.uk/cpb/documents/Project%20Management%20Framework%20v2%20March%202017.pdf
3. Binder, L. (2018). Monday Blog. Retrieved from The top project management methodologies: Which is right for you?: https://monday.com/blog/top-project-management-methodologies/#pmbok
4. Buehring, S. (2019, May 17). Knowledge Train. Retrieved from PRINCE2® vs the PMBOK® Guide: A comparison: https://www.knowledgetrain.co.uk/project-and-programme-management/pmi/prince2-and-pmbok-guide-comparison
5. CIO. (2011). PMBOK vs PRINCE2 vs Agile project management. Retrieved from CIO From IDG: https://www.cio.com.au/article/402347/pmbok_vs_prince2_vs_agile_project_management/
6. Hartney, J. (2018, October 29). Project Engineer. Retrieved from The 7 Principles of PRINCE2: https://www.projectengineer.net/the-7-principles-of-prince2/
7. HiLogic. (2019). Retrieved from PRINCE2 & PROJECT MANAGEMENT PROFESSIONAL (PMBOK) COMPARISON: https://www.hilogic.com.my/prince2-pmp-pmbok-comparison/
8. Project Management Institute. (2017). Job Growth and Talent Gap 2017-2027. Retrieved from Project Management Institute: https://www.pmi.org/-/media/pmi/documents/public/pdf/learning/job-growth-report.pdf

9. Radujković, M., & Sjekavica, M. (2017). Project Management Success Factors. Procedia Engineering, 607-615. doi:10.1016/j.proeng.2017.08.048
10. Support of Project Management Methods by Project Management Information System. (2015). Procedia - Social and Behavioral Sciences, 96-104. doi:10.1016/j.sbspro.2015.11.333
11. Swanberg, K. (2015, January 5). HubSpot. Retrieved from The 12 Basic Principles of Agile Project Management: https://blog.hubspot.com/agency/basic-principles-agile-project-management
12. Tripathi, A. (2019, June 11). SimpliLearn. Retrieved from PMBOK® - A Guide to Project Management Body of Knowledge: https://www.simplilearn.com/pmbok-a-guide-to-project-management-body-of-knowledge-rar73-article
13. Watt, B., & Watt, A. (2017). Framework for Project Management. Retrieved from Open Text BC: https://opentextbc.ca/projectmanagement/chapter/chapter-4-framework-for-project-management-project-management/

Ketagihan Media Sosial dan Impak ke atas Kesihatan Mental

By | Redy Jeffry bin Mohamad Ramli

Sewaktu majlis anugerah British Academy Film Awards (BAFTA) yang berlangsung pada 15 Mei 2023, pelakon Kate Winslet yang memenangi anugerah Pelakon Wanita Terbaik melalui lakonannya dalam siri mini "I Am Ruth" dalam ucapan kemenangannya menggesa pihak yang mempunyai kuasa untuk melakukan perubahan dengan mengambil tindakan undang-undang ke atas mereka yang membuat atau menyediakan kandungan yang boleh menyebabkan orang lain (pengguna) merasa terancam.

Menurut Kate;
"To people in power and to people who can make change: please, criminalise harmful content. Please eradicate harmful content. We don't want it. We want our children back." (1)

Siri mini 'I Am Ruth' yang antara lain berkisar tentang dilema ibu bapa yang sukar berkomunikasi dengan anak-anak mereka yang mengalami ketagihan dengan media sosial. Kate menggesa agar generasi muda yang ketagihan media sosial dan apa jua sisi gelap dunia dalam talian agar berubah kerana kehidupan bukanlah semata-mata tentang media sosial.

Gesaan Kate itu adalah rentetan daripada isu ketagihan media sosial yang sedang melanda United Kingdom (UK) yang sudah mencapai tahap serius sehingga kumpulan pengamal undang-undang mengesa kerajaan UK menambah baik 'Online Safety Bill' yang antara lain mewajibkan firma teknologi menghalang kandungan yang mengancam daripada muncul atau disiarkan dalam platfom mereka.

Sisi Baik Media Sosial

Hari ini, media sosial telah menjadi sebahagian yang penting dalam kehidupan seharian manusia di seluruh dunia. Tidak dinafikan bahawa banyak kebaikan yang telah dinikmati oleh manusia dengan wujudnya media sosial, antaranya;

1. Merevolusikan platform berkomunikasi, berkongsi dan berhubung dengan orang lain bukan sahaja hanya di sekitar kita malah di seluruh pelusuk dunia.
2. Perkongsian idea, maklumat dan luahan perasaan menjadi lebih terbuka.
3. Pencarian maklumat mudah dan pantas dilakukan kerana ia boleh diakses dengan mudah melalui pelbagai peranti teknologi khasnya telefon pintar yang sebelum ini terhad kepada teknologi komputer.
4. Media sosial adalah sebahagian daripada elemen penting tuntutan pekerjaan mahupun peribadi sehinggakan tanpa media sosial, kerja mahupun urusan peribadi boleh terganggu.

Sisi Gelap Media Sosial

Banyak lagi sisi baik media sosial boleh disenaraikan malah impak positif media sosial berbeza bagi setiap individu yang menggunakannya, namun seperti juga setiap sesuatu ada sisi baik dan buruknya, begitu jugalah dengan media sosial yang tidak terlepas daripada kesan negatifnya. Berikut adalah antara sisi gelap media sosial yang lumrah dialami oleh hampir kebanyakan masyarakat di dunia:

1. Sukar menjauhkan diri daripada media sosial walaupun sesaat kerana sudah terjerumus dalam ketagihan digital tanpa individu itu sedari mereka dalam ketagihan.
2. Ketagihan digital ini antaranya termasuklah terhadap media sosial, permainan dalam talian, judi dalam talian dan pornografi.
3. Bercakap tentang ketagihan media sosial, ia antara lain berlaku kerana dorongan untuk tidak mahu ketinggalan dalam isu terkini terutama yang membabitkan hal-hal hiburan dan suka ramai yang tular dalam media sosial, meskipun maklumat itu antaranya tidak memberi manfaat khasnya hal-hal yang membabitkan fitnah atau berita palsu.
4. Berlumba-lumba untuk menjadi orang pertama yang membuat komen atau mengulas sesuatu isu sehingga sulit untuk individu berkenaan berenggang dengan media sosial.

5. Akibat terlalu berlumba-lumba untuk menjadi orang pertama yang tahu hal-hal terkini, maka wujud tekanan 'rakan media sosial' yang menyebabkan individu itu sendiri dalam tekanan untuk sentiasa nampak 'baik dan terbaik' pada pandangan pengguna media sosial lain.

6. Akhirnya 'penagih media sosial' akan sentiasa dalam kebimbangan dan tekanan semasa menggunakan media sosial kerana perlu sentiasa mencapai piawaian penerimaan yang terlalu tinggi oleh pengguna media sosial lain.

7. Akibat terlalu ingin memenuhi penerimaan orang lain, maka harga diri mula menerima kesan kerana individu berkenaan mula merasa rendah diri apabila tidak dapat memenuhi harapan orang lain.

8. Selain itu, pola tidur dan kualiti tidur mula terjejas kerana terlalu banyak menghabiskan masa dengan media sosial, malah bukan itu saja, individu tersebut juga akhirnya mungkin akan mengalami gangguan tidur atau insomnia.

9. Akibat paling buruk ketagihan digital ialah runtuhnya institusi kekeluargaan jika yang menjadi penagih digital itu sama ada ibu bapa atau dalam kalangan anak-anak. Bukan sedikit cerita tentang rumah tangga porak peranda, bercerai berai dan anak-anak terbiar akibat daripada ketagihan digital seperti judi dalam talian dan pornografi.

Impak terhadap Kesihatan Mental

Senarai di atas hanyalah sebahagian daripada kesan negatif ketagihan media sosial dan salah satu impak ketagihan media sosial atau ketagihan digital secara amnya ialah terjejasnya kesihatan mental individu berkenaan tanpa disedari.

Apa pula yang dimaksudkan dengan kesihatan mental? Kesihatan mental adalah satu keadaan yang sejahtera dimana seseorang individu menyedari tentang keupayaan diri, dapat mengendalikan tekanan dengan baik, dapat bekerja secara produktif dan mampu menyumbang kepada masyarakat.

Ini bermaksud, kesihatan mental adalah asas kepada kesejahteraan individu dan kemampuan masyarakat berfungsi secara efektif. Kesihatan mental adalah ekspresi emosi dan melambangkan keupayaan untuk menyesuaikan diri dalam pelbagai tekanan dan tuntutan hidup. (2)

Oleh yang demikian, bolehlah kita ketegorikan masalah ketagihan media sosial sebagai penyumbang kepada masalah kesihatan mental kerana kesan negatif daripada ketagihan media sosial itu menepati ciri-ciri kesihatan mental yang terjejas.

Keselamatan Ketika Di Dunia Digital Terancam

Bercakap tentang kesan negatif media sosial, sesungguhnya kita sebenarnya sedang membicarakan tentang keselamatan pengguna itu secara tidak langsung apatah lagi apabila kesannya telah menjejaskan kesihatan mental.

Apabila penggunaan media sosial itu telah meninggalkan kesan yang negatif kepada penggunanya, bermakna keselamatannya secara langsung sudah terancam atau terjejas, maka sesuatu perlu dilakukan untuk memastikan keselamatannya itu kembali terjamin.

Mengembalikan Jaminan Keselamatan Siber

Jadi apakah yang perlu diambil oleh 'penagih media sosial' untuk mengembalikan jaminan keselamatan sebagai seorang pengguna media sosial.

Hadkan Masa Penggunaan Media Sosial
Bagi mendisplinkan diri untuk mengehadkan masa menggunakan media sosial bukanlah sesuatu yang mudah apatah jika sudah bergelar 'penagih media sosial'. Namun apabila menyedari bahawa anda sudah menjadi 'penagih media sosial' dan sedar akan kesihatan mental anda terjejas, maka perlu kesungguhan dan keazaman yang tinggi untuk menjauhkan diri daripada media sosial sekerap yang mungkin.

Malah kini terdapat perisisan yang percuma atau murah yang boleh digunakan untuk mengehadkan penggunaan media sosial yang boleh dipasang pada telefon pintar anak-anak.

Guna Media Sosial Untuk Keperluan Sahaja
Jika hendak menggunakan media sosial, memadai ia digunakan untuk keperluan penting sahaja seperti untuk mendapatkan maklumat, urusan perbankan dan kewangan, pembelian dalam talian dan hal yang berkaitan dengan kerja.

Libatkan Diri Dalam Hal-hal Berfaedah Luar Talian

Kurangkan kebergantungan dengan media sosial, sebaliknya tumpukan lebih banyak masa dengan perkara-perkara luar talian seperti mengikuti ceramah atau kuliah agama, beriktikaf di masjid, hobi, aktiviti sukan dan rekreasi, berkebun mahupun bertukang, asalkan yang dilakukan itu bermanfaat dan memang kena dengan jiwa anda.

Dapatkan Bantuan Profesional

Salah satu punca yang menjerumuskan individu bermasalah kepada jurang kebinasaan ialah apabila individu berkenaan cuba menyelesaikan masalah tersebut tanpa bantuan daripada pakar.

Kesihatan mental bukanlah masalah kecil yang mudah ditangani tanpa bantuan pakar kerana silap cara untuk mengatasinya boleh menyebabkan kesihatan mental bertambah teruk. Oleh yang demikian, dapatkanlah bantuan daripada mereka yang berkelayakan untuk memulihkan kesihatan mental anda.

Perlu dijelaskan di sini bahawa isu ketagihan media sosial sehingga menjejaskan kesihatan mental tidak akan selesai atau terubat hanya dengan membaca artikel sebegini atau merujuk 'rakan media sosial', mencari jawapan melalui "Google" atau kini melalui aplikasi Kepintaran Buatan (AI) sebaliknya hal yang paling utama perlu dilakukan oleh 'penagih media sosial' ialah berjumpa dengan pakar yang lebih arif tentang kesihatan mental.

Apabila ‘penagih media sosial’ sudah mengambil langkah-langkah yang disebutkan di atas atau apa jua langkah-langkah lain yang bersesuaian untuk memulihkan kesihatan mentalnya, maka usaha tersebut adalah sebahagian daripada langkah untuk mengembalikan jaminan keselamatan yang terjejas.

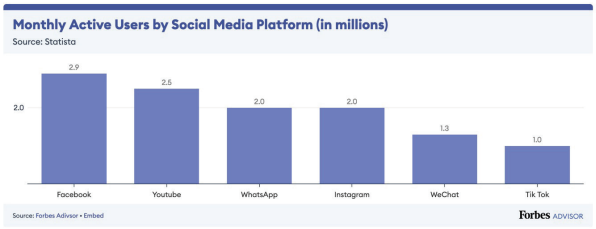
Dengan adanya jaminan keselamatan seperti tidak mudah terpengaruh dengan komen atau pandangan orang lain, sabar dan tidak melulu ketika membalas atau mengulas isu-isu dalam media sosial, tidak terikut dengan kehendak atau harapan ‘rakan media sosial’ serta sentiasa mengehadkan penggunaan media sosial atau aplikasi dalam talian yang lain untuk keperluan sahaja, tidak mustahil ‘penagih media sosial’ boleh pulih dan mampu berhadapan semula dengan media sosial secara lebih baik, berhemah dan matang.

Rujukan

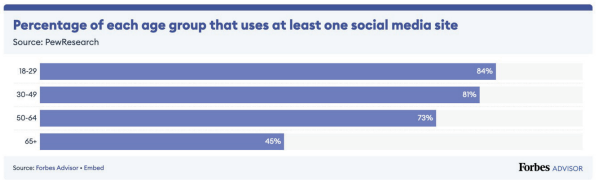
1. Kate Winslet calls for action against harmful social media content in impassioned speech https://www.sbs.com.au/news/article/kate-winslet-calls-for-harmful-social-media-content-to-be-eradicated/k9cwfvot2
2. Definis Kesihatan Mental https://care.upm.edu.my/artikel/definisi_kesihatan_mental-56729

Statistik Media Sosial 2023

- Dianggarkan 4.9 bilion manusia menggunakan media sosial di seluruh dunia setakat 2023
- Jumlah tersebut dijangka menikat kepada 5.85 bilion menjelang 2027
- Facebook merupakan media sosial paling berpengaruh dengan pengguna aktif berjumlah 2.9 juta diikuti oleh Youtube dengan 2.5 juta pengguna.



- Akses utama pengguna media sosial di seluruh dunia ialah melalui peranti mudah alih sama ada telefon pintar atau tablet.
- Nigeria merupakan negara yang paling ramai pengguna yang mengakses media sosial
- 84% individu berusia antara 18 hingga 29 tahun mengunakan sekurang-kurangnya sati media sosial



Sumber: https://www.forbes.com/advisor/business/social-media-statistics/

Securing The Future: The Safety And Security Of Smart Homes

By | Madihah Zulfa Mohamad & Nur Hidayah Hasnol

Introduction

Smart home technology has revolutionised the way people manage their homes, allowing them to do everything from turning on lights and regulating ambient temperature to watching security cameras and activating locks (Shah et al., 2020). Smart home systems and appliances, which form part of Internet of Things (IoT), often communicate with one another, sharing data and automating activities in accordance to preferences set by the homeowner. The smart home concept was introduced back in 1975 with the creation of X10, a platform for home automation that could transmit digital information over radio frequency pulse via a homes' electrical wiring system (Sundar et al., 2006).

According to a recent article **"Top 35 Smart Home Facts and Statistics (2023),"** there will be 478.2 million smart homes worldwide by 2025. The rapid surge in popularity of smart homes in recent years can be attributed to its remarkable ability to remotely automate and regulate our living spaces effortlessly. However, contrary to popular belief convenience comes at the expense of security and safety. This article explores the advantages of smart homes, the dangers they may pose, and the safety precautions that should be implemented.

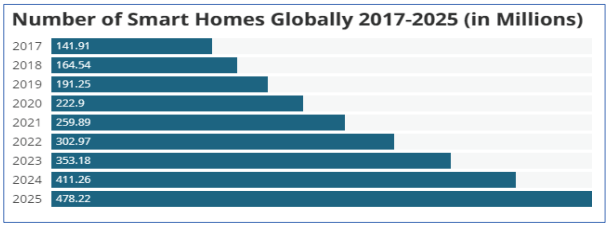


Figure 1: Number of Smart Homes Globally 2017-2025 (in Millions)
Source: Top 35 Smart Home Facts and Statistics (2023)

Benefits of Smart Home

There are numerous advantages with smart homes, such as creating simplicity in home living, increasing energy efficiency, and enhancing security (Sovacool et al., 2020). One can manage many aspects of a house by using smart home technologies from just about anywhere in the world. For instance, you can use your smartphone or tablet to control door locks, light switches, and even the thermostat from a far. Such convenience could improve the quality of life while saving time.

Moreover, smart homes are designed to be energy efficient. Lower energy costs can be achieved, for instance, by using smart thermostats that can track and follow your preferences, daily pattern and change the temperature intuitively. Similarly, smart lightning system could turn off lights in an empty room and thus, save energy.

A smart home system can also enhance security. Homeowners can have peace of mind by remotely monitoring their home through cameras and activating door locks when necessary. Some smart home systems can also identify irregular activities and notify homeowners or security firms. In fact, there are security systems which records suspicious movements and relay to the homeowners for review.

Figure 2: Smart house technology concept with centralized control.
Source: The Advantages of a Smart House

Risks of Smart Homes

While smart homes powered by Internet of Things (IoT) devices can provide convenience, they may nevertheless pose risks and dangers due to connectivity (Geneiatakis et al., 2017). Identity theft is one of the most serious threats linked to smart homes, which can occur if criminals gain access to personal information via unsecured IoT devices. Another issue is the potential release of private data, which may endanger the security and privacy of people and

their families. Additionally, smart homes can track a person's movement and location which will be unsettling for those who value privacy.

1. **Identity theft**
   Smart homes which are equipped with Internet-connected devices are exposed to identity theft (Jacobsson et al., 2016). Hackers could gain access to private information stored on networked devices. Credit card numbers and other personal information stored on these devices are also vulnerable. Identity theft could lead to monetary loss, damage to one's credit rating, and a variety of complications. Additional safety measures are therefore required to be taken by homeowners to secure their private information.

2. **Illegal tracking of location**
   Smart home systems are not immune to security breaches, and one such vulnerability is the illegal tracking of location. Without the owner's knowledge or consent, hackers may be able to access smart home devices and exploit them to track the location of its residents. This is a major invasion of privacy that puts the safety of families at risk. For instance, if a hacker could ascertain the location of its homeowner, they could utilize this information to commit theft or robbery. Additionally, this data could be sold on the dark web, creating additional risks for homeowners.

3. **Leak of personal information**
   One of the most dangerous risks related with smart homes is the possibility of personal information leak. Smart home systems and appliances capture a massive amount of data, from daily routines to personal preferences, which might be intercepted or accessed by cybercriminals should the devices are not properly secured. This could lead to identity theft, financial fraud, or other criminal activity (Jose et al., 2015). It is crucial to secure smart homes by using strong passwords, updating software regularly, and carefully examining privacy rules before connecting any new devices to the network.

4. **House break-in**
   No system is fool-proof. It is still possible for hackers to break into a smart home system and use it to exploit the devices such as lock security, cameras and home gates to their advantage (Coboi et al.,2021). Such vulnerability makes it easier for hackers to physically break-in and trespass the houses without the homeowner's knowledge, causing unimaginable harm to the family. They can steal valuables, important documents and even cause physical assault. The break-in could also be "virtual". By gaining control of home devices such as security cameras, hackers could turn the surveillance system to their advantage.

	From literature review	From exemplar cases
Privacy intrusion	Breaches of smart water meters reveal home activities [22]	Smart doorbell camera invades neighbour's privacy (UK court case[2])
	Uncontrolled/unauthorised access to private data recorded by aged care monitoring devices [39]	App companion of smart sex toy records private moments without consent of the user (USA court case[3])
Hacking	Voice replay and voice injection attacks on voice assistants [5]	Smart TV hacked to access victim's personal details (UK police report)
	False data injection on smart devices [26]	Smart camera and baby monitor feeds from 700 households were hacked and published online (USA court case[4])
Malware	652,881 interactions with botnets targeting IoT devices [28]	Mirai malware disables CCTV, routers, and other devices (USA court case[5])
	8,713 IoT malware samples [44]	Botnet targeting smart home devices and requesting ransom (Bitcoinabuse report)
DoS/DDoS	Semantic DoS attacks on five smart home devices [27]	Devices infected with Mirai malware to carry our DDoS attacks (USA court case[6])
	DoS attacks on seven routers [52]	DDoS attacks on gaming networks (USA[7] and Finland[8] court cases)
Stalking	Controlling partner activities through smart cameras, thermostats, TVs and locks [34]	Control of ex-partner's activities through Amazon Alexa (UK police report)
	Inferring activity of household members from smart thermostat and air detector [59]	App companion of ELAN smart home system used to control ex-partner activities (UK police report)

Figure 3: Examples of digital harms identified in literature review and case studies.
Source: The digital harms of smart home devices: A systematic literature review

How to secure your smart homes

There are ways to enjoy your smart homes without having to worry about cyber threats. To ensure security of your smart home, it is most important to secure the Internet router (Lee et al., 2019). First and foremost, change the default login and password as they are usually very simple to figure out. Use a strong password with letters, numbers, and special characters to protect your account.

Next, make sure that the router's firmware is updated regularly. Updates from manufacturers are frequently released to fix performance issues and solve weaknesses in security (Lin et al., 2016). The information on how to upgrade the firmware can be found in the router's manual or manufacture's website. Changing your Internet router's default network name (SSID) and turning off remote administration are also important security measures. Most routers use a common default network name which makes it simple for hackers to recognize and target your network.

The network name should be changed to something unique with remote administration disabled, so as to ensure that only authorised devices can connect to your network. Enabling network encryption, such as WPA2 or WPA3, which encrypts data transmitted across your network, is also crucial (Lamers et al., 2021). If hackers managed to intercept your data, encryption ensures that they will not be able to read it. Finally, consider encrypting all internet traffic from your smart home devices through a virtual private network (VPN). Even if your router is breached, a VPN adds an additional level of security by encrypting all data transmitted across your network.

Conclusion

Smart homes offer many advantages which have completely changed how people manage their homes. Such systems offer convenience, comfort, energy efficiency, and improved security. Although smart homes bring about unprecedented convenience, they also raise concerns about security and safety from identity theft, illegal tracking of location, personal information leak to the possibility of "virtual" break-in. Such risks can pose serious threats to homeowners and their families. To maintain a secure and safe environment, smart homeowners must be vigilant of the dangers and keep abreast of the latest home security measures.

Reference

1. https://books.google.com.my/books?hl=en&lr=&id=ruoIdrgFFmoC&oi=fnd&pg=PA43&dq=Smart+homes+were+introduced+back+in+1975+when+the+creation+of+X10&ots=PL2Aop1PYR&sig=7M9BluOrbR67av99zdW07Y37ZIM&redir_esc=y#v=onepage&q&f=false
2. https://www.researchgate.net/profile/Syed-Kashan-Ali-Shah-2/publication/344471523_Smart_Home_Automation_Using_IOT_and_its_Low_Cost_Implementation/links/6094419d92851c490fbf94a9/Smart-Home-Automation-Using-IOT-and-its-Low-Cost-Implementation.pdf
3. https://www.sciencedirect.com/science/article/pii/S1364032119308688
4. https://ieeexplore.ieee.org/abstract/document/7973622
5. https://www.sciencedirect.com/science/article/abs/pii/S0167739X15002812

System Effectiveness Leads To Robust Structure In An Organization: A Case Study

By | Ku Nurfadhlin, Zarina Musa, Noor Asyikin Zulkifli, Azatulsheera Mohd Azman

Introduction

Information technology (IT) plays a crucial role in every organization by helping them manage their business more effectively. Even basic usage of technology could significantly boost a company's production and efficiency. IT systems provide users with information they require to complete tasks efficiently. Every organization must continuously analyze their IT system landscape and select projects that fulfil business requirements while adding value to the company. This article looks at how IT system enhancement could lead to more robust structure in an organization. Organization can tighten security while improving performance in terms of scalability, security, user interface and user experience. Additionally, implementing a load balancing strategy can enhance the system's scalability.

Based on Gartner's 2011 survey of the priorities gathered from more than 2,000 chief information officers, most organizations develop IT systems to meet important business objectives such as improving competitiveness, increasing productivity and efficiency, accelerating growth, encouraging innovation, and reducing costs (Linton, 2011). [3]. A Business Management System is an integrated set of management processes and tools that helps align a company's strategy and annual targets with daily operations, monitor performance, and initiate corrective actions. It enables managers and employees to drive process improvements every day, thereby allowing sustained progress (Hatto & Pate, 2022). [2]. A Business Management System helps identify stakeholders within an organization from end-users, IT staff, to management, and all related parties. The system also identifies each stakeholder's needs and expectations in order to align its focus on enhancement processes which boosts performance.

Since 2021, CyberSecurity Malaysia under MySEF Department has implemented a system known as Quality and Project Management System. Prior to its implementation, all operations and documentation related to quality and project management task were controlled manually which took a lot of effort and created massive paper trail. To overcome the challenges, a system was developed to help each department meet their quality objective requirements in service delivery to customer, tracking of all progress, approval, request, and all relevant tasks ranging from management to operational level. This system assisted in ISO/IEC 17025 audit requirements and maintained timely and quality delivery of all projects. The system received positive feedback from users and it improved the business process within the department. Through a well configured management system, the department is in a position to add more security features, and enhance the system functionality to boost the user experience.

According to Amaravadi & L. Lessard 2017, Yourdon and others [1] pioneered a structured methodology in the 1980s to develop a system that could meet requirements with minimal maintenance. Based on a software development life cycle, they created a number of tools and techniques for systems such as SDLC. According to their methodology, systems were designed using Data-flow-diagramming, a data dictionary, and Structured English during the analysis phase. Systems theory helped develop systems engineering, which is concerned with the design of complex systems. The purpose of systems engineering is to manage complicated systems in order to ensure their reliability (Wikipedia '16a). It includes concepts such as user requirements, systems design, and reliability analysis, which opened the path for software engineering (Seedat, 2020). [5]. For instance, enhancing the system's user interface and user experience is crucial to improving usability and user satisfaction. A well-designed user interface and user experience can help enhance user engagement, productivity, and attain overall satisfaction. Moreover, a good system will improve data management capabilities from data retrieval, processing, storage, and integration of advanced analytics and reporting features. This could bring about more benefits for any organization if they apply this approach in their organization.

Common Issues in Developing A Good System

1. **Data leakage**
   In the modern digital economy, companies have greater access to data and information than ever before. Data serves as the foundation for critical business decisions. Companies must therefore invest in data management systems that increase visibility, dependability, security, and scalability to ensure staff have proper information for decision-making. As time progresses, it is important that organizations protect their confidential information and data from any data loss or leakage. Data leakage is the unauthorized transmission of information from an organization to an external source. This data leak could then be exposed publicly or fall into the hands of a cybercriminals either physically or electronically through hard drives, USB devices, mobile phones, and other devices (ManageEngine, n.d.). [4]. Information and data leaks are mostly caused by exchange of information through unsecured tools, stealing of company data by employee, disclosure of confidential information without authorization, information transmitted to the wrong recipients by error, and phishing scams.

2. **IT Security**
   Each organization should create, implement, and maintain a thorough data security plan. This strategy should encompass all types of data that an organization collects, stores, processes, or communicates. The purpose of IT security is to prevent unauthorized users, sometimes known as threat actors, from disrupting, stealing, or exploiting an organization's digital assets, devices, and services. Moreover, an effective security strategy must be put in place to reduce vulnerabilities and address a wide range of cyberthreats against the system. Users who connect directly to the Internet may be not secured by the traditional security stack when utilizing applications or transmitting data and migrating identities to the cloud. Cloud security may be deployed as software-as-a-service (SaaS) applications and public cloud usage. It can also be activated through the engagement of a cloud-access security broker (CASB), a secure Internet gateway (SIG), or cloud-based unified threat management (UTM) (What Is IT Security? - Information Technology Security, n.d.). [8]. In this regard, enhancing the system's security is essential in order to protect sensitive data and ensure compliance with relevant regulations and industry standards. A robust security framework not only protects the organizations valuable and confidential information but also build trust with customers and stakeholders.

Suggestions criteria for Quality and Project Management System in MySEF

1. **Functionalities**
   The functionality of MySEF's system allowed its department's staff to access and use the system in an efficient, accurate and safe manner. In addition, the system is designed to track all documents, records and projects involved within MySEF Department for ease of use. It has built in privilege access according to their department or unit. Besides, access to the system is protected by firewall and Virtual Private Network (VPN) which are essential for protecting sensitive data, preventing unauthorized access, and defending against hacking, malware, and denial-of-service attacks. This is an essential component of a robust and secure network infrastructure for both individual users and organizations.

   The system can be further improved through a more user friendly navigation. Efficient navigation is critical to enable users to find the information they require easily and navigate effortlessly between various sections of the system. With an intuitive navigation, users can explore the system confidently. Improving navigation requires restructuring menu options, providing clear labels and categorization, and implementing a search functionality that can quickly locate specific features or content. Integrating user feedback can also help an organization discover any issues or problems that arise and gain insight into user preferences. Integrating such feedback at user interface and during user experience design process, allows an organisation to modify the system to meet the needs and expectations of the users. User feedback can also be collected within the system through surveys, usability testing, or feedback forms.

2. **New Technology**
   Today, every organization needs to be fully prepared to defend against cyber attacks on their information systems. Cybersecurity

threats affect just about any organization—from businesses, governments, non-profit organizations to even individuals. Cybersecurity threats could also spark the development of new cybersecurity technology. [6] Based on the research by Simmons 2020, the following are some of the latest trends in cybersecurity technology:

Blockchain
Blockchain is a type of database that stores data in secure blocks. It uses cryptography to connect the blocks. Blockchain enables data collection but not editing or deleting. Blockchain can be used by cybersecurity professionals to secure systems or devices, implement standard security processes, and make it nearly impossible for hackers to breach databases. Blockchain benefits include improved user privacy, less human error, increased transparency, and cost savings by eliminating the need for third-party verification. Blockchain also eliminates the security issue of storing data in a single location. Data is instead distributed among networks, resulting in a decentralized system that is less vulnerable to hackers. Such storage architecture could enhance database systems protection against data breach.

Cloud-Encryption
Cloud services promote efficiency and enable organizations to provide better remote services at a lower cost. Yet, keeping data in the cloud could lead to vulnerabilities. Cloud encryption technology converts data from intelligible information to unreadable code before it enters the cloud. To unravel cloud encryption, cybersecurity specialists utilize a mathematical technique to create an encryption key. Only authorized users with such key can decrypt the code, allowing data to be read again. Having restricted access reduces the likelihood of any unauthorized intruders from breaching the data. Cloud encryption, according to experts, is an effective cybersecurity tool for data security. Unauthorized users can be prevented from having access to usable data by using cloud encryption. Cloud encryption also increases client trust in cloud services and help businesses comply with regulatory requirements.

Defensive Artificial Intelligence (AI)
Defensive artificial intelligence (AI) is used by cybersecurity professionals to detect and prevent cyberattacks. As offensive AI and adversarial machine learning are more difficult for conventional cybersecurity techniques to detect, savvy cybercriminals often employ them. Deep fakes, bogus photos, fake personas, and reels that convincingly depict individuals or events that never take place or exist are examples of offensive AI. Adversarial machine learning can be used by malicious actors to deceive machines into malfunctioning by feeding them erroneous data. Defensive AI can be deployed by cybersecurity professionals to identify and prevent offensive AI from monitoring, testing, and learning how the system or network work. Defensive AI can fortify algorithms, making them more difficult to decipher. Through defensive AI, machine learning models can be subjected to more rigorous vulnerability testing by cybersecurity researchers. Such tests could be implemented across all departments to achieve technical improvements which can enhance the systems functionality. Through upgrading of hardware, software, or infrastructure components, an integration of emerging technologies can also add value to a system.

Zero Trust
Traditional network security methodology is based on "trust but verify," basis which assumes that users within an organization's network perimeter are not dangerous risks. Zero Trust, on the other hand, adheres to the principle of "never trust, always verify." Zero Trust is a network security strategy that requires all users to authenticate themselves before accessing an organization's data or applications. Zero Trust does not assume that network users are more trustworthy than anyone else. Such heightened verification of all users could result in improved overall information security for an organization. Cybersecurity professionals can use Zero Trust to liaise with remote workers and overcome difficulties such as ransomware threats more safely. A Zero Trust architecture may include a combination of capabilities such as multi-factor authentication, data encryption, and endpoint security.

Data Loss Prevention (DLP)
DLP is a technique of detecting and preventing sensitive data breaches, leaks, or deletion. DLP is used by organizations to protect and secure their data while still complying with requirements. The term data loss prevention (DLP) refers to defending against both data loss and preventing data leakage. Data loss refers to

loss of critical enterprise data which could occur with a ransomware attack. Data loss prevention focuses on preventing data from being transferred out of organizational boundaries. By implementing a data loss prevention strategy, organizations can reduce the risk of data breaches, thereby complying with data protection regulations, and preserving their reputation and the trust of their customer and partners.

Conclusion

Every organization or company should implement a good business management system so that they can secure and protect all vital or confidential data and information systematically. This would prevent any cyber threats or cyberattacks from occurring anytime and anywhere. From the aforementioned case study, a Quality and Project Management System can be fortified by deploying the latest technology to obtain an effective and efficient system by reducing staff workload and enhancing departmental performance. By building a systematic and efficient navigation, the system would become more user friendly. Hence, resulting a more effective and manageable work flow which yields satisfaction and achieve the overall goals of meeting the customers' and organization's requirements.

References

1. Amaravadi, C., & L. Lessard, Z. (2017, March). The Characteristics of Good Systems. ResearchGate; London Journal of Research in Computer Science and Technology. https://www.researchgate.net/publication/314412163_The_Characteristics_of_Good_Systems
2. Hatto, M., & Pate, D. (2022, July 7). Case Study: Tips for Making Your Business Management System More Effective. TBM Consulting. https://www.tbmcg.com/resources/blog/case-study-tips-for-making-your-business-management-system-more-effective/#:~:text=An%20effective%20Business%20Management%20System%20is%20a%20deliberately%20integrated%20set
3. Linton, I. (2011). Five Reasons Organizations Develop IT Systems. Chron.com. https://smallbusiness.chron.com/five-reasons-organizations-develop-systems-23853.html
4. ManageEngine. (n.d.). Data visibility and security solution by ManageEngine DataSecurityPlus. ManageEngine DataSecurityPlus. https://www.manageengine.com/data-security/what-is/data-leakage.html
5. Seedat, H. (2020, February 28). Plan for Successful System Implementations. ISACA. https://www.isaca.org/resources/isaca-journal/issues/2020/volume-2/plan-for-successful-system-implementations
6. Simmons, L. (2020, October 8). Hot Technologies in Cybersecurity - Cyber Degrees. Cybersecurity Degrees | Cybersecurity Degrees Online. https://www.cyberdegrees.org/resources/hot-technologies-cyber-security/
7. Tableau. (n.d.). Data Management: What It Is, Importance, And Challenges. Tableau. https://www.tableau.com/learn/articles/what-is-data-management#:~:text=Data%20management%20protects%20your%20organization
8. What Is IT Security? - Information Technology Security. (n.d.). Cisco. https://www.cisco.com/c/en/us/products/security/what-is-it-security.html#~types-of-it-security

Data Protection Officer (DPO): A Critical Role To Safeguard Data Privacy In The Organization

By | Naqliyah Zainuddin &Mayasarah Maslizan

Introduction

Businesses today collect and process data for the purpose of advertising, marketing, analytics, research, product delivery, communication with customers, and product/service functionalities improvements. The collection and processing of enormous amount of data may include Personally Identifiable Information (PII), Payment Card Information (PCI) and Protected Health Information (PHI).

Emerging technologies are also capable of harnessing enormous amounts of real time data and seamlessly transmitting that data through a complex network of connected technologies. Mass data flows and inter-connectivity of multiple devices pose challenges to how an organization can best protect its data privacy.

Data or information privacy is a subset of data security which is concerned with the proper handling of data to comply with data protection laws, regulations, and general privacy best practices. Data Privacy also focuses on individual rights on how data is gathered, stored, managed, and shared with other parties in accordance with the existing privacy regulations such as General Data Protection Regulation (GDPR). With technology advancement and exponential growth in data, managing massive amount of data and upholding data privacy become an arduous task.

Data Privacy Impacts And Challenges

Over the last decade, data has enabled the advent of revolutionary and impactful innovations and technologies. However, maintaining consumer data privacy and preferences is a major concern. In the absence of mandatory data privacy protection or violation of one or more relevant privacy safeguarding requirements, an organization may fall victim to data privacy breach. A data privacy breach is an incident in which sensitive, confidential, or otherwise protected data are accessed, viewed, stolen, or used by an individual or organization without the knowledge or authorization of the data owner. Data privacy breaches can occur in any organization, from small businesses to large corporations, and result in serious consequences for both the organization and its customers.

Organizations may also face legal action, financial losses, and reputational damage due to data privacy breach. As a result of their data being compromised, customers may also suffer financial losses, identity theft, and other forms of fraud. In addition, data privacy breaches can lead to the loss of customer trust and loyalty, which will have long-term consequences for an organization. To grasp the relevance and significance of global data privacy, one must understand the challenges an organization encounters in protecting personal data.

Managing data access is one of the most challenging tasks of any data management plan for any organizations. It is not sufficient to declare who has and does not have access to the data. A rigorous adherence to the relevant standards/guidelines in access control privilege is required. There may be a possibility of malicious agents trying to access numerous devices and data without one's knowledge or permission. Besides, various methods are used by advertisers, websites, and other entities to track and identify internet users. Third-party cookies and browser fingerprinting are two examples of such methods. IP addresses can also reveal a lot of information about someone's identity and behaviour on the Internet.

To better protect their citizens' privacy, governments all over the world have outlined strong guidelines on enforcing data privacy practices in organizations. Although phrasing of such legislation varies, the goal is the same in which organizations must act to ensure protection of their citizens' privacy. Violations of any of the privacy legislations such as GDPR can result in fines of up to 4% of total revenue. These restrictions also hold businesses accountable in

the event of a data privacy breach. Thus, in view of such compliance requirements, organizations must take necessary steps to protect their customers and its business operations.

Importance Of Data Privacy Protection In An Organization

Data is one of most valuable assets for an organization. Organizations see significant value in collecting, sharing, and using data. Transparency in how organizations obtain consent, adherence to privacy policies, and management of data obtained are critical to establishing confidence and accountability with customers and partners. Privacy is an individual's fundamental right to be free from unauthorised surveillance. In a democratic society, it is essential to be able to exist in one's own space and express one's thoughts openly behind closed doors.

Data privacy protection encompasses a process of safeguarding important data from corruption, compromise or loss and providing the capability to restore data to a functional state should something render it inaccessible or unusable. Data privacy protection assures that data is not corrupted, accessible for authorized purposes only, and in compliance with applicable legal or regulatory requirements.

Every organization, regardless of size, must be compliant to the relevant data protection laws and regulations on management and protection of personal data, as well as implementation of policies and processes on data privacy and security. Every employee must ensure they are following the right policies and procedures in place. Hence, it is crucial for an organization to appoint dedicated personnel such as Data Protection Officer (DPO) to manage and protect the data.

Requirement Of Appointing DPO In The Organization

If your organization's fundamental activities entail processing sensitive data on a large scale or regular and systematic surveillance of persons, you must designate a DPO, regardless of whether the organisation is a data controller or data processor.

According to Article 39 of GDPR, the scope of responsibilities of a DPO vary depending on the organization and its specific demands for privacy legislation compliance. The following are typical DPO responsibilities:

a. inform and advise the organization and its employees on their data protection obligations;
b. monitor the organization's compliance with GDPR and internal data protection policies and procedures. This will include monitoring the assignment of responsibilities, awareness training, and training of staff involved in processing operations and related audits;
c. advise on whether a DPIA is necessary, how to conduct one and the expected outcomes;
d. cooperate with the supervisory authority; and
e. serve as contact point for data subjects on privacy matters, including data subject access requests.

Singapore's Personal Data Protection Act (PDPA) requires organizations to appoint at least one person as the DPO to manage data protection obligations and ensure PDPA compliance. The DPO function may be a separate responsibility or an addition to an existing organizational role. Responsibilities of a DPO based on Singapore PDPA are as follows:

a. ensure PDPA compliance when establishing and implementing personal data management rules and processes;
b. Promote data-protection culture among employees and convey personal data-protection rules to stakeholders
c. Manage questions and complaints about personal data protection;
d. Notify management of any potential concerns involving personal data; and
e. If necessary, interact with the PDPC on data protection issues.

While the appointment of DPO is not currently required under the Malaysian Personal Data Protection Act 2010 (PDPA) yet, there have been recent proposals to introduce the same as a mandatory requirement. Based on the Public Consultation Paper, the Commissioner has recommended making it mandatory for data users to appoint DPOs, as well as issuing recommendations on the appropriate criteria for DPO appointment including under which categories to appoint DPOs.

Need For DPO In Ensuring Data Protection

A Data Protection Officer (DPO) is a professional who is in charge of ensuring that an organization abide by the laws and regulations governing the processing and protection of personal data. This involves ensuring an organization has adequate safeguards in place to protect the privacy and security of personal data, educating employees on best practices, and responding to any data protection-related concerns or complaints. A DPO is also in charge of reviewing the organization's data protection policies and practices periodically, as well as offering data protection guidance and support to other employees. In some situations, a DPO may also carry out Data Protection Impact Assessment (DPIA) and liaise with regulatory authorities on data protection issues.

Today's stringent data protection and privacy regulations present serious challenges for organizations around the world. In recent years, more ASEAN countries such as Singapore, Thailand and Philippines have enacted and enforced data protection legislation. These laws demand organizations to demonstrate accountability in their day-to-day operations, not just on paper. This increases the demand for DPOs, as organizations face increased pressure to comply with applicable regulations while maintaining consumer trust.

Data protection is now a critically important issue in the modern business world, especially in corporations which handle, process, and store sensitive information. Accountability in an organization extends over the entire lifecycle of personal data in an organization, beginning with collection, usage and storage, and finally to disclosure or transfer of the information. Each stage of the information lifecycle presents risks that must be identified and managed. Inadequate protection of personal data, such as information submitted by customers via an online form, may increase the risk of unauthorized access. Such vulnerability frequently goes undiscovered in the absence of a DPO, until it is too late when a data breach occurs.

Roles And Responsibilities Of A DPO

The DPO's primary role is to oversee data protection and management programme, which governs how personal data is gathered, used, disclosed, and kept inside an organization in accordance with the requirements of applicable data protection legislation. The DPO must collaborate with all departments to create procedures that address and correct gaps and vulnerabilities in personal data processing. DPOs also collaborate with department heads to ensure that all employees are aware of the organization's privacy policy and receive proper training on data protection best practices.
Several important duties that may come under this role, including:

a. Implementing and enforcing the company's data protection policy throughout the organizations;
b. Creating guidelines for all employees and ensuring that they are strictly adhered to;
c. Organizing necessary employee training sessions, either in-house or at external sites;
d. Mentoring and supervising the company's data processors, as well as nurturing exceptional team members;
e. When necessary, providing information to upper management, which typically involves extremely sensitive data; and
f. ensuring that all data is up to date and that data deletion procedures are followed.

CONCLUSION

Due to current technology convergence that enables processing and collection of personal data, data privacy protection requires serious effort and investment from organizations in aspects of people, process and technology. Appointing dedicated personnel as a Data Protection Officer (DPO) can demonstrate to employees, customers, and other stakeholders that the organization takes data protection seriously and is committed to preserving personal data. This can contribute to the development of trust and the enhancement of an organization's reputation.

Reference

1. https://www.snia.org/education/what-is-data-privacy#_ftnref1
2. https://www.reference.com/world-view/data-protection-important-7419357969089455?utm_content=params%3Ao%3D740005%26ad%3DdirN%26qo%3DserpIndex&ueid=410674c8-9f68-42ba-b571-e67009557978
3. https://www.lexology.com/library/detail.aspx?g=ec5c2b84-c3aa-44d1-a61e-df0f35092c63
4. https://www.techtarget.com/searchcio/definition/data-privacy-information-privacy
5. https://www.financierworldwide.com/the-road-ahead-for-malaysias-personal-data-protection-act-2010#.ZF4GGy8RqO0
6. https://www.christopherleeong.com/media/4724/220211_client_update_on_the_pdpa.pdf
7. https://www.humanresourcesonline.net/data-protection-why-data-privacy-and-dpos-matter
8. https://pandectes.io/blog/the-main-responsibilities-of-the-data-protection-officer-dpo/
9. https://harperjames.co.uk/article/does-my-business-need-a-data-protection-officer/
10. https://community.atlassian.com/t5/Trust-Security-articles/Roles-and-Responsibilities-of-a-Data-Protection-Officer-Guide-to/ba-p/2306650
11. https://gdpr-text.com/read/article-39/
12. https://segment.com/resources/data-privacy/what-is-a-data-protection-officer/

Introduction to Cyber Resilience

By | Nur Fazila Binti Selamat, Nor Radziah Binti Jusoh, Mohd Nor A'kashah Bin Mohd Kamal & Mohd Faisal Bin Abdullah

What is Cyber Resilience?

Cyber resilience refers to an entity's ability to continuously deliver the intended outcome despite adverse cyber events. Cyber resilience is an evolving perspective that is rapidly gaining recognition. The concept essentially brings the areas of information security, business continuity and resilience together. (Cyber resilience, n.d.)

Cyber resilience encompasses the ability of an entity to anticipate, withstand, recover from and evolve to infrastructure and in the face of adverse conditions, stresses, or attacks on the supporting resources it needs to function.

To be resilient, a holistic approach to understanding and prioritizing organizational risk and management activities needs must be integrated into day-to-day operations (across all functions).

A resilient entity is cognizant on which information and communication systems are mission critical. It has put in place a system that prevents disruption; while also acknowledging that total protection is not possible.

Cybersecurity versus Cyber Resilience

Cybersecurity consists of technologies, processes and measures that are designed to protect systems, networks and data from cyber-attacks. Effective cybersecurity reduces the risk of a cyber-attack and protects entities, organisations and individuals from the deliberate exploitation of systems, networks and technologies. Cyber resilience entails a wider scope where it comprises cybersecurity and business resilience. Cybersecurity is effective without compromising the usability of systems and there is a robust continuity business plan to resume operations, if the cyber-attack is successful. (Cyber resilience, n.d.) `

Cyber resilience helps organizations recognize that hackers possessing the advantage of innovative tools with element of surprise could succeed in their attempt. This concept helps business prepare, prevent, respond and successfully restore to the intended secure state as swiftly as possible. This is a cultural shift as traditionally organizations see security as a full-time job requiring embedded security best practices in day-to-day operations. In comparison to cybersecurity, cyber resilience requires a business to think differently and be more agile on handling attacks. (Cyber resilience, n.d.)

	Definition	Characterization of Types of Cyberattacks
Cybersecurity	Method and processes of protecting electronic data including identifying it, where it resides, and implementing technology and entity practices that will protect it.	Affect data, whether it is the theft of data, modification or deletion of data (e.g ransomware modifying data so it is unusable)
Cyber Resilience	Ability to withstand or quickly recover from cyber events that disrupt operations.	Knock an entity offline and/or disrupt regular operations (e.g DDoS attack)

Table 1: Comparison of Cybersecurity and Cyber resilience

Components of Cyber Resilience

Figure 1: Components of Cyber Resilience

Cyber resilience is a broader approach to cybersecurity that encompasses both **CYBERSECURITY AND BUSINESS CONTINUITY** management. The aim is to defend against potential cyberattacks as well as ensure the entity's survival from an attack.

Cybersecurity and business continuity are no longer separate and distinct considerations, as both need to be amalgamated to minimize costs, protect data, and execute a streamlined, timely and effective response to any attack or data breach.

Value of Integrating Cybersecurity into Business Continuity Plans

- Significantly reduces the time required to identify and contain a data breach incident
- Business continuity management is recognized as a valuable addition to data breach incident response planning
- Significantly reduces the cost of data breach
- Results in substantial per day cost savings
- Reduces the likelihood of having recurring data breaches
- Minimizes disruptions to operations when a data breach occurs
- Improves the resilience of IT operations
- Diminishes the negative impact on reputation following a material data breach
- Business continuity management involvement reduces the average per day cost of a data breach
- Disaster recovery automation and orchestration reduces the per day cost of a data breach (Richmond, n.d.)

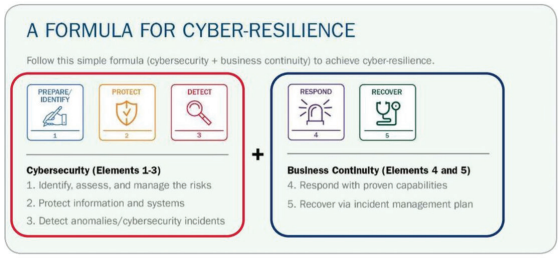


Figure 2: Cyber resilience – cybersecurity and business continuity. (Richmond, n.d.)

The Five Elements of Cyber-Resilience

Cyber-resilience must be constantly improved as threats and organizational requirements change. The refinement process can be divided into five crucial components: prepare/identify, protect, detect, respond, and recover. Each component of the cyber-resilience plan can be assessed by organizations using this approach.

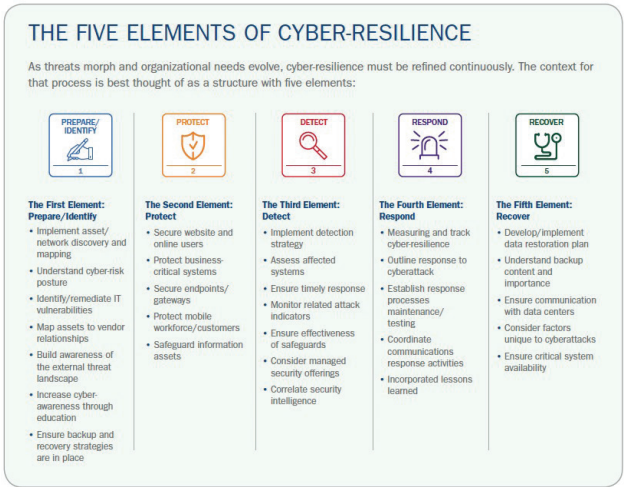


Figure 3: The five elements of Cyber-Resilience. (Richmond, n.d.)

First Element: Prepare/Identify

Understanding the organization's security and risk posture is essential in spotting attacks early and successfully defending against them.

1. Identifying and classifying the organization's critical information should be the first step.
2. Thereafter, execute a security vulnerability assessment on all infrastructure and information assets.
3. Then, compare and contrast the organization's results with those of similar organizations using the results as a baseline.

4. An organization will become a less desirable target for potential attacks once visibility issues are fixed. (Richmond, n.d.)

Second Element: Protect

The development and implementation of safety measures for critical infrastructure and services is the focus of the second component, which is intended to reduce or contain the effects of a cyberattack.

Although no amount of time, money, or effort can ensure success, cyber-resilience lowers the likelihood that a breach could be successful and, if it did, to respond rapidly to contain the damage. (Richmond, n.d.)

In particular focus on protecting and securing, the following infrastructure from cyber-attacks and/or targeted attacks:

- Website and online users
- Business-critical systems (the data center is typically the best place to start)
- Endpoints and gateways
- Mobile workforce and customers
- Information assets over their lifecycle, including protection from data loss or illegal access (consider encryption or using a data vault)

Third Element: Detect

The detect component is concerned with creating and putting into practice procedures for quickly identifying attacks, evaluating potentially impacted systems, and ensuring prompt responses.

This stage also focuses on maintaining network monitoring for any relevant attack indications and guaranteeing the efficacy of protection. A significant drawback of spending so much time and energy trying to defend against attacks is that the entity frequently neglects to plan for what needs to be done should an attack succeeds. The organization's inability to respond to the breach efficiently is one of the most serious consequences of lack of planning. (Richmond, n.d.)

The only approach to reduce harm after a breach is to put in place policies, processes, and technologies for detection and response. Although many organizations already have detection and response plans, they must routinely assess if they are sufficient and determine whether they can quickly contain and resolve breaches. The emergence of cloud, mobile, and social computing, together with big data and related analytical tools, enables the capacity to process and analyze structured and unstructured data linked to cybersecurity. (Richmond, n.d.)

Clearly, the goal is to detect breaches before they become noticeable by internal operations and customers. The objective is to reduce latency, or the period between when a breach occurs and when an organization realizes that it has been compromised. (Richmond, n.d.)

Fourth Element: Respond

The respond element offers recommendations on the types of activities that, once an attack has been identified, can accelerate remediation response to reduce its effects. A prompt response is necessary for an effective detection process. Although there are various options for services and solutions, most of the critical responses require action by staff members and internal organizational. (Richmond, n.d.)

A comprehensive response strategy that outlines what to do in the event of an incident is mandatory. It is advisable to create a Computer Security Incident Response Team (CSIRT) and incorporate it into the BCM incident management team with well-defined roles and responsibilities. The duties of reporting an incident, organizing the CSIRT's actions, and managing the team should be delegated to a team leader or manager. (Richmond, n.d.)

Having a pre-defined action plan that is understood by everyone helps streamline response efforts. A well laid response plan enables you to assess the risk levels and respond. For the quickest response, automated remediation levels are ideal — in addition to cyber drills during which employees practise executing policies and procedures. In developing the plan, focus on (Richmond, n.d.) :

- Managing risk by measuring and tracking cyber-resilience including how well systems are protected during an attack
- Creating an outline for the intended response to cyber incidents.
- Determining how response processes and procedures will be maintained and tested.
- Coordinating communication response and understanding how analysis and mitigation

activities will be performed.
- Devising a system whereby lessons learned are incorporated into future response.

Fifth Element: Recover

The final element that needs to be addressed is recovery. In order to restore data and services that may have been impacted during a cyberattack, clear processes and procedures must be developed and put into action. A cyberattack may cause implications even if it is swiftly thwarted. Whatever the consequence, organisations must be ready to quickly restore order to their people, processes, and systems. A detailed and well-thought-out recovery plan is essential for success. (Richmond, n.d.)

Many organizations may have established business continuity and disaster recovery plans that include elements such as backup and recovery, cloud storage, off-site archives, redundant and geographically separated data centers, and other business continuity measures. However, these plans often fail to anticipate essential recovery practices and scenarios. (Richmond, n.d.)

Critical systems must be available post incident to help determine how to restore other systems and data after an incident. Similar to response plans, recovery plans should be reviewed and updated frequently as well. (Richmond, n.d.)

Conclusion

Cyber threats have become increasingly more frequent, affecting the operations of organisations. Relying solely on cybersecurity and business continuity management can only help an organisation survive, but it will take longer to fully recover. The organisation may still struggle to withstand in the next cyberattack. Therefore, it is a prudent to include cyber resilience as a contingency plan.

Cyber resilience should be incorporated as part of an organization's survival strategy; in addition to cybersecurity and business continuity management. The five Cyber resilience elements spread across a company's cybersecurity and business continuity management procedures. The first three elements, "Prepare/identify, Protect, and Detect," are synonymous with cybersecurity, whereas the remaining two elements, "Respond and Recover," are synonymous with business continuity management. The key is to incorporate all cybersecurity and business continuity management actions and ideologies with the five elements of cyber resilience.

As the world becomes more interconnected in real time via world wide web and mobile devices, its vulnerability to cyber-attacks become more profound. A strategic approach to cyber resilience is therefore essential to ensure such technological advancements benefit businesses' competitiveness and agility.

References

1. Cyber resilience. (n.d.). Retrieved 10 8, 2023, from Wikipedia: The Free Encyclopaedia: http://en.wikipedia.org/wiki/Cyber_resilience
2. Richmond, W. P. (n.d.). DRII International. Retrieved from DRII International: https://drii.org/crm/presentationlibrary?plsharekey=dadc975d3468676
3. Resilient control systems. (n.d.). Retrieved 10 8, 2023, from Wikipedia: The Free Encyclopaedia: http://en.wikipedia.org/wiki/Resilient_control_systems

Ekonomi Perisian Tebusan: Memahami Model Perniagaan Di Sebalik Jenayah Siber

By | Nurfarhana Nasrulhaq binti Mohd Zulkifli

Pendahuluan

Serangan perisian tebusan telah menjadi suatu bentuk jenayah siber yang semakin meningkat dan menguntungkan. Kaedah perisian tebusan adalah penjenayah siber mengeksploitasi kelemahan dalam sistem komputer dan rangkaian untuk menyulitkan data dan seterusnya menuntut bayaran sebagai pertukaran untuk kunci penyahsulitan. Serangan ini telah menjejaskan individu, perniagaan, dan juga infrastruktur kritikal. Malah, jenayah ini telah mengakibatkan kerosakan berbilion dolar di seluruh dunia. Untuk memahami sepenuhnya kesan perisian tebusan, adalah penting untuk mengkaji ekonomi di sebalik bentuk jenayah siber ini.

Dalam artikel ini, penulis akan mengupas mengenai model perniagaan serangan perisian tebusan dan cara ekonomi industri ini berkembang. Penulis juga akan mengkaji peningkatan penggunaan Perisian Tebusan sebagai Perkhidmatan (Ransomware as a Service (RaaS) dan kesan serangan ini terhadap individu, perniagaan dan ekonomi global. Selain dari itu, penulis akan membincangkan pelbagai faktor yang menyumbang kepada perkembangan serangan perisian tebusan, termasuklah peningkatan penggunaan mata wang kripto.

Dengan memahami bagaimana dan mengapa serangan perisian tebusan boleh berlaku akan dapat membantu individu dan organisasi untuk mengambil langkah proaktif bagi melindungi diri mereka daripada menjadi mangsa dari ancaman yang semakin meningkat ini.

Bagaimana Serangan Perisian Tebusan Menjadi Industri yang Menguntungkan

Serangan perisian tebusan telah menjadi industri yang menguntungkan kerana mereka menawarkan penjenayah siber cara yang berkesan untuk membuat duit dengan aktiviti haram mereka. Secara umumnya melalui serangan perisian tebusan, penyerang akan mendapat akses tanpa kebenaran kepada sistem komputer mangsa, menyulitkan fail mereka dan menuntut bayaran tebusan sebagai pertukaran untuk kunci penyahsulitan.

Salah satu sebab serangan perisian tebusan telah menjadi sangat menguntungkan ialah mangsa sering merasakan mereka tidak mempunyai pilihan lain selain daripada membayar wang tebusan terutamanya kepada perniagaan dan organisasi yang bergantung penuh kepada data mereka untuk berfungsi. Contohnya, hospital mungkin sanggup membayar wang tebusan untuk mendapatkan semula akses kepada rekod pesakitnya, atau peniaga-peniaga kecil mungkin membayar wang tebusan untuk mendapatkan kembali dan memulihkan fail perakaunan mereka.

Faktor lain yang telah menyumbang kepada pertumbuhan industri perisian tebusan ialah peningkatan platform "perisian tebusan sebagai perkhidmatan" (RaaS). Perkhidmatan ini membolehkan sesiapa sahaja melancarkan serangan perisian tebusan, walaupun mereka mempunyai sedikit atau tiada langsung kepakaran teknikal. Platform RaaS menyediakan segala-galanya daripada kod perisian hasad sehingga kepada infrastruktur yang diperlukan untuk melakukan serangan. Sebagai pertukaran menggunakan platform tersebut adalah dengan berkongsi pembayaran tebusan berdasarkan peratusan yang ditetapkan.

Di samping itu, kebanyakan penyerang perisian tebusan telah menggunakan kaedah yang semakin canggih dan kompleks. Mereka mungkin menggunakan teknik kejuruteraan sosial untuk menipu mangsa supaya memuat turun perisian hasad atau mengeksploitasi kelemahan dalam perisian yang biasa digunakan untuk mendapatkan akses kepada sistem. Sesetengah penyerang juga menggunakan taktik "peras ugut berganda", di mana mereka bukan sahaja menyulitkan fail mangsa tetapi juga mencuri dan mengancam untuk memaparkan atau menjual data sensitif sekiranya wang tebusan tidak dibayar.

Secara keseluruhannya, gabungan dari beberapa faktor seperti bayaran yang tinggi daripada mangsa, ketersediaan alat serangan yang mudah digunakan, dan penggunaan teknik yang canggih dan kompleks telah menjadikan serangan perisian tebusan sebagai industri

yang menguntungkan dan berkembang pesat bagi penjenayah siber.yang mudah digunakan, dan penggunaan teknik yang canggih dan kompleks telah menjadikan serangan perisian tebusan sebagai industri yang menguntungkan dan berkembang pesat bagi penjenayah siber.

Mengenalpasti motif kewangan disebalik perisian tebusan

Salah satu faktor utama yang mendorong serangan perisian tebusan ialah potensi untuk memperolehi hasil kewangan yang tinggi. Dengan menyulitkan fail mangsa dan meminta bayaran sebagai pertukaran untuk kunci penyahsulitan, penyerang perisian tebusan selalunya meminta sejumlah wang yang besar. Dalam sesetengah kes, permintaan tebusan boleh mencecah jutaan dolar terutamanya kepada organisasi yang besar dan kritikal.

Selain itu, serangan perisian tebusan mempunyai risiko yang agak rendah untuk pelaku ditangkap. Kebanyakan penyerang perisian tebusan beroperasi dari negara yang sukar diakses oleh penguatkuasa undang-undang atau mempunyai undang-undang jenayah siber yang lemah. Mereka juga menggunakan mata wang kripto untuk menerima bayaran untuk menyukarkan pihak berkuasa menjejaki aliran wang tersebut.

Serangan perisian tebusan juga menguntungkan kerana boleh dilaksanakan secara besar-besaran. Sesetengah penyerang menggunakan alat automatik untuk mengimbas sistem yang terdedah dan melancarkan serangan berskala besar. Ini membolehkan mereka berpotensi menyasarkan beribu-ribu malah berjuta-juta mangsa sekaligus bagi meningkatkan potensi atau peluang keuntungan mereka.

Selain itu, hasil kewangan daripada pembayaran tebusan, penyerang perisian tebusan juga mungkin mendapat keuntungan dengan cara lain. Sebagai contoh, mereka mungkin mencuri data sensitif mangsa dan menggunakannya untuk memeras ugut atau menjualnya di pasaran gelap seperti di sesawang gelap. Mereka juga mungkin menggunakan serangan perisian tebusan sebagai satu kaedah untuk berada dalam rangkaian sistem mangsa, bagi membolehkan penyerang melakukan serangan siber yang lain atau mencuri data tambahan.

Motivasi kewangan disebalik perisian tebusan adalah kompleks. Walaupun potensi ganjaran kewangan yang tinggi sudah tentu menjadi faktor pendorong utama, penyerang juga mungkin didorong oleh faktor lain seperti keinginan untuk berkuasa kerana kekurangan peluang ekonomi mengikut undang-undang yang sah. Memahami motivasi ini adalah kunci untuk membangunkan strategi yang berkesan untuk mencegah dan bertindak balas terhadap serangan perisian tebusan.

Peranan Mata wang digital dalam serangan perisian tebusan

Mata wang digital, terutamanya mata wang kripto seperti Bitcoin memainkan peranan penting dalam memudahkan serangan perisian tebusan. Berikut ialah beberapa faktor utama yang menerangkan cara mata wang digital menyumbang kepada ekosistem perisian tebusan:

a. **Ketanpanamaan:** Mata wang kripto menawarkan tahap kerahsiaan yang tinggi sehingga menjadikannya sukar untuk mengesan aliran dana. Transaksi dalam mata wang kripto direkodkan pada lejar awam yang dipanggil blok rantai (blockchain), tetapi identiti individu yang terlibat selalunya menggunakan nama samaran. Ketanpanamaan ini cukup menarik kepada pengendali perisian tebusan kerana ia membantu mereka mengelak daripada penguatkuasaan undang-undang dan berpotensi mengeluarkan pendapatan haram mereka tanpa dikenal pasti dengan mudah.

b. **Ketakterbalikan:** Transaksi mata wang kripto lazimnya tidak boleh diterbalikkan sebaik sahaja disahkan pada blok rantai. Ciri ini berfungsi dengan memberikan kelebihan kepada pengendali perisian tebusan kerana ia mengurangkan risiko mangsa cuba membalikkan atau membatalkan pembayaran tebusan mereka selepas transaksi dilakukan. Sebaik sahaja pembayaran tebusan dibuat, menjadi amat mencabar bagi mangsa untuk mendapatkan semula dana mereka atau mempertikaikan transaksi tersebut.

c. **Mudah digunakan:** Mata wang kripto adalah berbentuk digital dan boleh dipindahkan dengan mudah merentasi sempadan tanpa memerlukan perantara atau institusi kewangan. Ini membolehkan pengendali perisian tebusan menerima pembayaran dengan cepat dan cekap daripada mangsa yang berada di mana-mana sahaja di dunia. Selain itu, dompet mata wang kripto yang mesra pengguna telah memudahkan proses menghantar dan menerima mata wang kripto walaupun individu yang mempunyai

pengetahuan teknikal yang terhad.

d. **Kekurangan Peraturan:** Mata wang kripto beroperasi di luar sistem perbankan tradisional, dan pada masa yang sama peraturan terhadap mata wang kripto di peringkat global masih kurang dan terhad. Kekurangan peraturan ini memudahkan pengendali perisian tebusan untuk mengeksploitasi mata wang kripto untuk aktiviti haram mereka. Walaupun usaha sedang dibuat untuk memperkenalkan langkah kawal selia untuk memerangi pengubahan wang haram dan transaksi haram, landskap kawal selia pematuhan kekal tidak stabil.

Penting untuk diambil perhatian bahawa mata wang kripto itu sendiri tidak semestinya berniat jahat atau direka untuk aktiviti yang menyalahi undang-undang. Namun, buat masa ini mata wang kripto menawarkan banyak faedah dan digunakan selain sebagai perisian tebusan. Walau bagaimanapun, ciri unik mata wang kripto telah menjadikan mereka pilihan yang menarik untuk pengendali perisian tebusan.

Perisian Tebusan sebagai Perkhidmatan: Kebangkitan Pasaran Jenayah Siber

Perisian tebusan sebagai perkhidmatan (Ransomware-as-a-Service (RaaS)) ialah sejenis pasaran jenayah siber yang semakin popular sejak beberapa tahun kebelakangan ini. RaaS membenarkan penjenayah siber melancarkan serangan perisian tebusan tanpa perlu mempunyai kemahiran teknikal atau infrastruktur yang ketara.

Pada asasnya, RaaS ialah model perniagaan berasaskan langganan yang membolehkan ahli gabungan melancarkan serangan perisian tebusan dengan mengakses dan menggunakan alat perisian tebusan yang telah dibangunkan. Pembekal RaaS mencipta dan menyelenggara perisian tebusan. Kemudiannya, sedia untuk digunakan oleh penjenayah siber lain dengan bayaran tertentu. Bayaran mungkin ditetapkan berdasarkan jumlah peratusan daripada bayaran keseluruhan wang tebusan yang diterima atau bayaran secara tetap untuk setiap serangan.

Pembekal RaaS biasanya menawarkan pelbagai ciri dan perkhidmatan kepada pelanggan mereka, termasuk nota tebusan yang boleh ubah suai, penyahsulitan automatik selepas pembayaran dan sokongan pelanggan. Sesetengah penyedia RaaS juga menawarkan program ahli gabungan (affiliate), di mana pelanggan boleh memperoleh peratusan daripada bayaran tebusan yang diterima oleh pengguna lain yang mereka rujuk kepada perkhidmatan tersebut.

Salah satu faedah utama RaaS untuk penjenayah siber ialah membolehkan mereka melancarkan serangan secara berskala dengan pelaburan yang minimum. Mereka tidak perlu mencipta perisian hasad atau infrastruktur mereka sendiri, dan mereka mendapat manfaat daripada skala ekonomi yang datang daripada pangkalan pengguna yang besar. Ini membawa kepada peningkatan dalam bilangan dan kecanggihan serangan perisian tebusan, kerana lebih ramai individu dan kumpulan akan masuk dalam pasaran.

Walau bagaimanapun, RaaS memberikan cabaran untuk penguatkuasa undang-undang dan pihak professional dalam keselamatan. Pembekal RaaS mungkin beroperasi berdasarkan bidang kuasa undang-undang jenayah siber yang lemah atau menggunakan saluran komunikasi tanpa nama untuk mengelakkan pengesanan. Mereka juga mungkin menggunakan penyulitan atau teknik pengeliruan lain untuk menyembunyikan sifat sebenar aktiviti mereka.

Berikut merupakan contoh kumpulan Raas yang terkenal :

a. **GandCrab:** GandCrab adalah salah satu operasi RaaS yang paling popular sehingga pengendalinya mengumumkan persaraan mereka pada pertengahan 2019 setelah mengaut keuntungan sebanyak $2 bilion dari wang tebusan mangsa. Kumpulan ini terkenal kerana melakukan kempen secara agresif dan penggunaan teknik penyulitan yang terbaru. Kumpulan itu menyediakan platform yang mesra pengguna untuk ahli gabungan dan menawarkan model keuntungan yang dikongsi bersama, di mana pembangun mengambil peratusan daripada pembayaran wang tebusan.

b. **Sodinokibi (REvil):** Sodinokibi, juga dikenali sebagai REvil, muncul sebagai salah satu kumpulan RaaS yang paling terkenal. Ia mendapat perhatian yang meluas pada 2019 dan 2020 untuk serangan berprofil tinggi dan menuntut wang tebusan dalam jumlah yang besar. Kumpulan ini beroperasi di laman web gelap, menyediakan ahli gabungan dengan perisian hasad yang sedia untuk digunakan dan papan pemuka yang komprehensif untuk menguruskan sebaran jangkitan perisian dan rundingan tebusan.

RaaS memberikan cabaran penting bagi organisasi dan individu yang ingin melindungi diri mereka daripada serangan perisian tebusan. Adalah penting bagi profesional keselamatan untuk memahami motivasi dan taktik pembekal RaaS untuk membangunkan strategi yang berkesan untuk pencegahan dan tindak balas.

Kos Serangan Perisian Tebusan bagi Individu dan Perniagaan

Serangan perisian tebusan melibatkan kos yang besar terhadap individu dan perniagaan, baik dari segi kerugian kewangan dan kesan bukan kewangan. Salah satu kos kewangan secara langsung bagi serangan perisian tebusan ialah pembayaran tebusan itu sendiri. Permintaan wang tebusan boleh mencapai beratus hingga berjuta-juta dolar, bergantung pada saiz dan jenis organisasi mangsa. Walaupun wang tebusan dibayar, tidak ada jaminan bahawa penyerang akan memberikan kunci penyahsulitan, malah meninggalkan mangsa dengan data yang disulitkan.

Selain daripada pembayaran tebusan, serangan perisian tebusan boleh mempunyai kos kewangan tidak langsung. Contohnya, mangsa mungkin perlu mengupah firma keselamatan siber atau perunding IT untuk membantu memulihkan data dan memulihkan sistem. Mungkin juga terdapat kos guaman yang berkaitan dengan menyiasat serangan dan melaporkannya kepada penguatkuasa undang-undang.

Serangan perisian tebusan juga boleh memberi kesan bukan kewangan kepada mangsa. Bagi perniagaan, serangan boleh menyebabkan gangguan produktiviti, merosakkan reputasi dan kehilangan kepercayaan pelanggan. Organisasi juga boleh dikenakan denda dan tindakan undang-undang jika data peribadi terjejas. Bagi individu, serangan perisian tebusan boleh mengakibatkan kehilangan data peribadi, termasuk foto, video dan dokumen penting.

Satu lagi kesan potensi serangan perisian tebusan ialah kos pencegahan dan mitigasi. Organisasi mungkin perlu melabur dalam meningkatkan langkah keselamatan tambahan, seperti data sandaran, pembahagian rangkaian dan latihan pekerja, untuk mengurangkan risiko serangan. Mereka juga mungkin perlu melabur dalam membangunkan garis panduan terhadap tindak balas insiden dan mengujinya untuk bertindak balas dengan cepat dan berkesan jika serangan berlaku.

Kos serangan perisian tebusan boleh menjadi sangat penting dan menyebabkan kerugian dalam skala yang besar. Adalah penting bagi individu dan perniagaan untuk memahami potensi kesan serangan dan mengambil langkah untuk mengurangkan risiko mereka dan bersedia untuk menghadapi sebarang kemungkinan kejadian.

Impak Perisian Tebusan terhadap Ekonomi Global

Serangan perisian tebusan telah memberi kesan yang besar terhadap ekonomi global, baik dari segi kerugian kewangan dan ekonomi itu sendiri. Walaupun sukar untuk menganggarkan impak yang tepat disebabkan oleh kurang laporan dan metodologi yang berbeza-beza. Namun, beberapa kajian dan laporan memberikan anggaran jumlah yang dikaitkan dengan kesan perisian tebusan. Berikut ialah gambaran keseluruhan:

a. **Kerugian Kewangan:** Serangan perisian tebusan mengakibatkan kerugian kewangan yang besar untuk kedua-duanya samada individu, mahupun organisasi. Menurut Statistik Perisian Tebusan 2023 oleh Tech.co melaporkan kos perisian tebusan global dijangka melebihi $30 bilion menjelang akhir 2023 Kos ini termasuk pembayaran wang tebusan, kos yang berkaitan dengan pemulihan, produktiviti dan kerosakan reputasi.

b. **Pembayaran Wang Tebusan:** Pembayaran wang tebusan kepada penjenayah siber telah meningkat dalam tempoh beberapa tahun kebelakangan ini. Sebagai contoh, bayaran tebusan purata pada suku keempat 2022 ialah AS$327,883.00 seperti yang dilaporkan oleh Coveware. Walau bagaimanapun, tidak semua mangsa melaporkan atau membayar wang tebusan, dan jumlah sebenar mungkin berbeza-beza bergantung pada sasaran dan rundingan.

c. **Gangguan Produktiviti:** Serangan perisian tebusan sering menjejaskan perniagaan. Seterusnya membawa kepada gangguan produktiviti dan operasi. Masa yang diperlukan untuk memulihkan sistem, memulihkan data daripada data sandaran dan membina semula rangkaian memerlukan kewangan yang banyak.

d. **Kesan Riak (ripple effect) Ekonomi:** Serangan perisian tebusan boleh membawa

kesan ekonomi yang lebih luas yang melebihi daripada sasaran mangsa terdekat. Sebagai contoh, gangguan dalam sektor kritikal seperti penjagaan kesihatan, pengangkutan atau tenaga boleh memberikan kesan kepada keseluruhan ekonomi. Seperti serangan perisian tebusan NotPetya pada 2017 yang menyasarkan Ukraine tetapi turut memberi kesan kepada organisasi di seluruh dunia, dianggarkan telah menyebabkan kerugian berbilion dolar.

e. **Peningkatan Perbelanjaan Keselamatan Siber:** Memandangkan ancaman perisian tebusan terus berkembang, organisasi dan kerajaan perlu melabur dengan lebih banyak sebagai langkah meningkatkan keselamatan siber. Ini termasuk perbelanjaan untuk penyelesaian keselamatan lanjutan, tindak balas insiden, latihan pekerja dan langkah pencegahan lain. Perbadanan Data Antarabangsa (IDC) meramalkan bahawa perbelanjaan global untuk keselamatan siber akan mencecah AS$300 bilion pada 2026.

Anggaran jumlah ini memberikan gambaran keseluruhan tentang kesan perisian tebusan terhadap ekonomi global, tetapi kos sebenar boleh menjadi lebih tinggi apabila mempertimbangkan faktor seperti kos tidak langsung, kerosakan reputasi jangka panjang dan kesan psikologi secara keseluruhan terhadap individu dan organisasi yang terjejas oleh serangan ini.

Kesimpulan

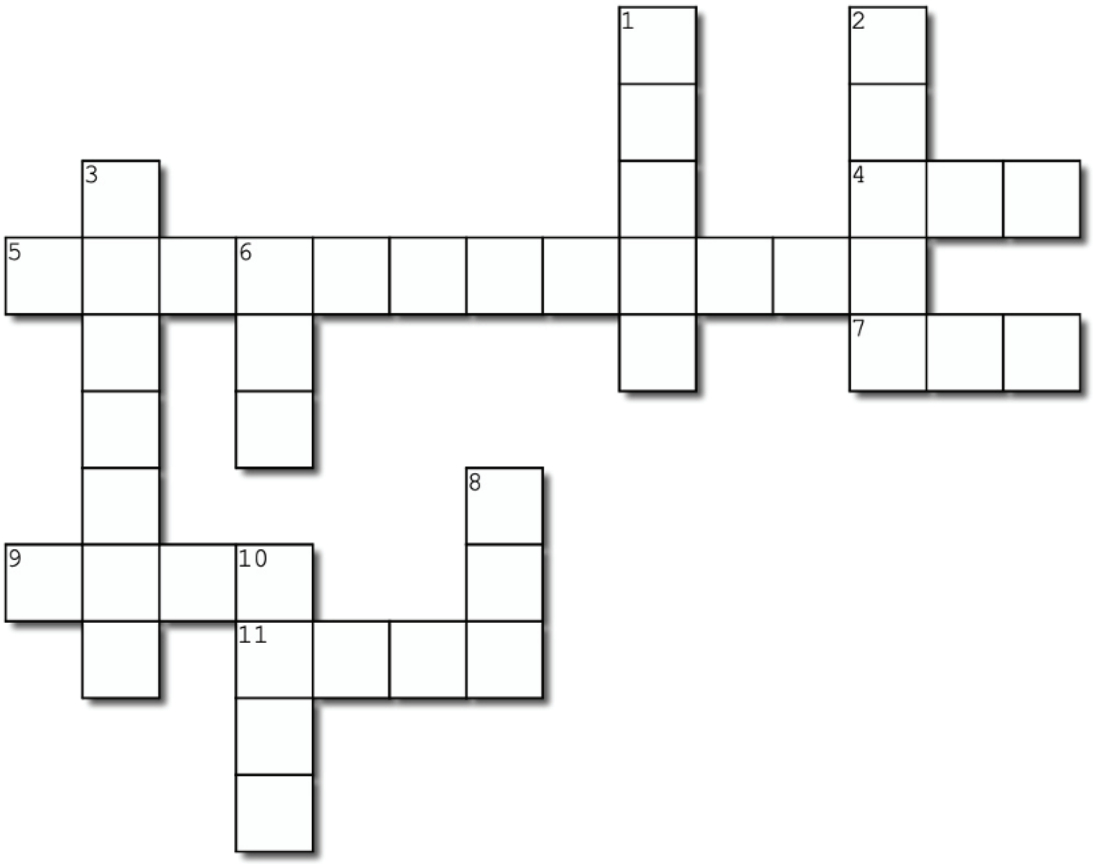
Kesan serangan perisian tebusan melangkaui kos kewangan langsung, kerana ia boleh menyebabkan gangguan produktiviti, reputasi, kos undang-undang dan kehilangan kepercayaan pelanggan. Perniagaan kecil dan sederhana (PKS) sangat terdedah kepada serangan perisian tebusan kerana mereka kekurangan sumber dan kepakaran untuk melaksanakan langkah keselamatan siber yang lebih stabil dan komprehensif. Selain itu, kesan serangan perisian tebusan terhadap infrastruktur kritikal, seperti grid tenaga dan bekalan air, boleh memberi kesan ekonomi yang lebih berimpak tinggi.

Untuk mengurangkan risiko serangan perisian tebusan, individu dan organisasi perlu melaksanakan langkah keselamatan siber yang komprehensif, termasuk data sandaran tetap, pembahagian rangkaian, latihan pekerja dan perancangan tindak balas insiden. Agensi penguatkuasaan undang-undang dan industri keselamatan siber juga penting untuk bekerjasama menangani perisian tebusan, dan memastikan penjenayah siber bertanggungjawab atas tindakan mereka. Dengan memahami ekonomi perisian tebusan dan mengambil langkah proaktif untuk melindungi daripadanya, kita dapat mengurangkan kesan ancaman yang semakin meningkat ini.

References

1. https://www.knowbe4.com/gandcrab-ransomware
2. https://tech.co/antivirus-software/ransomware-statistics#:~:text=Key%20Stats%20to%20Know,demands%20%241.5%20million%20in%202023
3. https://www.upguard.com/blog/what-is-ransomware-as-a-service
4. https://outpost24.com/blog/ransomware-report-2023-targets-motives-and-trends/
5. https://www.titanhq.com/blog/why-are-so-many-financially-motivated-cyber-attacks-based-on-ransomware/
6. https://www.sangfor.com/blog/cybersecurity/cryptocurrency-fueling-ransomware-attacks#:~:text=The%20report%20further%20states%20that,victims%20across%20diverse%20sectors%20with
7. https://www.marsh.com/us/services/cyber-risk/insights/ransomware-paying-cyber-extortion-demands-in-cryptocurrency.html
8. https://www.makeuseof.com/why-ransomware-attackers-demand-bitcoin-ransom-payment/
9. https://www.malwarebytes.com/gandcrab
10. https://threatcop.com/blog/revil-group/#:~:text=REvil%20Group%20(Ransomware%20Evil)%2C,ransomware%20attacks%20on%20organizations%20worldwide.
11. https://www.nomios.com/resources/what-is-revil-ransomware/
12. https://www.coveware.com/blog/2023/4/28/big-game-hunting-is-back-despite-decreasing-ransom-payment-amounts
13. https://www.cybersecuritydive.com/news/cybersecurity-spending-increase-idc/645338/#:~:text=Global%20security%20spending%20will%20reach,an%20IDC%20forecast%20released%20Thursday

Crossword Puzzle: Introduction to SOC



Across

4. Digital or physical evidence of a cyber attacker's intention to attack (*detected before a data breach)

5. A type of security breach which happens when data belonging to an individual or organization is improperly copied

7. The behaviour of a threat actor and a structured framework for executing a cyberattack

9. Tools that provide real-time analysis of security alerts generated by applications and network hardware

11. The technology that helps coordinate, execute and automate tasks between various people and tools

Down

1. A new and efficient IT security approach to handle vulnerability

2. The gathering of intelligence from public sources that could indicate something suspicious

3. Use of software or command to exploit weaknesses in computer systems

6. Evidence on a computer that indicates that the security of a network has been breached

8. Cybersecurity technology that continuously monitors end-user devices to detect and respond to cyber threats

10. Deliver management and outsourced monitoring of systems and security devices

Compilation Of ISO Documents And MYCEL'S Role In Cryptographic Evaluation Standards

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

Introduction

Cryptographic evaluation is a critical process in assessing the security and reliability of cryptographic systems. The International Organization for Standardization (ISO) has developed a series of documents to establish globally recognised standards and guidelines for cryptographic evaluation. These ISO standards cover various aspects related to cryptographic evaluation, providing organisations with a comprehensive framework to ensure the effectiveness and robustness of cryptographic solutions.

This article presents an overview of ISO standards on cryptographic evaluation. These standards serve as essential references for organisations seeking to assess their security capabilities in cryptographic modules, algorithms, and protocols. By adhering to these ISO standards, organisations can ensure a reliable and trustworthy foundation for their cryptographic systems.

The ISO documents related to cryptographic evaluation encompass a wide range of topics, including evaluation criteria, testing methodologies, and requirements for cryptographic modules and algorithms. These standards play a significant role in ensuring the interoperability, functionality, and resistance against attacks on cryptographic solutions.

By adhering and complying to the standards in ISO documents for cryptographic evaluation, organisations can enhance their understanding of internationally recognised guidelines and best practices in the field. Such knowledge empowers organisations to make informed decisions regarding the selection, implementation, and evaluation of cryptographic systems, enabling them to protect sensitive information, achieve compliance with industry standards, and maintain the trust of their stakeholders.

LIST OF ISO DOCUMENTS

ISO Document	Description
ISO/IEC 19790	**Security Requirements for Cryptographic Modules** · Provides the security requirements for a cryptographic module utilised within a security system, protecting sensitive information in computer and telecommunication systems
ISO/IEC 24759	**Test Requirements for Cryptographic Modules** · Specifies the methods by which testing laboratories could use to test whether the cryptographic module conform to the requirements specified in ISO/IEC 19790:2012.
ISO/IEC 30104	**Physical Security Attacks, Mitigation Techniques & Security Requirements** · Addresses how security assurance can be given for products where the risk of the security environment requires the support of such mechanisms.

ISO/IEC 18367	**Cryptographic Algorithms and Security Mechanisms Conformance Testing** · Provides guidelines for cryptographic algorithms and security mechanisms conformance testing methods. Based on the conformance testing methods employed in JCMVP and in CAVP.
ISO/IEC 29128	**Verification of Cryptographic Protocols** · Specifies design evaluation criteria as well as methods to be applied in a verification process for such protocols. It also provides definitions of different protocol assurance levels consistent with evaluation assurance components in ISO/IEC 15408.
ISO/IEC 19249	**Catalogue of Architectural & Design Principles for Secure Products, Systems and Applications** · Provides a catalogue of architectural and design principles that can be used in the development of secure products, systems and applications, together with guidance on how to use those principles effectively.
ISO/IEC 20543	**Test and Analysis Methods for Random Bit Generators within ISO/IEC 19790 and ISO/IEC 15408** · Specifies a methodology for the evaluation of non-deterministic or deterministic random bit generators intended to be used for cryptographic applications.
ISO/IEC 19896	**Competence Requirements for Information Security Testers and Evaluators** · Provides a framework and minimum requirements for the knowledge, skills and effectiveness of individuals performing testing activities for a conformance scheme.
ISO/IEC TS 20540:2018	**Testing cryptographic modules in their operational environment** · Provides recommendations and checklists which can be used to support the specification and operational testing of cryptographic modules in their operational environment within an organisation's security system.
ISO/IEC 29128	**Verification of cryptographic protocols** · Establishes a technical base for the security proof of the specification of cryptographic protocols. · Specifies design evaluation criteria for these protocols, as well as methods to be applied in a verification process for such protocols. · Provides definitions of different protocol assurance levels consistent with evaluation assurance components in ISO/IEC 15408.
ISO/IEC 15408	**Evaluation criteria for IT security — Part 1: Introduction and general model** · The Common Criteria facilitate mutual recognition of evaluation and certification results of Information Technology products. · Defines a common set of security functions to establish that IT products adhere to international regulatory requirements.
ISO/IEC 20085-1:2019	**Test tool requirements and test tool calibration methods for use in testing non-invasive attack mitigation techniques in cryptographic modules — Part 1: Test tools and techniques** · Provides specifications for non-invasive attack test tools and information on how to operate such tools. The purpose of the test tools is the collection of signals (i.e., side-channel leakage) and their analysis as a non-invasive attack on a cryptographic module implementation under test (IUT).

ISO/IEC 20085-2:2020	**Test tool requirements and test tool calibration methods for use in testing non-invasive attack mitigation techniques in cryptographic modules — Part 2: Test calibration methods and apparatus** · Specifies the test calibration methods and apparatus used when calibrating test tools for cryptographic modules under ISO/IEC 19790 and ISO/IEC 24759 against the test metrics defined in ISO/IEC 17825 for mitigation of non-invasive attack classes.

MYCEL'S Role

CyberSecurity Malaysia Cryptographic Evaluation Laboratory (MyCEL) is an accredited laboratory for validating the Cryptographic Module Validation (CMV) and the Cryptographic Algorithm Validation (CAV) services based on **ISO/IEC 19790** and **ISO/IEC 24759** standard, in line with Dasar Kriptografi Negara or National Cryptography Policy (NCP) implementation. NCP is a national strategic approach to improve efficiency and achieve self-reliance in the use of cryptography towards economic prosperity, social welfare and national security.

The objective of the validation is to increase trust in using cryptography technology in Information and Communication Technology (ICT) products and digital environments. The validation process also provides expertise and certification towards cryptographic modules and algorithm validation in compliance with ISO/IEC 19790 and ISO/IEC 24759 standards.

Conclusion

In conclusion, the ISO standards on cryptographic evaluation offer organisations a standardised framework for assessing the security capabilities of cryptographic systems. These comprehensive standards cover various aspects, such as evaluation criteria, testing methodologies, and requirements for cryptographic modules, algorithms, and protocols. By adhering to these guidelines, organisations can establish a robust foundation for their cryptographic solutions, enhancing security and mitigating vulnerabilities. The ISO standards contribute to trust-building, compliance with industry best practices, and safeguarding of sensitive information. Staying updated with the latest ISO documents is essential to aligning cryptographic evaluation practices with evolving technological advancements and emerging threats. Overall, the ISO documents provide organisations with a reliable approach to ensure secure communication and data protection, while fostering trust and integrity.

Reference

1. "NIST" in Security requirements for cryptographic modules, Federal Information Processing Standards Publication FIPS, pp. 140-3, March 2019.
2. G. Alagic, J. Alperin-Sheriff, D. Apon, D. Cooper, Q. Dang, J. Kelsey, et al., "Security requirements for cryptographic modules", ISO/IEC 19790:2012(E), 2012.
3. "Test tools and techniques", ISO/IEC 20085-1:2019(E), 2019.

Raising the Shield: A Comprehensive Look at Security Risks in Native vs. Hybrid Apps

By | Nurul Asha Jeffridin & Ummi Haziqah Mohd Jumari

Abstract On Native And Hybrid Mobile Apps

There are almost over 6.3 billion smartphones all around the world. Along with the booming mobile app industry, it is forecasted that mobile app and smartphone usage will continue to escalate. Statistics reveal that 88% of mobile users' time is spent using mobile apps [1].

Native mobile applications have transformed the way we use smartphones and tablets by providing a tailored experience based on the design of the operating systems (OS), especially iOS and Android. Native apps are designed to take full advantage of the hardware and software capabilities given by the respective operating systems and been written in platform-specific programming languages such as Swift, Objective-C, Java, or Kotlin. To create mobile app(s) that communicates elegantly with the underlying operating system, native app development necessitates the use of Integrated Development Environments (IDEs). By adhering to the specifications and standards that were established based on the OS platforms, developers could use the power of the device's hardware characteristics to deliver optimum performance and functionality.

Hybrid mobile applications have emerged as a viable alternative for businesses and developers seeking to create mobile apps seamlessly running across several platforms. In contrast to native apps, which are designed for a specific operating system (OS), hybrid apps use web technologies such as HTML5, CSS, and JavaScript to deliver a comprehensive user experience.

Battle Of The Apps: Native Vs Hybrid

Mobile applications have become essential in our daily lives, influencing how we interact with technology and the world around us. Developers are left to choose between native and hybrid app development as the demand for smooth and engaging user experiences develops. Each strategy has specific advantages that cater to different project requirements. The following is an overview of the benefits of both native and hybrid mobile apps, focusing on their distinctive features that drive app innovation.

The Pros Of Native Apps

One of the primary advantages of native apps is its ability to efficiently use built-in device functions such as the camera, microphone, GPS, and others. These apps with default hardware features as well as OS-specific APIs, provide an enhanced and smoother user experience because native apps have unlimited accessibility to the device's functionality. According to Adam and Christoffer (2013), native apps outperform WebView counterparts in terms of performance, consuming less CPU, RAM, and energy. Such superiority is evident in devices such as the Samsung Galaxy S2, Galaxy 3, and AllWinner A10. Native programs perform CPU-intensive operations more efficiently, maintain moderate memory use, and are more power efficient. These benefits underpin the enhanced efficiency and resource management that native app development provides, resulting in seamless user experiences [2]. Therefore, they are able to provide significant and pertinent interactions that adhere to the design principles and user interface standards of an individual OS. The ability of native apps to fully interact with the mobile OS environment gives them a distinct edge. Native apps can also tap into the extensive range of UI graphical elements, animations, and device-specific experiences by properly complying with the OS requirements. This kind of integration enables developers to create visually compelling, responsive, and user-friendly interfaces that meet the needs and preferences of the user.

The Pros Of Hybrid Apps

Developers can use a hybrid approach to design a single codebase that is published on different operating systems, including iOS, Android, and web browsers. Integration across platforms

provides considerable benefits in terms of development time, price effectiveness, and reach. Frameworks such as Apache Cordova (formerly known as PhoneGap), React Native, or Ionic are used to create hybrid apps. These frameworks offer a native-like container that wraps around the web code of the app, allowing it to access device features via native APIs. Such bridging allows hybrid apps to integrate with capabilities like the camera, accelerometer, and geolocation in a similar way that native apps do. In addition, hybrid apps can benefit from web-based technologies such as responsive design to deliver a consistent user experience across a variety of devices and screen sizes. They are an enticing alternative for businesses that want to reach a wider range of users because of their adaptability. Hybrid apps provide the extra benefit of lower maintenance in addition to cross-platform compatibility and responsive design [3]. A single codebase allows developers to make modifications and enhancements with ease, reducing the time and effort required to manage multiple versions of an application. As hybrid mobile applications expand, developers are coming up with creative approaches to bridge the gap between native and web-based technologies, resulting in improved performance and user experiences. Because of its potential to combine the strengths of native and web-based development, hybrid applications have become an appealing solution for businesses wishing to expand the reach of their app while lowering development overhead.

Risk Factors Uncovered: Security Challenges In Native And Hybrid Mobile Apps

In the rapidly evolving mobile app development industry, it is vital to produce applications that are not just feature-rich but secure. As we acknowledge the utility and potential of mobile apps, we must also consider the security risks they may bring about. This section explores security of both native and hybrid mobile apps, covering several risks that developers and consumer should be aware of.

Native Apps Security Risk

Despite their numerous advantages, native mobile apps are not immune to security risks, which can have far-reaching consequences for users and developers. These risks include:

a. Code Vulnerabilities: Native apps developed using platform-specific languages are susceptible to code vulnerabilities such as buffer overflows, SQL injection, and insecure data storage. Attackers can exploit these vulnerabilities to gain unauthorized access or manipulate sensitive data.

b. OS Exploits: Native apps rely on the underlying operating system for security features. However, if the OS has vulnerabilities or security weaknesses, attackers can exploit them to compromise the app or the device. Unpatched OS vulnerabilities can leave native apps exposed to attacks. It is hard to achieve comprehensive OS security, although integrating features, securing architecture, deactivating inactive functions, and prioritizing the least privileges will improve protection [4].

c. c) Reverse Engineering: Native apps can be reverse-engineered, enabling attackers to access the app's source code, algorithms, and sensitive data. Reverse engineering may lead to code tampering, creation of counterfeit apps, or extraction of sensitive information.

d. d) Malicious App Distribution: While native apps are typically distributed through official app stores, malicious apps can still slip through the screening process. Users who download and install these apps risk exposing their data to malware, spyware, or other malicious activities.

Hybrid Apps Security Risk

Hybrid mobile apps, while offering convenience and cross-platform compatibility, are not immune to security vulnerabilities either. The security risk of hybrid mobile apps include:

a. Use of WebViews in Hybrid apps can expose to Web-Specific attacks such as JavaScript Injection, Weak SSL implementation, and caching issues. These functions of native apps are more secure than hybrid apps. However, native apps cannot be considered fully secure in this function. Android's WebView enhances user experience but compromises security [5]. To mitigate WebView's vulnerable, developers can block the use of JavaScript. However, if JavaScript needs to be enabled, it is compulsory to include steps for sanitizing input to avoid cross-site scripting attacks.

b. Server-Side Vulnerability is a common vulnerability with hybrid apps having weak server-side controls. All communication

between an app and the user occurs through a server. This means the server is often targeted to hack the app's database. The application programming interface (API) should also have security measures that verify the identity and administrative privileges of the caller to thwart cybercriminals from hacking into the server.

c. Hybrid apps often use third-party libraries and plugins for enhanced functionality. However, if these libraries have security vulnerabilities, attackers can exploit them to compromise the app and its users.

d. Increased Attack Surface: Hybrid apps have a larger attack surface compared to native apps because they utilize web views and rely on web connections for certain functionalities. This broader attack surface can increase the risk of potential vulnerabilities and attacks.

e. Compatibility and Dependency Risks: Hybrid apps need to be compatible with multiple platforms and versions of web browsers. If not thoroughly tested and maintained, compatibility across various devices and browser versions can bring about additional security risks.

f. Limited Control over Security Updates: Hybrid apps depend on the web view and underlying system for security updates. This can create challenges as developers have limited control over the timely deployment of security patches, relying instead on the user's device and web browser updates.

Conclusion

To meet the different needs of consumers, two major forces in mobile app development have emerged, namely native and hybrid apps. Native apps, crafted with platform-specific languages to perfection, provide a new level of flexibility and engagement with device hardware and software. In the meanwhile, hybrid apps powered by web technologies offer a versatile alternative for cross-platform deployment.

After weighing the advantages of both frameworks, it is clear that each has distinct advantages. Native apps stand out in terms of performance, responsiveness, and full hardware integration, whereas hybrid apps scores in adaptability, lower maintenance, and a broader reach. Despite the greatness of innovation, security is an inevitable concern. Native and hybrid apps are both prone to various risks that must be managed with attention to detail. These issues highlight the importance of strong security safeguards at every level of development, from coding vulnerabilities and reverse engineering to server-side flaws and malicious distribution.

In conclusion, developers have the power to determine the direction of app experiences in a landscape dotted with both opportunities and risks. They can ensure that the mobile apps we rely on remain not only dynamic but also secure by embracing security best practices, cognizant of emerging risks, and nurturing a culture of awareness. As we move forward into the app-driven era, the balance between technology's wonders and protections will pave the path for a more secured digital future.

Reference

1. Y. Wurmser, "The Majority of Americans' Mobile Time Spent Takes Place in Apps," INSIDER INTELLIGENCE, 2020.
2. Adam Krauser and Christoffer Cortes, "Android: Resource Consumption in Native," School of Computing, Blekinge Institute of Technology, Sweden, 2013.
3. E. R. OZIGHOR and J. JIMMY, "HYBRID MOBILE APPLICATION DEVELOPMENT: A," Global Scientifics Journal, vol. 8, no. 5, 2020.
4. Z. IQBAL and K. KHAN, "SECURITY ANALYSIS OF SMARTPHONE OPERATING SYSTEMS," VFAST Transactions on Software Engineering, vol. 2, no. 2, pp. 08-15, 2013.
5. Tongbo Luo, Heng Yin and Hao Hao, "Attacks on WebView in the Android system," ResearchGate, California, 2011.

United Nations' Framework for Responsible State Behaviour in Cyberspace (Part 2)

By | Mohd Rizal bin Abu Bakar

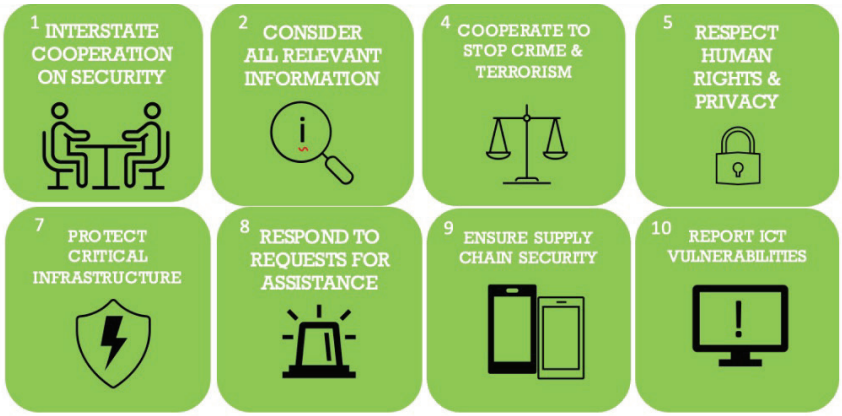
Introduction

Our previous article explored the definition of the United Nations' 4 normative framework components for responsible state behaviour in cyberspace. Some of the framework's component such as International Law as stated in United Nations' Charter and the 11 norms were also touched upon. The article also delved into possible avenues for states to share, demonstrate and prove the effectiveness of their implementation on the framework.

In this article, we continue to focus and explore one of the framework's components for responsible state behaviour in cyberspace by implementing the 11 cyber norms by United Nations through possible engagements internationally; specifically in the ASEAN region. Although the cyber norms were initially designed for western and European countries, the norms are generally similar in nature and can also be used as the basis for ASEAN state members to shape national cybersecurity policies, strategies and legislation.

As agreed in the United Nations Group of Governmental Experts (UNGGE) and United Nations Open Expert Working Group (UNOEWG), the 11 norms in the framework and their description are as below:

1. Out of the 11 norms, 8 are positive norms (in green); which are norms that nation states are encouraged to implement.



2. 3 out of 11 norms are behaviours states should avoid (in red); which are actions that are confrontational and can create tension between states.

Practical implementation of UN norms in the ASEAN region

In this section, each of the 11 norms are elaborated with implementation guidance and examples. Questions are then presented to assist policymakers to analyse and shape their policies, legislation as well as strategize their cybersecurity plan; based on the situational awareness on the topic of cybersecurity.

In line with the United Nations' objectives of promoting global peace and security, it is essential for states to collaborate on security matters, specifically with regards to the use of information and communication technologies (ICTs). This involves working together to establish and implement "digital diplomacy" measures that enhance stability and security in the use of ICTs, while also preventing the adoption of harmful ICT practices that could potentially jeopardize international peace and security.

In order to establish and implement measures that enhance stability and security, States are recommended to put in place or strengthen existing mechanisms, structures and procedures at the national level, such as:

- Cybersecurity policies, legislation and review processes
- Mechanisms for crisis management
- Whole-of-government cooperation and partnerships
- Dialogues with private sectors, academic institutions, civil society and technical communities.

States are also encouraged to share information on norms implemented with other states; including best practices and other initiatives at the national level.

Based on the above guidance, the following are questions a State or the National cybersecurity body (if any) should ask to assess their cybersecurity maturity level:

I. Is my country adequately involved in multilateral and multistakeholder forums, both regionally and technically, that address issues of cybersecurity and regional peace and security? If so, where and how is it represented?

II. Furthermore, does my government possess the resources and abilities necessary to participate in the international forums it deems significant? If the answer is yes, which forums are they?

III. Has the government formulated a set of strategic direction principles and objectives for international engagement regarding cybersecurity? If the answer is yes, what are the specific strategic direction principles and objectives?

Based on the aforementioned inquiries, the following are the action and exemplary procedures that Malaysia (and CyberSecurity Malaysia) have contributed to the ASEAN region that are aligned with the UN 11 norms in the Framework for Responsible State Behaviour:

a. Malaysia is an active participant in cybersecurity forums as part of bilateral, multilateral or multistakeholder frameworks such as:
   - ASEAN Regional Forum (National Level)
   - Asia-Pacific CERT (MyCERT, CyberSecurity Malaysia)
   - Organisation of Islamic Cooperation OIC-CERT (MyCERT, CyberSecurity Malaysia)
   - International Organisation for Standardisation, ISO (ISCB, CyberSecurity Malaysia)
   - Forum of Incident Response Security Teams (FIRST)

b. Participation in the Open Ended Working Group (OEWG) and United Nations' Group of Governmental Experts (UNGGE);
   - The Malaysian government and Philippines have the second highest active participation in both OEWG and UNGGE meetings.

c. Strategic direction principles and objectives on cybersecurity
   - Endorsement of UN resolutions and ASEAN Regional Forum (ARF) statements (National level).
   - Legislation currently under review to amend the Privacy Data Protection Act (PDPA) 2010 to strengthen law to protect personal data.

Further initiatives to explore at the national and at agency (CyberSecurity Malaysia) level:

1. United Nations' Internet Governance Forum (IGF)
    a. Mandates of IGF
        i. Discuss public policy issues related to key elements of Internet governance in order to foster the sustainability, robustness, security, stability and development of the Internet.
        ii. Facilitate discourse between bodies dealing with different cross-cutting international public policies regarding the Internet and discuss issues that do not fall within the scope of any existing body.
        iii. Interface with appropriate intergovernmental organizations and other institutions on matters under their purview.
        iv. Facilitate the exchange of information and best practices, and in this regard make full use of the expertise of the academic, scientific and technical communities.
        v. Advise all stakeholders in proposing ways and means to accelerate the availability and affordability of the Internet in the developing world.
        vi. Strengthen and enhance the engagement of stakeholders in existing and/or future Internet governance mechanisms, particularly those from developing countries.
        vii. Identify emerging issues, bring them to the attention of the relevant bodies and the general public, and, where appropriate, make recommendations.
        viii. Contribute to capacity building for Internet governance in developing countries, drawing fully on local sources of knowledge and expertise.
        ix. Promote and assess, on an ongoing basis, the embodiment of WSIS principles in Internet governance processes.
        x. Discuss issues relating to critical Internet resources.
        xi. Help to find solutions to the issues arising from the use and misuse of the Internet, of particular concern to everyday users.
        xii. Publish its proceedings.

The existing initiatives, services and functions/ roles of CyberSecurity Malaysia all fulfil the UN Framework for Responsible State Behaviour and the mandates of the Internet Governance Forum. In addition to joining the IGF as a participating member (Singapore and Indonesia is an existing member), CyberSecurity Malaysia and the country can participate in shaping and securing the ASEAN region cybersecurity landscape through other additional global initiatives such as:

- **United Nations' Global Digital Compact (GDC)**
  The Global Digital Compact is expected to "outline shared principles for an open, free and secure digital future for all". The Common Agenda report suggests issues that it might cover, including digital connectivity, avoiding Internet fragmentation, providing people with options as to how their data is used, application of human rights online, and promoting a trustworthy Internet by introducing accountability criteria for discrimination and misleading content.

Action Plan

1. CyberSecurity Malaysia via its Outreach's CyberSAFE, SiberKASA, ISCB, MyCERT, Digital Forensics, Government and International Engagement departments to apply to join the Internet Governance Forum (IGF) as a member/technical advisor to the Malaysian government by contribution to the UN Framework's Positive Norms 1,2,3,4,5,7 and 9 (related to the above IGF mandates).

2. CyberSecurity Malaysia to participate and submit views on United Nations' Global Digital Compact Technology Track on the country's cybersecurity landscape and share best practices specifically on the personal data protection, accountability criteria for discrimination and misleading content (fake news) in support of the UN Secretary General's Common Agenda; in response to the UN75 Declaration, prioritizing digital space and the need to "protect the online space and strengthen its governance." This contributes to the UN Framework's Positive Norms 1,2,4,5,7 and 9.

    a. Norm 1 – Interstate Cooperation on Security
    Malaysian government to focus on Inter-State cooperation on cross border/ jurisdiction related to cybersecurity through:
        i. CSIRT/CERT/National Focal Points (Govt, Law Enforcement)
        ii. Joint Task forces

b. Norm 9 – Ensure Supply Chain Security
   i. Requiring ICT vendors to incorporate safety and security in the design and development throughout the life cycle of ICT products.
   ii. The Malaysian government can make it compulsory for ICT vendors to comply with the national cybersecurity legislation/ requirement.
   iii. Legislative and other safeguards that enhance the protection of data and privacy by:

      a. The Malaysian government making compliance to the PDPA 2010 in the national cybersecurity legislation compulsory for personal data controllers and processors.

      b. Introduce compulsory compliance of ICT products in the legislation via testing to be conducted before it is sold to consumers and the industry.

      c. Introduction of programs for public-private partnership between ICT vendors, industry players and CyberSecurity Malaysia to promote best practices in enhancing quality, integrity and security of ICT products.

4. Actively contribute to the Malaysian representatives to the UNGGE and UN OEWG by sharing information related to cybersecurity.

5. CyberSecurity Malaysia via the Malaysian government to participate in The Global Forum on Cyber Expertise (GFCE) by sharing in the multistakeholder dialogue on the implementation of cyber capacity building based on five themes:

   a. Cybersecurity policy & strategy
   b. Cyber incident management & cri tical information protection;
   c. Cybercrime
   d. Cybersecurity culture & skills
   e. Cybersecurity standards

In conclusion, the United Nations' Framework for Responsible State Behaviour in Cyberspace presents a comprehensive and adaptable approach to addressing the challenges of the digital age. Through its 11 cyber norms, nations are provided with a roadmap to foster stability, security, and cooperation in cyberspace. This two-part exploration of the framework's components highlights its relevance not only for Western and European countries but also for regions like ASEAN. The norms' general applicability underscores their potential to serve as the foundation for shaping national cybersecurity policies, strategies, and legislation within the ASEAN community.

The implementation of these norms requires collaborative efforts on an international scale. By embracing the principles of "digital diplomacy" and actively participating in multilateral forums, nations can contribute to global peace and security. Establishing mechanisms for crisis management, fostering cooperation across sectors, and engaging with private sectors, academia, civil society, and technical communities are vital steps toward enhancing stability and security in cyberspace.

The case of Malaysia and CyberSecurity Malaysia serves as an exemplar of responsible state behaviour aligned with the UN's 11 norms. Through active participation in international cybersecurity forums, endorsement of resolutions, and legislation review to bolster data protection, Malaysia showcases a commitment to fostering a secure digital landscape. Additionally, Malaysia's proactive involvement in initiatives like the Internet Governance Forum and potential participation in the United Nations' Global Digital Compact further demonstrate its dedication to shaping a trustworthy and open digital future.

As we navigate the complexities of an interconnected world, the UN's framework provides a beacon for all. Its emphasis on positive norms for implementation, coupled with actions that nations can take, paves the way for a safer and more cooperative digital realm. By adhering to these principles, nations can contribute to global cybersecurity and build a foundation for sustainable digital development, ensuring that the benefits of technology are enjoyed by all, while mitigating potential risks.

Enhancing Online Security With Password Manager

By | Aliya Farhana Binti Mohd Nasran

Imagine finding yourself staring at a login screen, racking your brain trying to remember a password that you have used countless times before. It gets worse if you cannot recall it and must go through the hassle of resetting password yet struggling to remember the answer to your security question! Due to these tedious processes, a growing number of individuals are opting to use password managers to securely save and manage their confidential information. Password managers have emerged as a robust solution to this problem. In this article, we will explore the benefits of password manager and how they provide enhanced security to protect sensitive data.

The Role of Password Manager

A myriad of online accounts, makes it challenging for one to create and remember passwords for each one. A password manager is a valuable tool for anyone who wants to improve their online security. Instead of trying to remember numerous complicated passwords, users only need to recall one master password which will grant access to their secure password vault, where all their credentials are stored securely. They offer a convenient and efficient way to generate and elusive passwords without the need for users to memorize them individually.

How Do Password Managers Keep Data Secure?

Password manager maintains a master password, which serves as the key to unlock the password vault. Several password managers bolster security by integrating extra biometric measures like fingerprint or facial recognition. This removes the necessity of entering the master password every time, adding an additional layer of protection in case the device is accessed by unauthorized individuals.

Besides that, reliable password managers utilize well-established encryption methods such as Advanced Encryption Standards (AES). This means that all entered data becomes scrambled and indecipherable unless accessed by an authorized user. Even if the password manager were to be compromised, the exposed data would remain virtually impossible for hackers to interpret and use, making it a difficult target considering the effort they need to put through.

Password managers are typically constructed using zero-knowledge architecture, to ensure that your password manager provider is unable to view and access the information that is stored in your vault. Your master password and vault information are encrypted on your device before they are sent to the password manager's server. This means that even if the server is hacked, your passwords will be safe. In the event of a server breach, even if hackers gain access, they would not be able to interpret the encrypted data.

Password Manager Features

There are four main features in password manager which is high-grade encryption, the master password protection, two-factor authentication, and complex password generation.

a) High-grade encryption

Password managers employ strong encryption algorithms to safeguard sensitive data. When passwords and other login information are stored, they are encrypted using industry-standard encryption methods such as Advanced Encryption Standard (AES) with strong key lengths like 256 bits. By using this type of encryption, the stored password remains indecipherable and unusable even if a bad actor manages to access the database of the password manager.

b) The Master Password Protection

The master password serves as the sole key to unlocking the password manager's vault. It is essential to choose a strong and unique master password to maximize security. Password managers often employ measures like salting and hashing to protect the master password from being compromised. Salting is a technique that makes passwords more secure by adding a random string of data to the password before it is hashed. This makes it much more difficult for

attackers to crack passwords using brute-force attacks, as they would need to try each possible combination of the password and salt.

c) Two-Factor Authentication (2FA)

To further bolster security, many password managers offer the option of enabling two-factor authentication (2FA). This feature includes additional layer of protection by requesting the user for a second form of verification, for instance a code sent to the user's phone number, alongside the master password. With 2FA, your password vault is protected even if your master password is compromised.

d) Complex Password Generation

Creating strong, unique passwords for each online account is essential to minimize the risk of password-related breaches. Password managers simplify this process by providing built-in password generators. These generators can produce complicated, random passwords that are highly resilient to typical hacking approaches like dictionary attacks. By using unique and complicated passwords for each account, the potential damage caused by a single compromised password will be limited.

Benefits of Using a Password Manager

There are myriads of benefits of using a password manager. Those benefits include:

1. **Highly Secure Password Generator:** With password managers, there's no need to spend time brainstorming and creating passwords. Password generators can produce secure passwords with varying levels of complexity, saving time and essentially impossible to guess.

2. **Simplified Process:** Password managers not only ensure the safe storage of passwords but also enable users to manage all logins through a single application. This feature proves invaluable for individuals dealing with numerous websites and platforms.

3. **Auto-Fill Convenience:** Many password managers include a built-in auto-fill feature that streamlines the process of entering passwords and other recurring information. This convenience extends to payment details and addresses, alleviating the burden of memorizing multiple passwords.

4. **Secure Password Sharing:** Password sharing among friends and family is common, but simply pasting passwords into chats is risky. Password managers offer a secure way to share passwords with others, ensuring better protection.

5. **Compatibility Across Platforms:** Password managers are user-friendly applications that require minimal resources. Consequently, they can be easily developed for various platforms, such as web browsers and smartphone apps, ensuring users access their password vaults regardless of their preferred method of connection.

6. **Multi-Factor Authentication:** In the event a hacker gains access to the master password through a keylogger, enabling two-factor authentication adds an extra layer of security. Without this additional factor, the stolen password remains ineffective, ensuring continued safety and the vault remaining locked.

7. **Digital Inheritance:** In the unfortunate event of your passing, your designated family member or estate administrator will be granted access to your password vault.

Are Password Managers Safe?

It is an undeniable fact that passwords are incredibly secure within a password manager. In comparison to storing passwords in a spreadsheet or document, a fully encrypted virtual vault acts like a secure fortress, making it extremely difficult for hackers to breach.

However, all roses have sharp thorns.

In 2022, a popular password manager called LastPass announced it had suffered a security breach. Karim Toubba, a CEO of LastPass revealed that an unauthorized party was able to gain access to some elements of its customers' information and took portions of source code along with technical information. After the incident, many of its customers are left to wonder whether password managers can be trusted again

According to Kevin Higgins, a senior cybersecurity expert at Denver-based network security company Optiv, although possible to be hacked, a password manager is still considered the best choice to manage personal passwords. He stated that having a dedicated tool that can

auto-generate strong passwords in our stead increases security significantly.

Furthermore, when passwords are stored in an encrypted fashion, as is the case with LastPass on its servers, they retain their strength and complexity, thereby reducing the likelihood of attackers being able to decrypt and access the passwords in plaintext. Besides that, Nabil Alsharif, a software engineer, and information security consultant, stated in Cybernews that LastPass users who had been breached are still probably in a more secure position than people who do not use a password manager.

Password managers are safe, but the safety levels also depend on the person using them. If your password is as simple as “ASDFGH123” for all your accounts, not enabling 2FA, then it does not matter how secure your password manager is. There will be a person that is able to guess that password eventually. Nevertheless, since nothing is 100% secure, it is in best interest to adhere to password management best practices and use full-featured password managers from reputable brands to decrease the odds of becoming a victim.

Best Practices for Password Manager Usage

To ensure optimal security and convenience, it's important to follow best practices when utilizing a password manager. Here are best practices for using password managers securely with some of these coming from NIST Password Guidelines:

1. **Choose a Reputable Password Manager:** Choose a password manager from reputable companies with a proven track record in cybersecurity. Research user reviews, security audits, and expert opinions to assess their reliability.

2. **Create a Strong Master Password:** Your master password is the key to unlocking all your other passwords, so it's crucial to make it strong, unique, and difficult to guess. Based on NIST Password Guidelines, the minimum length for password is eight-character. The guideline also stated that the longer the password the better it will be. Refrain from using typical phrases, personal-related information, or easily detectable patterns. For example, "LOVEMOM1965" is easy to remember and type in, but it's not as secure as "KlmnT$#TOY-4."
3. **Screen Your Passwords:** Use password strength detection tools to measure the strength of your password before use. Always ensure that it was sufficiently complex (using a variety of letters, numbers, and special characters) and unique. Review security score within the security dashboard to know whether passwords that are commonly used, or weak.

4. **Enable 2FA or MFA (Multi-factor Authentication):** Whenever possible, enable two-factor or multi-factor authentication for an additional layer of security. For example, by connecting a phone or email to a login, a confirmation passcode can be sent to a device that will need to be entered for authentication. This acts as a safeguard against unauthorized access even if someone manages to obtain your master password. For example, a time-sensitive code or app push alert along with a password to gain access.

5. **Regularly Update and Patch:** Ensure that antivirus has been installed and keep your password manager and all associated applications up to date with the latest security patches. Regular updates often include bug fixes and security enhancements, reducing the risk of potential vulnerabilities.

6. **Never store the master password in the password manager:** This would defeat the purpose of using a password manager in the first place.

7. **Use a passphrase:** When creating a master password, use a passphrase. For example, a series of words that are easy to remember, but hard to guess. A combination of familiar and unconventional, like "bean burrito ice cream split," or a string of random objects easily imaginable for humans but difficult for computers, such as "fancy rat neon avocado car."

8. **Change master password regularly:** Never reuse password even with a password manager. Create unique passwords for every site. This will help to keep your passwords safe in case your master password is ever compromised.

9. **Never use password storage in an Internet browser.** This is referring to typical pop-ups asking if you'd like to "remember this password?” for next time. Those free built-in password managers may feel convenient and easy but not at all advisable to protect your credentials.

Conclusion

Password managers have become indispensable tools in today's cybersecurity landscape. They provide strong encryption to protect sensitive data, offer secure password generation, and streamline the login process with features like automatic form filling. By utilizing a password manager, individuals can significantly enhance their online security while simultaneously simplifying management of their numerous online accounts. In an era where data breaches and identity theft are prevalent, password managers serve as an effective defense against cyber threats, ensuring a safer online experience for users. Thus, password managers are secure, invaluable and the safest choice for data protection. While password managers are generally very secure, it is still important to conduct due diligence and make an educated decision. Remember, ongoing proactive measures are key to maintaining robust online security.

References

1. Nicoli, C. (2022a, January 20). Are Password Managers Safe? Forbes. Retrieved June 22, 2023, from https://www.forbes.com/sites/forbestechcouncil/2022/01/20/are-password-managers-safe/?sh=5abadaad6ba1
2. Norton. (2018, August 8). Are password managers secure? Retrieved June 22, 2023, from https://us.norton.com/blog/privacy/password-manager-security#:~:text=Password%20managers%20provide%20strong%20encryption,to%20protect%20its%20sensitive%20data
3. Jančis, M. (2023, March 16). Are password managers safe to use in 2023? Cybernews. Retrieved June 22, 2023, from https://cybernews.com/best-password-managers/are-password-managers-safe/#:~:text=Password%20managers%20can%20be%20hacked,access%20to%20the%20data%20stored
4. Productive Fish. (2023, May 31). Best Password Managers and How Do They Work. Education. Retrieved June 22, 2023, from https://vocal.media/education/best-password-managers-and-how-do-they-work
5. Fibertrain. (n.d.). 10 Types of Cyber Security Threats and How to Prevent Them. Retrieved June 22, 2023, from https://fibertrain.net/10-types-of-cyber-security-threats-and-how-to-prevent-them/
6. McAfee. (2023). What is a password Manager? McAfee. https://www.mcafee.com/learn/what-is-a-password-manager/
7. Newcomb, T. (2022, December 5). Password managers keep getting hacked. Should you still trust them? Popular Mechanics. https://www.popularmechanics.com/technology/security/a42138203/should-you-trust-password-managers/
8. Lapienytė, J. (Ed.). (2023, January 10). LastPass hack aftermath: Can we trust password managers? Cybernews. Retrieved January 1, 2023, from https://cybernews.com/security/lastpass-hack-can-we-trust-password-managers/
9. What is a password manager? | Malwarebytes. (n.d.). Malwarebytes. https://www.malwarebytes.com/what-is-password-manager
10. Blue, Ocean. (2023, March 16). Can you trust password managers after the LastPass hack? Medium. https://mr-oceanblue.medium.com/can-you-trust-password-managers-after-the-lastpass-hack-bf6c47195c9
11. NIST Special Publication 800-63-3. (2017, June). Retrieved June 27, 2023, from https://pages.nist.gov/800-63-3/sp800-63-3.html

Ransomware Unveiled: Navigating Trends, Causes, And Defense Strategies

By | Nur Shafiqah Binti Nor Aztawakal

Imagine waking up one morning and you suddenly find that your computer has been locked out. A message on the screen demands a payment in exchange for unlocking your computer and restoring access to your personal photos, work documents, and cherished memories. This is not a hypothetical scenario. It is a real and present danger which could happen to any of us in an increasingly interconnected world.

Ransomware attacks are becoming increasingly common and has emerged as one of the most significant and damaging cyber threats in recent years. It is a type of malicious software (malware) that encrypts the victim's files or locks their entire system, rendering it inaccessible until a ransom is paid to the attackers. In 2021, there were over 300,000 ransomware attacks worldwide. These attacks are not just targeting large corporations but also small businesses and individuals. The rise of ransomware cyber-attacks has cast a dark shadow over the digital landscape. With the development and rapid changes in the use of internet, ransomware is likely to increase in number and cause wide spread damage.

Evolvement of Ransomware

Ransomware has evolved over the years, becoming more sophisticated and posing greater risks to individuals, businesses, and even countries. The attack often begins with phishing emails or social engineering techniques. Attackers send fraudulent emails that appear legitimate, tricking users into clicking on malicious links or downloading infected files and attachments. Once the ransomware is executed, it starts encrypting files throughout the network.

When ransomware takes on a Service (RaaS) model, the attacks shift from individual to organization and even state level, which has significantly amplified its threat. As ransomware attacks become more sophisticated and profitable, this trend is likely to continue into the future. Organizations need to be aware of such threats and take concrete steps to protect themselves from these attacks.

The threat of ransomware is constantly evolving, making it difficult to defend against. A multi-faceted approach is therefore needed to address this threat, including improved cybersecurity measures, user education, international cooperation among law enforcement agencies, and efforts to disrupt the infrastructure and financial networks that support ransomware operations.

Below is the summary of statistical findings from **BlackFog** statement in 2022 on global ransomware attack:

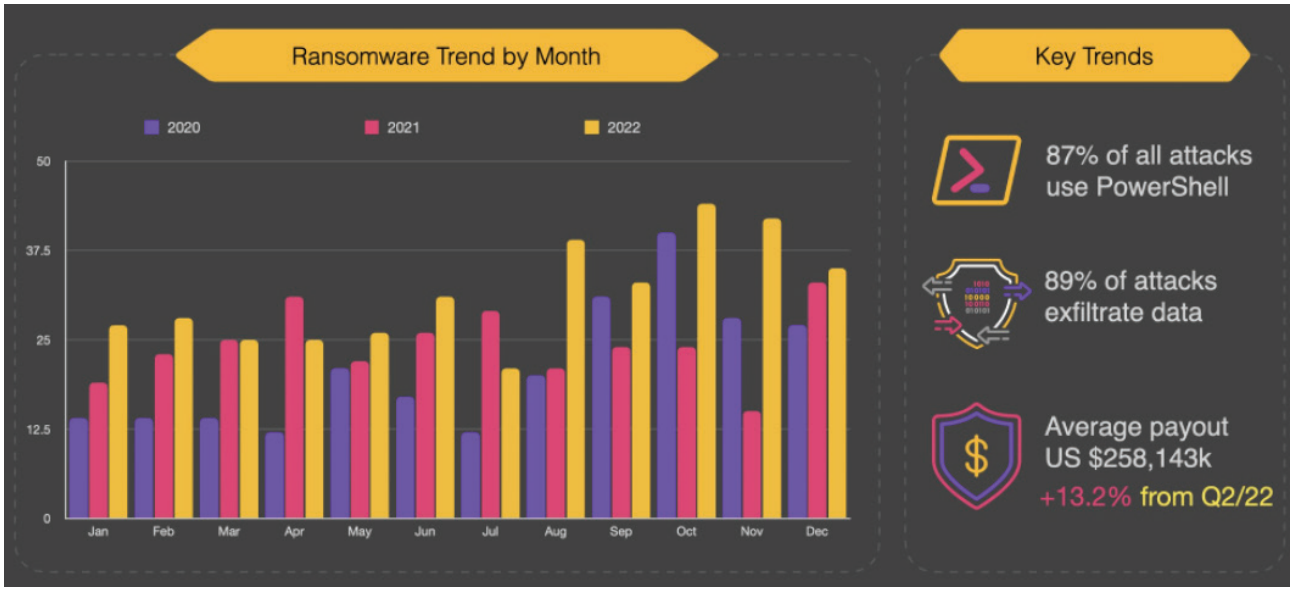


Figure 1: The State of Ransomware in 2022
Source: blackfog.com

An incident related to ransomware attack was reported on April 17, 2022 in Costa Rica. The country became the victim of a major ransomware attack by an assailants group known as Conti. The hackers initially targeted the Ministry of Finance, which announced the breach on Twitter the following day. The attack quickly spread to other government agencies, including the Ministry of Public Security, the Ministry of Health, and the Social Security Fund.

According to Costa Rica's President Chaves, Conti upped their ransom demand from $10 million to $20 million, probably believing that the harm they had done was sufficient to get the government to yield. At the same time, the hacking group urged Costa Ricans to exert pressure on their government to pay the demanded sum, threatening to delete the recovery keys and leave the government and citizens stranded if the ransom was not paid by the due date.

Root Cause of Ransomware

The surge in ransomware attacks can be linked to shortcomings in the technical safeguards employed by organizations. This scenario arises when organizations neglect to implement and sustain proper security measures, resulting in vulnerabilities that malicious actors can leverage. Deficient technical safeguards encompass various factors, such as outdated software, insufficient management of software updates, weak authentication methods, inadequate division of networks, and the absence of resilient backup systems. These deficiencies foster an environment where ransomware attackers can readily infiltrate and disseminate their malicious software. Consequently, the rise in ransomware attacks can be attributed to an organizations' failure to establish and uphold effective technical safeguards, rendering them susceptible to the continually evolving tactics by cybercriminals.

Additionally, human error, such as poor security practices, lack of cyber security awareness, or negligence, can also be a significant root cause of cyber-attacks. This can include actions such as clicking on malicious links or attachments, falling for phishing scams, using weak passwords, or misconfiguring systems. These mistakes typically encompass careless actions or lapses in judgment made by employees, which cybercriminals readily pounce on to infiltrate an organization's systems and initiate ransomware attacks. Other than that, social engineering involves manipulating individuals into performing actions or revealing sensitive information. Attackers could employ various tactics such as phishing emails, phone calls, or impersonation to deceive individuals and gain unauthorized access to systems or steal valuable data. Human susceptibility to manipulation is a significant factor in the success of social engineering attacks.

The Costa Rica ransomware attack, which was a successful attempt to extort money from the government, could be a precursor to similar attacks in the future. The complexity in Conti's legal case and as a country extends beyond the focus on Costa Rica being randomly targeted. A study shows that Costa Rica's vulnerabilities in terms of network and infrastructure played a significant role in making it vulnerable as a target. Despite its geolocation in a region often characterized by instability, Costa Rica has consistently remained a steady native boasting an exemplary record of democratic governance and effective public services.

Impact of Ransomware War

The immediate impact of a ransomware attack is the loss of access to critical data and systems. This can cripple businesses and even a country, disrupting their operations and causing significant financial losses. The encrypted data becomes inaccessible, leading to delays, downtime, and reputational damage.

In addition to the direct financial impact, organizations may also incur costs related to rebuilding efforts. This includes investigating the attack, restoring the data and information from compromised systems and subsequent implementation of stronger security measures to curb future incidents. These expenses can be significant and add further strain to an already challenging situation.

Overall, the impact of a ransomware attack is multifaceted and can have long-lasting effects on businesses, individuals, and even the wider economy. It underscores the critical importance of proactive cybersecurity measures, such as regular system updates, robust backup, and a comprehensive incident response plan in order to mitigate the risks associated with such attacks.

In the previous case of Costa Rica’s President Chaves, refusal to pay ransom after a cyber-attack. In response, Conti, the attacker group, disclosed 97% of information of the hacked website. This caused disruption in domestic services, impacting imports and exports, resulting in around $38 million in daily losses. The attack completely

halted the nation's trade, severely affecting commerce. Additionally, the ransomware attack negatively impacted data in over 800 servers belonging to the finance ministry.

In addition, more than 30,000 medical appointments had to be rescheduled, and tax payments were also affected. Due to the attacks, millions have been lost forcing personnel at affected organisations to resort to using paper and pen to complete tasks.

Meanwhile, the second attack unleashed chaos and destruction on May 31. The systems of the Costa Rican Social Security Fund (CCSS), which organizes health care, were taken offline, plunging the country into a further disarray. According to Brian Krebs, a Security Journalist, the attack left a devastating impact on people's lives. Health care systems were brought to a standstill. This caused widespread chaos and disruption with many left without access to essential services. Consequently, individuals seeking medical attention reported instances of treatment postponements, compelling CCSS to issue alerts to parents whose children were in the midst of surgical procedures, cautioning them about potential difficulties in locating patients.

As the newly elected president of Costa Rica, President Rodrigo Chaves Robles was forced to declare a **national state of emergency** due to the nation's month-long struggle with ransomware attacks which badly damaged its economy.

Evolving Security Countermeasures

As ransomware attacks continue to evolve and become more sophisticated, countermeasures must be put in place to effectively combat this threat. This requires a multifaceted approach. Organizations and individuals should prioritize regular data backups stored offline or in isolated environments. Endpoint protection tools, such as antivirus software and behavioural analysis systems, must be deployed to detect and block malware signatures and suspicious behaviour. Additionally, multi-factor authentication must be implemented to add an extra layer of security, and network segmentation to limit the spread of ransomware. Organisations can significantly enhance their security posture and lessen the risk of data breaches and other cyberattacks by combining multi-factor authentication with network segmentation. These steps form part of a defence-in-depth approach, which employs many levels of security to safeguard sensitive data and valuable assets.

In the meantime, intrusion detection and prevention systems (IDPS) should be activated to monitor network traffic in real-time while incident response plans outline proper procedures for containment and restoration. Implementing such countermeasures in a layered approach creates a robust defence against evolving ransomware threats. These programmes are designed to spot malicious or suspicious activity on a network and take the necessary precautions to block or lessen such dangers.

Conclusion

A ransomware attack could leave organizations and individuals alike with severe consequences. Cybersecurity awareness is crucial to mitigate the ransomware risk and hasten recovery. Immediate steps should be taken to isolate infected systems, shut down affected servers or networks, and disconnect compromised devices from the network. It demands a comprehensive and proactive approach that encompasses robust technical defences, well-defined incident response plans, and a commitment to constant improvement.

By implementing stringent security measures, fostering a culture of cybersecurity awareness, and maintaining an adaptable strategy that evolves with the threat landscape, organizations can effectively reduce their vulnerability to ransomware attacks. Through these collective efforts, the exposure to devastating consequences can be significantly minimized, thereby safeguarding critical data, systems, and the overall integrity of operations.

References

1. Matt Burgess. (2022, June 12). Conti's Attack Against Costa Rica Sparks A New Ransomware Era. Retrieved 14 July 2023, from https://www.wired.co.uk/article/costa-rica-ransomware-conti
2. Sangfor Technologies. (2022, June 28). Conti Ransomware Attack Throws Costa Rica into a National State of Emergency. Retrieved 14 July 2023, from https://www.sangfor.com/blog/cybersecurity/conti-ransomware-attack-throws-costa-rica-national-state-emergency
3. Latino. (2023, June 26). Costa Rica 'Under Assault' is a Troubling Test Case on Ransomware Attack. Retrieved 14 July 2023, from https://www.exemplars.health/-/media/files/egh/narrative-pdfs/costa-rica/overview/costa-rica-under-assault-is-a-troubling-test-case-on-ransomware-attacks.pdf
4. James Purtill. (2022, June 4). Costa Rica is 'At War' With Russian Hackers and Other Countries Will Be Next, Experts Warn. Retrieved 14 July 2023, from https://www.abc.net.au/news/science/2022-06-04/costa-rica-at-war-with-russian-hackers-cyber-criminals/101116930

Achieving Cybersecurity Excellence – The Role Of Project Management In The Cybersecurity Industry

By | Mohd Haleem Bin Abdul Sidek & Ameerul Aziz Bin Thaib

The cybersecurity industry is evolving rapidly, confounding organizations with a variety of complex challenges that require a methodical and systematic approach to address. In this context, effective project management is essential for the success and resilience of cybersecurity projects. This article explores the importance of project management in the cybersecurity industry, assessing the complex nature of cybersecurity projects and highlighting its roles and benefits in the planning, execution, and effective overseeing of cybersecurity projects. By implementing efficient project management practices, organizations can ensure a successful implementation of cybersecurity initiatives, risks mitigation, optimized resource utilization, and overall operational efficiency improvement.

Complex Nature of Cyber Security Projects

Cyber security and information security is one of the fastest-growing industries in the world, as new threats and challenges emerge every day. Cybersecurity projects are complex and multifaceted, with a wide range of objectives, scopes, and stakeholders. Project management in the cybersecurity domain presents unique challenges that require specialized skills and approaches due to the complex nature of security projects. The role of a Project Manager is assisting an organization to achieve their goals by managing complex projects that require coordination across multiple integrated technology areas, teams, and stakeholders.

One of the biggest challenges in cyber and information security is the dynamic and ever-evolving threat landscape. New cyber threats and attack vectors are constantly evolving, and this dynamic nature makes it challenging to accurately predict and prepare for potential risks. There are many contributing factors to the dynamic threat landscape, which include the increasing complexity of tools and cyber-attack methods, the availability of networks that enhance and profit from cyber-security attacks, such as the Dark Web, and the rapid development of new hardware and software. Organizations must stay updated with the latest threat intelligence and modify project plans accordingly to protect their systems and data.

Another major challenge in managing projects in the cybersecurity industry is the lack of clarity in the scope definition. Defining the scope of cybersecurity projects is challenging due to the interconnected nature of software systems and networks. Cybersecurity projects are tasked with objectives that go beyond traditional project goals. They aim to safeguard critical information assets, secure systems, and networks, and mitigate cyber threats. It is often difficult to assess the required scope of work for projects which spans across comprehensive security measures, covering various aspects of an organization's security ecosystem. It involves securing networks, implementing access controls, fortifying application security, establishing incident response mechanisms, and ensuring compliance with laws and regulations.

The complexity of technological and regulatory environment is also another major concern in managing the cybersecurity industry. The integration of cybersecurity measures involves sophisticated technical solutions and tools. Furthermore, project requirements are always open to rapid changes due to dynamic evolution of security threats or new cyber compliance regulations. Due to the dynamic nature of cyber threats, governments and regulatory bodies are compelled to continuously update and improve compliance standards. Compliance is not just a legal requirement; it is also a matter of reputation and trust for the company. Technological complexity and ever-changing regulatory environment present monumental challenges in managing cybersecurity projects.

Navigating these challenges, requires project managers in the cybersecurity industry to possess in-depth comprehension of both **project management principles and cyber security concepts.** They need to adapt conventional project management methodologies to meet the

unique requirements of cybersecurity projects while keeping up with emerging threats and technologies.

The Critical Roles Project Managers Play in Managing Cybersecurity Projects

Given the complexity associated with cybersecurity industry, managing critical projects is one of the most difficult responsibilities for any organization. As a result, project managers play a pivotal role in managing cybersecurity projects. Their expertise in project management methodologies, combined with their knowledge of the evolving threat landscape, enables them to successfully guide these initiatives toward success. Cybersecurity project managers need to collaborate with technical specialists and other critical stakeholders of a company to successfully complete their tasks for the organization. This includes defining the project scope, developing and managing the project strategic plans, coordinating with key stakeholders, managing budgets, making sure that all work items and personnel adhere to the necessary security standards, and finally managing the project within a given deadline.

Strategic planning and risk management are essential for effective project management especially in the cybersecurity industry. Project managers are responsible for meticulous strategic planning to lay out the objectives, scopes, and resources required for a project. During the planning stage, they collaborate closely with technical specialists and crucial stakeholders to ensure that all potential risks, compliance requirements, and technical complexities are well defined. Through strategic planning, project goals are aligned with organizational objectives, while risk management identifies and mitigates risks. Project management methodologies provide a structured approach to accomplish these tasks. By engaging stakeholders early in the process, project managers ensure that project objectives are aligned with organizational priorities. This helps ensure cybersecurity initiatives are effective and contribute to the overall success of an organization.

Risk management is another essential part of project management in the cybersecurity sector. Organizations must proactively identify, assess, and mitigate risks to protect their assets and information from cyber threats within a dynamic threat landscape. Project managers, by utilizing project management methodologies, are able to provide a structured approach to risk management and help the organizations to:

- Identify potential risks and vulnerabilities early in the project lifecycle.
- Assess the likelihood and impact of each risk.
- Prioritize mitigation efforts.
- Develop and implement appropriate control and countermeasure strategies.

By leveraging their knowledge of risk management, project managers are able to identify potential threats and vulnerabilities within the project. Organizations can gain valuable insights and perspectives by involving technical stakeholders in risk management to help them make informed decisions about risk tolerance and mitigation strategies, ensuring that security measures are robust and proactive. Organizations must demonstrate commitment in addressing security risks in compliance with regulations by evaluating vulnerabilities, estimating the impact of potential threats, and prioritizing countermeasures.

In addition, cybersecurity project managers are responsible to provide the essential management scope. They should clearly define project scopes that encompass various aspects of an organization's security ecosystem. Collaboration with relevant stakeholders is also crucial to ascertain the full requirements of the work needed to establish comprehensive security measures. Project scoping is one of the critical responsibilities for cybersecurity project managers as it will determine the main component of a project. Everything will be done precisely based on project scope.

Project managers need to ensure that the project adhere to relevant cybersecurity industry regulations and complex compliance standards. They need to have fundamental knowledge and collaborate effectively with compliance experts to incorporate legal and regulatory requirements into project planning, which includes privacy laws and data protection regulations. Project managers are accountable to proper documentation, which includes keeping a record of the project's objectives, scope, requirements, and goals. This is done to ensure compliance and security control implementation while safeguarding sensitive data. Project managers are also responsible for a detailed audit trail. Comprehensive audit trail is a cornerstone of compliance as it is mandatory to record project activities, verify security, and implement access control. During audits or inquiries, they serve

as proof of compliance efforts, demonstrating responsibility and adherence to regulations.

The above are major responsibilities expected of cybersecurity project managers to help organizations, manage a complex cybersecurity project. Their capabilities to balance technical expertise with project management acumen, adapt to rapid changes, foster collaboration, and ensure compliance positions them as critical point in safeguarding digital assets and triumphant project outcomes.

Benefits of Effective Project Management in Cybersecurity Industry

Project management offers a host of benefits that aid organizations in achieving their goals. It ensures that projects are in sync with organizational objectives, thereby enhancing the probability of achieving the desired results. Efficient distribution of resources, namely time, finances, and human resources, is facilitated through project management, thus resulting in reduced inefficiencies. The early identification and management of potential risks throughout a project lifecycle is critical in minimizing the repercussions of unforeseen challenges. It establishes effective communication channels between team members, stakeholders, and decision-makers, ensuring holistic understanding of project advancements and objectives.

By incorporating quality checks and monitoring, project management ensures that outcomes adhere to predetermined benchmarks. Precise scheduling and adept time management serve as the foundation for timely project completion, evading potential delays. Constant engagement of stakeholders across a project duration fosters and enhances a project's prospects. Amidst unforeseen fluctuations, transitions are facilitated seamlessly through change management strategies facilitated by project management methodologies. Stringent supervision of project costs lead to financial prudence which will proactively avert budget overruns and ensure optimal resource utilization. The inherent adaptability in project management methodologies enables customization across a spectrum of project domains and industries, facilitating tailor-made applications.

Implementing robust project management practices for cybersecurity initiatives can yield significant benefits for an organization. By fostering a culture of learning from mistakes, such practices not only prevent recurring errors but also realize continuous enhancements in processes, procedures, and project execution. Amid the demanding routines of IT and security experts, comprehensive project documentation creates immense value, not only as a repository of business insights but also to streamline future endeavors, ultimately saving time and resources. A proficient project manager will seamlessly integrate project kickoffs and key learnings as intrinsic components of a successful cybersecurity project, thus ensuring a holistic and refined approach.

Conclusion

Project management plays a pivotal role in ensuring success and resilience in the cybersecurity industry. Through best practices, organizations can navigate cyber challenges and optimize resources well to achieve goals. Project frameworks aid planning, risk management, agility, and teamwork. They also ensure compliance, improvement, and resilience. In an ever changing cybersecurity landscape, prioritizing project management enhances competitive edge to effectively secure all digital assets.

References

1. https://www.linkedin.com/pulse/why-project-management-essential-cyber-security-adrian-rodriguez/
2. https://hitachi-systems-security.com/5-benefits-of-project-management-for-cybersecurity/
3. https://hitachi-systems-security.com/how-to-overcome-common-cybersecurity-project-challenges/
4. https://www.upguard.com/blog/cyber-threat-landscape
5. https://en.wikipedia.org/wiki/Benefits_realisation_management

Stamp Duty In Malaysia

By | Hani Dayana binti Ismail & Azlin binti Samsudin

IStamp duty is a type of tax sanctioned by the Stamp Act 1949 (Act 378) ("the Act"). Stamp duties are imposed on instruments, which convey title to or interest in assets and properties, and not transactions. Instrument is defined by the Act as "every written document".

The rate of stamp duty varies depending on the transacted values and the nature of the document. The Inland Revenue Board (Lembaga Hasil Dalam Negeri "LHDN") determines the rate of stamp duty to be imposed on the instruments, as prescribed in Section 4 of the Act. There are two types of stamp duties, namely ad valorem duty and fixed duty.

For ad valorem duty, the amount payable will vary depending on type and value stated in the instrument or market value of a property, whichever is higher; for example, any instrument of transfer, Memorandum of Transfer (of landed or strata property), Deed of Assignment, service agreement, security documents and tenancy or lease agreements. Instruments without any consideration of the value transacted or the amount stated shall be imposed with fixed or nominal duty which starts from RM10 for each instrument; for example Discharge of Charge or Deed of Receipt and Reassignment, a duplicate or a subsidiary instrument whereby another document i.e., the original or principal/primary instrument has been duly stamped with ad valorem duty, and agreement or contract with no transacted value and/or transfer of interests or rights. Instruments liable for stamp duty are specified in First Schedule of the Act.

Section 47 of the Act states that an instrument is required to be stamped within thirty (30) days of its execution if executed within Malaysia. If the instrument is executed outside Malaysia, it must be stamped within thirty (30) days after it has been first received in Malaysia. The process of assessing stamp duty of an instrument/document is called adjudication. The adjudication process may take some time, depending on whether the supporting documents and details of property have been furnished in the application for adjudication. Upon successful assessment, LHDN will issue a notice of assessment *(Notis Taksiran)* of which payment must be made within thirty (30) days from the issuance of such notice or penalty will be payable for late payment.

The Malaysian Government may provide stamp duty exemption on certain instruments, for example government contracts; or certain exemptions as announced by the government from time to time such as purchase of low-cost houses or purchase of first residential property, etc.

Where instruments are not stamped within the stipulated time provided by the Act, Section 47A of the Act provides that an unpaid instrument will be payable together with the penalty as follows:

a. RM25.00 or 5% of the deficient duty, whichever is greater, if stamped within three (3) months after the time for stamping;
b. RM50.00 or 10% of the deficient duty, whichever is greater, if stamped after three (3) months but not later than 6 months after the time for stamping;
c. RM100.00 or 20% of the deficient duty, whichever is greater, if stamped after six (6) months from the time for stamping.

Stamping is done online at LHDN's Stamp Assessment and Payment System (STAMPS System). Upon successful application and payment of the stamp duty, the official stamp certificate will be issued electronically, which is to be printed and attached to the instrument/ document as proof of the stamp duty paid. Other forms of stamping i.e., via digital franking machine (or impressed/chopped stamping on physical instrument/document) and the revenue stamp (Setem Hasil), which is obtainable from the post office, may still be used. However, LHDN had recently announced that starting from 1 January 2024, the utilization of revenue stamp as stamping method will cease, and all submissions must be completed through the STAMPS System.

The Third Schedule of the Act provides for person who is liable to pay for stamp duty, depending on the instrument involved. For example, for an instrument of a conveyance/transfer, it is the grantee/transferee who is liable to pay the duty; for a lease or tenancy, it is the lessee or tenant.

In Malaysia, signed contracts which are not stamped is still valid and enforceable. The Act is silent on this, however the legal position on the validity of unstamped contract was established

in the case of **Malayan Banking Bhd v Agencies Service Bureau Sdn Bhd & Ors (1982) 1 MLJ 198**, where it was held that the unstamped document only affects the admissibility of the document in evidence and does not invalidate the document.

Section 52 of the Act provides that documents or instruments listed in First Schedule of the Act must be stamped in the manner provided and in accordance to the Act for it to be admissible as evidence in court. The purpose of stamping a contract is to provide protection to the contracting parties, as upon stamping, the document is admissible in the court in case of any dispute. As such, where a contract is subject to Malaysian laws and is subject to enforcement in Malaysia, the party who is relying on the contract as evidence in court is required to ensure adequate stamping of the document as per the Act.

Where a document/instrument is not stamped but required to be tendered as evidence in the court of law in a legal suit, the party relying on such unstamped instrument/document as evidence may get it stamped subject to penalty for late stamping. Section 53 of the Act provides that:

"When the person impounding an instrument under section 51 has by law or consent of parties authority to receive evidence and admits such instrument in evidence on payment of duty and penalty, if any, he shall, as soon as may be convenient, send such instrument, together with the amount of the duty and penalty, if any, paid in respect thereof, to the Collector…"

In conclusion, every written document that prescribes a specific transaction whether with or without value is required to be stamped in the manner provided by the Act and may be submitted to the court of law as evidence.

5 Essential Ways to Boost Your Online Safety

By | Ruhama Bin Mohammed Zain

In our digital world today, cybersecurity is of paramount importance to every netizen across the globe. As technology advances, so do the methods used by cybercriminals to exploit vulnerabilities. This article serves as a guide and reminder about the 5 fundamental cybersecurity practices that must be adopted to significantly enhance online safety.

There are essentially 5 cybersecurity best practices that everybody should try to adopt.

1. **Strong Password Management**

Creating and maintaining strong, unique passwords is the first line of defense against cyber threats. Weak passwords is akin to leaving the front door of your digital home unlocked.

2. **Regular Software Updates**

Outdated software is an open invitation to hackers. Regular updates keep security vulnerabilities patched and ensure your devices are fortified to fend off the latest threats.

3. **Phishing Awareness**

Phishing attacks are among the most prevalent cyber threats. Learn to identify and avoid phishing attempts to protect your personal and financial information.

4. **Safe Browsing Habits**

The Internet is rife with every imaginable danger. Employ safe browsing practices to avoid malicious websites and downloads that could compromise your data.

5. **Safe Social Media Practices**

Your online presence reveals more than you could imagine. Manage your social media settings, be cautious about what you share, and stay vigilant against social engineering attacks.

Let us examine each of the security practices more closely, discovering how to bolster our online security while using the Internet for both business and leisure activities.

1. Strong Password Management

In a digital world filled with accounts and online platforms, your password is your first line of defense against cyber threats. Unfortunately, many individuals still use weak, easily guessable passwords, making them vulnerable to attacks. Strong password management is crucial to prevent unauthorized access to your accounts and protect your personal information.

Creating Strong Passwords: Creating strong passwords involves using a combination of upper and lowercase letters, numbers, and special characters. Avoid using easily guessable information like birthdays, names, or common words. Instead, opt for a mixture of random characters that are difficult to predict.

Password Length: Longer passwords are generally more secure. Aim for a minimum of 12 characters. The longer the password, the more challenging it becomes for attackers to crack.

Unique Passwords for Each Account: Using the same password across multiple accounts is a common mistake that can lead to a cascade of security breaches if one account is compromised. Always use a unique password for each online account.

Password Managers: Keeping track of numerous complex passwords can be daunting. Password management tools, or password managers, are applications designed to securely store and manage your passwords. They also generate strong, random passwords, eliminating the need to remember them all.

Regularly Updating Passwords: Frequently changing your passwords reduces the risk of unauthorized access. Set reminders to update your passwords every few months.

Passphrases: Consider using passphrases – longer combinations of words or sentences that are easy for you to remember but difficult for others to guess. For example,

"LangitBiru#Berlari2Orang" is both strong and memorable.

Multi-Factor Authentication (MFA): While not directly related to passwords, multi-factor authentication (MFA) provides an additional layer of security. MFA requires you to provide two or more pieces of evidence to access an account, such as something you know (password) and something you have (a verification code sent to your phone).

By following these strong password guidelines, you can greatly enhance online security. Investing in strong passwords now can prevent future breaches and headaches.

2. Regular Software Updates

Software updates might seem like an annoying routine chore, but they play a vital role in maintaining the security of your devices and data. Regularly updating your operating systems, applications, and security software is crucial for your protection against cyber threats.

Why Software Updates Matter

1. **Security Patches:** Updates often include patches that fix known vulnerabilities. Hackers exploit these vulnerabilities to gain unauthorized access.
2. **Bug Fixes:** Software updates address bugs and glitches that could potentially compromise your device's performance or stability.
3. **New Features:** Updates can introduce new security features and enhancements.

Updating Your Devices

1. **Operating Systems:** Enable automatic updates for your operating system (Windows, macOS, Linux) to ensure you receive the latest security fixes.
2. **Applications:** Set applications to update automatically whenever possible. If not, regularly check for updates and install them promptly.
3. **Security Software:** Keep antivirus and anti-malware programs up to date. They help detect and prevent various types of threats.

Protecting Mobile Devices

1. **Smartphones and Tablets:** Regularly update the operating system and applications on your mobile devices.
2. **Apps:** Only download apps from official app stores, as they have undergone stringent security checks before being published.

Benefits of Regular Updates

1. **Defense Against Cyberattacks:** By staying up to date, you reduce the risk of falling victim to attacks that target known vulnerabilities.
2. **Data Privacy:** Updates often include improvements in data privacy, helping you control how your personal information is used.
3. **Enhanced Performance:** Software updates can improve the overall speed, functionality, and user experience of your devices.

Cautions and Best Practices

1. **Automatic Updates:** Enable automatic updates for your operating systems and applications to ensure you're always protected.
2. **Be Wary of Phony Updates:** Only download updates from official sources. Avoid clicking on pop-ups or links claiming you need to update immediately.
3. **Backup:** Before applying major updates, back up your important data to prevent loss in case of unforeseen issues.

Regular software updates are a fundamental aspect of maintaining your digital security. By keeping your devices and software up to date, you are actively reducing the risk of falling prey to cyber-attacks and ensuring a safer and smoother digital experience.

3. Phishing Awareness

Phishing is a deceitful cyber-attack where attackers masquerade as legitimate entities to trick you into divulging sensitive information such as passwords, credit card numbers, or personal details. Being vigilant about phishing is crucial to avoid falling victim to these deceptive tactics.

Recognizing Phishing Attempts

1. **Suspicious Sender:** Be cautious of emails, messages, or links from unknown or unexpected senders. Verify the sender's email address carefully.
2. **Urgent Language:** Phishing emails often create a sense of urgency, pressuring you to take immediate action.
3. **Generic Greetings:** Phishing emails might

use generic greetings like "Dear User" instead of addressing you by name.
4. **Mismatched URLs:** Hover over links before clicking on them to see where they lead. Beware of URLs that look slightly off or use domains that are similar to legitimate ones.
5. **Spelling and Grammar:** Poor grammar and spelling mistakes can be a sign of phishing attempts.

Avoiding Phishing Attacks

1. **Verify Requests:** If you receive an email requesting sensitive information, do contact the organization directly using their official contact information to verify the request.
2. **Don't Click, Verify:** Instead of clicking on links in emails, visit websites by typing the URL into the browser directly or using bookmarks.
3. **Check SSL Certificates:** Before entering any personal information on a website, ensure it has a valid SSL certificate, indicated by "https://" and a padlock icon in the address bar.
4. **Keep Software Updated:** Ensure your operating system, browser, and security software are up to date to benefit from the latest security patches.

Examples of Phishing Scenarios

1. **Fake Login Pages:** Attackers create fake login pages that mimic legitimate websites. When you enter your credentials, they steal your information.
2. **Emergency Scams:** Phishing emails might claim that your account has been compromised and urge you to provide sensitive information to "verify" your identity.
3. **Financial Fraud:** Phishers pose as financial institutions, requesting account information to supposedly resolve an issue.
4. **Shipping Notifications:** Fake shipping notifications may trick you into clicking a malicious link or opening a malware-laden attachment.

Preventive Measures

1. **Education:** Regularly educate yourself and your colleagues/family about phishing techniques and their indicators.
2. **Email Filters:** Enable email filters to stop and quarantine potential phishing emails.
3. **Report:** If you encounter a phishing attempt, report it to the organization being impersonated and relevant authorities.

Phishing attacks continue to evolve, becoming more sophisticated and harder to detect. Staying informed and remaining cautious are essential to safeguard your personal and financial information from falling into the wrong hands.

4. Safe Browsing Habits

The Internet is a vast digital landscape filled with valuable information and resources, but it's also home to potential risks. Developing safe browsing habits is essential to protect your personal data, privacy, and ensure overall digital security.

Using HTTPS

1. **Look for HTTPS:** When browsing websites, always look for the "https://" prefix in the URL. This indicates a secure, encrypted connection.
2. **Avoid Unsecured Sites:** Avoid websites that lack HTTPS, especially when entering sensitive information like passwords or credit card details.

Beware of Suspicious Links and Pop-ups

1. **Don't Click on Unknown Links:** Be cautious about clicking on links from unfamiliar sources, especially in emails, messages, or advertisements.
2. **Verify Links:** Hover over links to preview the destination URL before clicking. Be cautious if the link seems unrelated or suspicious.
3. **Pop-up Blockers:** Enable pop-up blockers in your browser to prevent malicious pop-ups that might lead to phishing sites or malware.

Public Wi-Fi Safety

1. **Use Secure Networks:** When using public Wi-Fi, connect to networks that require a password or are provided by trusted sources.
2. **Use a VPN:** If you must use public Wi-Fi, consider using a Virtual Private Network (VPN) to encrypt your Internet connection and protect your data from potential spying.

Downloading Files and Software

1. **Be Cautious:** Only download files and software from reputable sources. Avoid downloading cracked software or files from unofficial websites.
2. **Scan Downloads:** Use security software to scan downloads for malware before opening them.

Regularly Update Browsers

1. **Keep Browsers Updated:** Browsers receive updates that include security patches. Regularly update your browser to benefit from these improvements.
2. **Security Plugins and Extensions:** Install reputable security plugins or extensions for your browser. These tools can provide additional layers of protection by blocking malicious websites, phishing attempts, and other online threats. Keep these plugins/ extensions up to date as well to ensure they provide the latest security features.

   By updating your browser and its security plugins/extensions regularly, you enhance your online security against the latest vulnerabilities and exploits.

Safe browsing habits are essential to maintaining your online security. By adopting practices such as using secure websites, being cautious with links and downloads, and avoiding risky public Wi-Fi networks, you can significantly reduce your risk of falling victim to cyber threats. Remember that vigilance and awareness are key in creating a safer online experience.

5. Safe Browsing Habits

Social media platforms provide a convenient way to connect and share, but they can also expose you to various security risks if not used cautiously. By adopting secure social media practices, you can safeguard your personal information and protect yourself from potential cyber threats.

Privacy Settings

1. **Review Settings:** Regularly review and adjust your privacy settings on social media platforms. Limit who can see your posts, profile information, and friend lists.
2. **Friend Requests:** Be cautious when accepting friend requests from unknown individuals. Scammers often create fake profiles from gathering other people's personal information.

Oversharing

1. **Limit Information:** Avoid sharing sensitive personal information publicly, such as your home address, phone number, and financial details.
2. **Vacation Updates:** Refrain from sharing real-time updates about your vacations, as this can signal that your home is vacant and becomes an easy target for burglars.

Social Engineering

1. **Be Skeptical:** Be wary of messages from friends or contacts asking for money or personal information, especially if the request seems unusual or out of the ordinary.
2. **Verify Requests:** If you receive a message requesting sensitive information or funds, contact the person through a separate channel to verify its legitimacy.

Avoid Clicking Suspicious Links

1. **Malicious Links:** Be cautious in clicking on links shared on social media, especially if they come from unknown sources. These links could lead to phishing sites or malware.
2. **Double-Check Shortened URLs:** If you encounter a shortened URL (e.g., bit.ly), use online URL expanders to reveal the full link before clicking. This extra step helps you verify the destination and minimize the risk of landing on malicious websites.

Taking the time to expand shortened URLs before clicking adds an extra layer of caution and reduces the chances of falling victim to phishing or malware-laden links.

Log Out of Shared Devices

1. **Public Computers:** When using a shared or public computer, remember to log out of your social media accounts to prevent unauthorized access.
2. **Use Private Browsing Mode:** When using shared or public computers, utilize private browsing or incognito mode. This mode does not store your browsing history, passwords, or other sensitive information after you close the browser, reducing the risk of your data being accessed by others.

   Using private browsing mode adds an extra layer of privacy protection when using shared computers, as it prevents the storage of your browsing activity and credentials after your session ends.

Beware of Scams

1. **Offers and Contests:** Be cautious of offers, contests, or giveaways that require you to provide personal information. Verify the legitimacy of such promotions.
2. **Trust Your Instincts:** If an offer or message

seems too good to be true, or if you feel pressured to take immediate action, take a step back and trust your instincts. Scammers often rely on creating a sense of urgency to catch victims off guard.

Trusting your instincts and exercising caution when encountering offers or messages that seem too good to be true can prevent you from falling victim to scams and fraudulent schemes.

Secure social media practices are crucial in maintaining online privacy and digital security. Practising mindfulness in sharing information and configuring privacy settings as well as scepticism on messages and links would ensure you enjoy social media with minimal cyber risks. Taking a proactive approach in maintaining your online presence helps ensure a safer and more enjoyable user experience across social platforms.

Conclusion

As technology continues to weave through our lives, the importance of cybersecurity cannot be overemphasized. Implementing the above 5 cybersecurity best practices empowers you to navigate the digital realm safely and confidently. By taking a proactive approach, you not only protect your personal information but contribute to a more secure online ecosystem for all.

References

1. Zilka, G.C., 2019. eSafety and sharing habits with family and friends among children and adolescents. Child and Adolescent Social Work Journal, 36, pp.521-535.

2. Reeder, R.W., Ion, I. and Consolvo, S., 2017. 152 simple steps to stay safe online: Security advice for non-tech-savvy users. IEEE Security & Privacy, 15(5), pp.55-64.

3. Akhawe, D. and Felt, A.P., 2013. Alice in warningland: a {Large-Scale} field study of browser security warning effectiveness. In 22nd USENIX security symposium (USENIX Security 13) (pp. 257-272).

4. Sandella, C. 2023. Protect Yourself Online with Safe Browsing Habits, Seton Hall University, viewed 28 Aug 2023, <https://www.shu.edu/technology/news/safe-browsing-habits.html>

5. Panda Security, n.d. Top 10 tips for safer, more secure web browsing, viewed 28 Aug 2023, <https://www.pandasecurity.com/en/mediacenter/mobile-news/tips-browsing-safer/>

6. vcpi, n.d. 10 Best Practices for Secure Web Browsing for Senior Living Communities, viewed 28 Aug 2023, <https://www.vcpi.com/best-practices-for-secure-web-browsing/>

Jenis-Jenis Scam Shopee Yang Perlu Diketahui Dan Dielakkan

By | Nur Haslaily Mohd Nasir & Alifa Ilyana Chong Abdullah

Kes penipuan kewangan dalam talian menunjukkan jumlah kerugian yang tinggi di Malaysia. Justeru, kerajaan telah mewujudkan Pusat Respons Scam Kebangsaan *(National Scam Response Centre, NSRC)* dengan usaha sama antara Pusat Pencegahan Jenayah Kewangan Nasional *(National Anti-Financial Crime Centre, NFCC)*, Polis Diraja Malaysia (PDRM), Bank Negara Malaysia (BNM), Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM) serta institusi kewangan dan industri telekomunikasi bagi membanteras penipuan kewangan dengan lebih cepat dan berkesan. Menurut statistik NSFC dalam tempoh 5 bulan beroperasi (12 Oktober sehingga 28 Februari 2023), sebanyak 20,881 panggilan yang diterima oleh talian 997. Jumlah kerugian yang dilaporkan adalah sebanyak RM68.5 juta.

Pandemik Covid-19 dengan perlaksanaan Perintah Kawalan Pergerakan (PKP) sedikit sebanyak menyebabkan rakyat Malaysia terpaksa mengubah gaya hidup dan tingkah laku pembelian daripada kaedah membeli-belah secara tradisional kepada pembelian secara atas talian kerana bimbang dijangkiti wabak tersebut. Penipu *(scammer)* juga pandai menyesuaikan diri dan mengeksploitasi peluang yang ada. Shopee sebagai salah satu platform e-dagang terbesar di Asia Tenggara bagi tahun 2021, dengan 343 juta pelawat bulanan juga tidak dapat lari daripada ancaman penipuan atas talian oleh pelbagai jenis *scammer*.

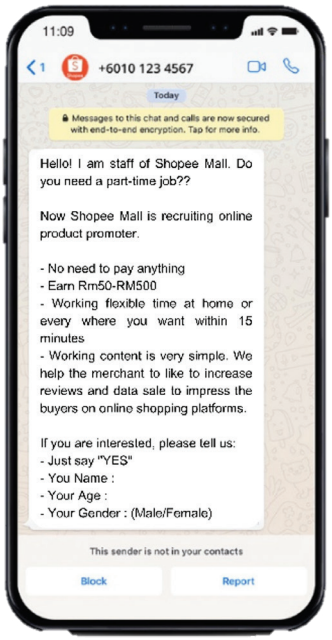
Pelbagai modus operandi yang dirancang untuk memperdaya mangsa dan sentiasa berubah mengikut keadaan dan teknologi. Berikut disenaraikan lima jenis scam Shopee yang sering berlaku dan bagaimana cara untuk mengelakkan diri daripada menjadi mangsa:

1. Scam Pekerjaan *(Job Scam)*

MODUS OPERANDI:

- *Scammer* akan menghubungi mangsa melalui platform seperti WhatsApp, Facebook, iklan Instagram atau Sistem Pesanan Ringkas (SMS) yang mendakwa menawarkan peluang pekerjaan.
- Scammer akan mendekati mangsa dengan mendakwa menawarkan ganjaran harian bernilai RM100 hingga RM300 selepas menyelesaikan tugas mudah yang tertentu. Ganjaran juga dijanjikan untuk diberi secara berperingkat.
- Mangsa kemudiannya akan dimasukkan kepada kumpulan chat *(chat group)* untuk diberikan taklimat kerja. Kumpulan chat tersebut konon-kononnya terdiri daripada beberapa 'pekerja' lain, membuatkan ia nampak menarik dan menyakinkan. Walhal, mereka adalah sekutu yang bersubahat dengan scammer tersebut.
- Pada permulaan, mangsa akan menerima sedikit ganjaran dalam bentuk komisen dan akan dibayar dalam tempoh 10-15 minit selepas selesai tugasan yang diberi. Ini salah satu taktik untuk menyakinkan mangsa dan membentuk rasa selamat dengan andaian bahawa penipu tidak akan pernah memberikan wang kepada mangsa mereka.
- Seterusnya, mangsa akan diminta membuat pembayaran sebagai sebahagian daripada prosedur untuk menerima ganjaran hasil daripada tugasan berikutnya.
- Walau bagaimanapun, apabila pembayaran telah dibuat, *scammer* terus tidak dapat dihubungi.

CONTOH MESEJ:



Cara Mengelakkan Diri Dari Menjadi Mangsa Penipuan:

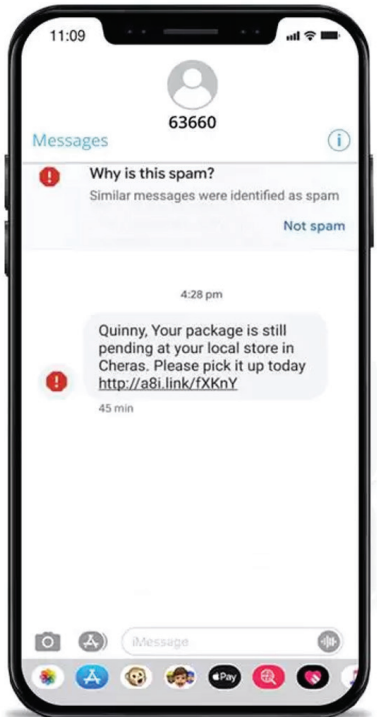
- Jangan mudah terpedaya dengan muslihat tawaran kerja kerana Shopee tidak pernah menggaji mana-mana individu untuk merekrut pekerja melalui platform Sistem Pesanan Ringkas (SMS) mahupun media sosial.
- Shopee tidak akan sekali-kali meminta bayaran pendahuluan daripada pelanggan atau sebaliknya.
- Sentiasa ingat bahawa semua aktiviti berkaitan pembayaran akan dilakukan melalui aplikasi atau laman sesawang Shopee sahaja.
- Apabila ragu-ragu tentang tawaran kerja yang sedang diiklankan, hubungi hr.my@shopee.com untuk mendapatkan penjelasan lanjut sebelum membuat sebarang tindakan.

2. Scam Bungkusan *(Parcel Scam)*

MODUS OPERANDI:

- *Scammer* yang menyamar sebagai syarikat kurier akan menghantar SMS kepada mangsa.
- *Scammer* akan memaklumkan kepada mangsa bahawa terdapat bungkusan yang belum dituntut.
- Mangsa diminta untuk klik pada pautan yang diberikan. Selepas mengklik pada pautan, mangsa akan melihat mesej yang memberitahu bahawa bungkusan telah ditahan atas beberapa faktor seperti caj penghantaran atau cukai yang tidak dijelaskan.
- Mangsa dikehendaki membuat bayaran untuk mendapatkan bungkusan tersebut.
- Setelah mangsa terpedaya dan membuat pindahan wang, scammer tersebut akan hilang dari radar.

CONTOH MESEJ:



Cara Mengelakkan Diri Dari Menjadi Mangsa Penipuan:

- Jangan terburu-buru, pastikan anda semak profil pengirim SMS untuk sebarang kesahihan.
- Anda juga boleh menyemak status penghantaran bungkusan anda pada bila-bila masa di bahagian "Pembelian Saya".
- Status penghantaran bungkusan boleh juga dijejaki mengunakan penjejak bungkusan mengikut syarikat kurier masing-masing.

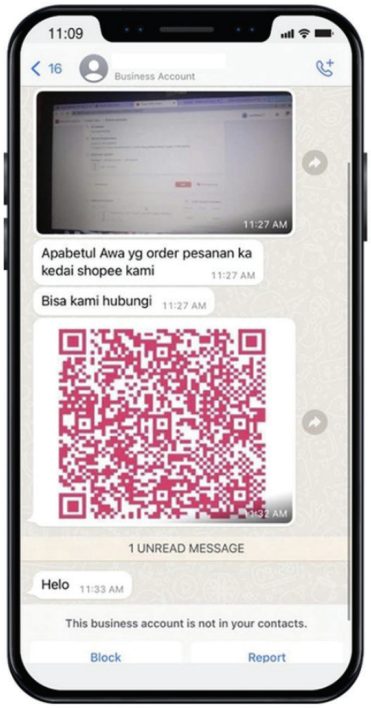
3. Scam QR *(QR Scam)*

MODUS OPERANDI:

- Selepas mangsa membuat pesanan di aplikasi Shopee, penjual akan menghubungi mangsa melalui Shopee chat untuk menawarkan harga yang jauh lebih murah.
- Jika mangsa berminat, penjual akan membatalkan pesanan terdahulu yang dilakukan di aplikasi Shopee.
- Kemudian, untuk meneruskan pesanan baru, penjual akan menghubungi mangsa melalui saluran lain seperti Whatsapp.
- Penjual akan memberikan kod QR Shopee Pay dengan harga promosi berserta arahan untuk membuat pembayaran.
- Setelah mangsa selesai membuat bayaran

- melalui kod QR yang diberi, scammer yang menyamar sebagai penjual itu akan hilang tanpa dapat dihubungi dan pastinya pesanan mangsa tidak akan dipenuhi.

CONTOH MESEJ:



Cara Mengelakkan Diri Dari Menjadi Mangsa Penipuan:

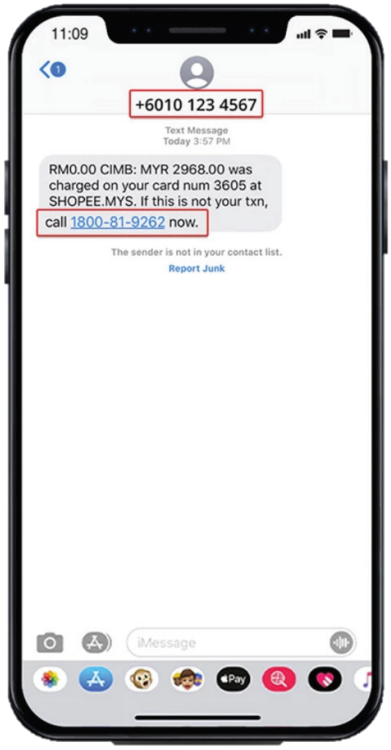
- Jangan mudah terpedaya dengan helah penjual yang menawarkan sesuatu produk pada harga yang lebih murah melalui pembayaran kod QR di luar aplikasi Shopee.
- Jangan sekali-kali berurus niaga di luar aplikasi Shopee dan pastikan semua pembayaran dilakukan di dalam aplikasi Shopee.
- Jangan teragak-agak untuk membuat laporan kepada pihak Shopee sekiranya mangsa dikehendaki membuat transaksi di luar aplikasi Shopee.

4. Scam Butiran Bank *(Bank Details Scam)*

MODUS OPERANDI:

- *Scammer* akan menghantar Sistem Pesanan Ringkas (SMS) kepada mangsa menyatakan akaun bank mangsa telah dicaj dengan jumlah tertentu setelah membuat pembayaran melalui Shopee.
- Diakhir mesej itu ada dinyatakan ayat bahawa sekiranya mangsa tidak melakukan transaksi itu, sila hubungi nombor telefon yang tertera.
- Jika mangsa menghubungi nombor telefon yang dinyatakan di dalam mesej tersebut *scammer* yang menyamar sebagai pegawai bank akan mengangkat panggilan tersebut.
- *Scammer* akan membuatkan mangsa terfikir bahawa butiran kad kredit/debitnya telah disalah guna oleh seseorang untuk melakukan transaksi di aplikasi Shopee.
- Semasa perbualan, mereka akan meminta butiran akaun bank mangsa sebagai pengesahan maklumat.
- Setelah memperoleh butiran akaun yang lengkap, scammer akan mendapat akses penuh ke akaun mangsa dan mencuri duit dari akaun bank mangsa.

CONTOH MESEJ:



Cara Mengelakkan Diri Dari Menjadi Mangsa Penipuan:

- Bertenang, usah panik. Jangan terpedaya untuk terus menghubungi nombor telefon yang tertera dalam SMS.
- Sebarang mesej rasmi dari pihak bank akan dihantar melalui sistem penghantar SMS, bukan dari mesej nombor telefon bimbit persendirian.

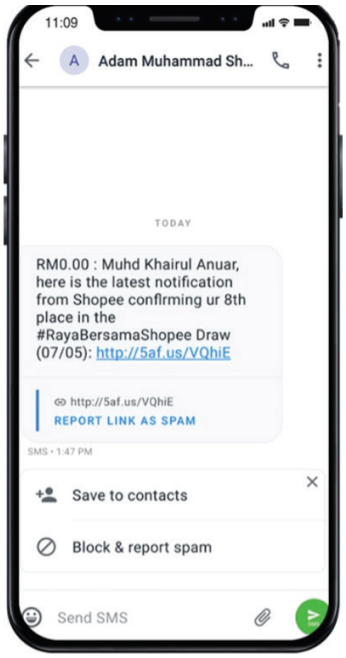
- Semak sama ada mangsa mempunyai akaun dengan bank yang dinyatakan. Jika ada, hubungi nombor hotline rasmi bank tersebut sebagai mana yang tertera di laman sesawang bank masing-masing.
- Jangan sekali-kali berkongsi maklumat peribadi seperti nombor kad pengenalan, butiran kad kredit/debit, Kata Laluan Sekali Guna (OTP) atau nombor Kod Kebenaran Transaksi (TAC) dan sebagainya dengan sesiapa sahaja samada melalui mesej mahupun panggilan telefon.

5. Scam Pembayaran *(Payment Scam)*

MODUS OPERANDI:

- *Scammer* akan menyamar sebagai Shopee, menghantar SMS melalui saluran tidak rasmi yang menyatakan mangsa telah berjaya memenangi sesuatu dari kempen *(giveaway)* Shopee.
- Untuk menuntut hadiah, mangsa perlu klik pautan yang disertakan dalam mesej tersebut.
- Mangsa diminta memasukkan maklumat sulit seperti butiran log masuk dan kata laluan akaun Shopee anda.
- *Scammer* yang mendapat akses penuh daripada butiran log masuk akaun Shopee mangsa boleh menyebabkan ia disalahgunakan untuk transaksi tanpa kebenaran di Shopee mahupun platform lain.

CONTOH MESEJ:



Cara Mengelakkan Diri Dari Menjadi Mangsa Penipuan:

- Jangan klik pada mana-mana pautan yang diberikan kepada anda melalui mesej atau e-mel walaupun ia menawarkan sesuatu yang menarik.
- Tidak menjawab permintaan dan tuntutan daripada orang yang tidak dikenali.
- Jangan terus percaya kepada orang yang menghubungi anda melalui saluran tidak rasmi (nombor telefon peribadi atau alamat e-mel bukan korporat).

Bagi mana-mana pelanggan mahupun orang awam yang mendapati diri mereka telah menjadi mangsa penipuan Shopee, boleh hubungi saluran berikut yang bersesuaian:

- Khidmat Pelanggan Shopee atau 03-2777 9222 (Isnin hingga Ahad, 9 pagi – 6 petang termasuk Cuti Umum) untuk mendapatkan bantuan.
- Dail 997 ke The National Scam Response Center (NSRC) untuk melaporkan kes scam (Isnin - Ahad, 8 Pagi - 8 Malam, termasuk cuti umum) atau rujuk laman sesawang NSRC untuk keterangan lanjut: https://nfcc.jpm.gov.my/index.php/en/soalan/mengenainsrc.
- SEMAKMULE, platform PDRM untuk menyemak akaun bank dan nombor telefon yang terlibat dengan jenayah komersial: https://semakmule.rmp.gov.my/
- Infoline CCID (8 Pagi - 12 Tengah Malam), saluran PDRM bagi memeriksa status laporan polis dan mengemukan maklumat mengenai jenayah komersial: 013-211 1222.
- Pusat Tindak Balas Penipuan CCID (8 Pagi - 8 Malam), hotline maklumat PDRM untuk menghantar maklumat atau meminta maklumat mengenai penipuan atas talian: 03-2610 1559 / 03-2610 1599.

Selain daripada lima jenis scam yang disenaraikan di atas, ada pelbagai lagi taktik penipuan melalui aplikasi Shopee. Pengguna boleh juga mengambil sikap sentiasa berwaspada sebelum membuat sebarang pembelian dengan mengenal pasti tanda-tanda mencurigakan seperti mana berikut:

- Produk mewah atau berjenama disenaraikan pada harga yang sangat rendah.
- Imej produk berkualiti rendah, kabur, atau imej yang menunjukkan hanya sebahagian daripada produk.
- Produk mengandungi pautan ke tapak

- sesawang pihak ketiga, yang mungkin merupakan tapak pancingan data.
- Penjual tidak mempunyai laman sesawang rasmi, akaun media sosial atau sebarang tanda bahawa mereka menjalankan perniagaan yang sah.
- Ulasan negatif dan penilaian rendah oleh pelanggan lain terhadap produk yang dijual.

Senarai ini pastinya tidak lengkap. Bagaimanapun, apabila merasa ragu-ragu, jangan teruskan pembelian anda! Sebaliknya, lihat jika anda boleh mendapatkan produk yang diingini daripada penjual sah atau kedai rasmi (Shopee Mall). Semua orang boleh jadi mangsa dan terdedah kepada penipuan atas talian yang mensasarkan orang dari semua latar belakang, umur dan juga tahap pendapatan. Jadi, sentiasalah berhati-hati.

Reference

1. Mengenai NSRC: https://nfcc.jpm.gov.my/index.php/en/soalan/mengenainsrc

2. Online Shopping Safety Tips: https://shopee.com.my/m/online-shopping-safety-tips

3. Jenis Penipuan Scammer! Hati-Hati Anda Mungkin Mangsa Seterusnya: https://www.mcmc.gov.my/ms/media/press-clippings/jenis-penipuan-scammer!-hati-hati-anda-mungkin-man

4. Akauntan Terpedaya Menang Wang Daripada Shopee: https://www.kosmo.com.my/2021/06/12/akauntan-terpedaya-menang-wang-daripada-shopee/

5. MyCert Issues Alert On Scammers Pretending To Be Shopee Employees: https://www.thestar.com.my/tech/tech-news/2022/07/28/mycert-issues-alert-on-scammers-pretending-to-be-shopee-employees

6. Penipuan Dalam Talian Jadi Jenayah Komersil Utama Negara: https://www.bharian.com.my/berita/nasional/2022/06/969890/penipuan-dalam-talian-jadi-jenayah-komersil-utama-negara

Data Masking And Its Significance In Ensuring Data Security

By | Nurfaezah Hanis Halim, Ida Rajemee Ramlee, Muhammad Haziq Aiman Fakhrudin, Syafiqa Anneisa Leng Abdullah, Naqliyah Zainuddin

Overview

ISO/IEC 27001 or better known as the Information Security Management System (ISMS) is an international standard that provides a framework for implementing and maintaining an effective information security management system within an organization. It outlines the requirements for establishing, implementing, maintaining, and continually improving an information system, with the goal of ensuring the confidentiality, integrity, and availability of information assets. A new revision of the standard i.e., ISO/IEC 27001:2022 has been published in October 2022 where 11 new information security controls were introduced. One of the new controls is data masking, a technique used to protect sensitive data by replacing it with fictitious, obfuscated, or masked data.

This control aims to limit the exposure of sensitive data and to comply with legal, statutory, regulatory and contractual requirements [1]. It can be used as one of the effective controls and robust countermeasures to protect valuable information assets and safeguard their sensitive information within the organization. This will help address the mounting challenges faced by organizations where data breaches and privacy concerns have become all too common driven by an ever expanding and digital landscape. The article will discuss the importance and significance of data masking by exploring its common process, techniques as well as real-life applications.

Types of Data

There are many types of information that can be classified as sensitive or confidential data depending on the functionality of the organization/institution. The following are the types of data that are suitable for data masking [2].

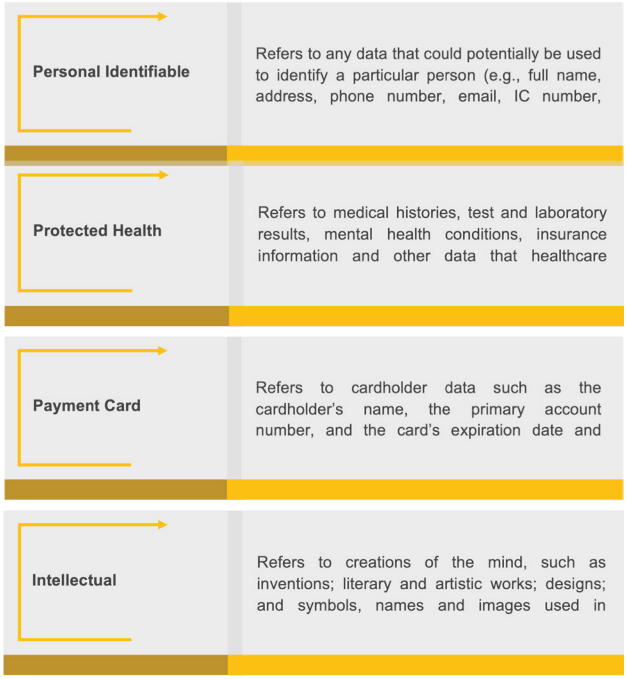


Figure 1: Types of data that require data masking

What is Data Masking

Data masking, in simple terms, is all about disguising sensitive information to protect it from unauthorized access. It involves changing the sensitive data by hiding or replacing certain parts of sensitive data with fake or scrambled values; or replacing some of the digits with asterisks or random numbers while keeping the overall structure intact. In a way, the data still looks realistic but is not the actual information thereby ensuring the original information is protected. This way, even if someone sees the masked data, they cannot easily make sense of it or misuse it. In essence, data masking helps safeguard your sensitive information by making it look different while preserving its usability for authorized users.

Stemming from the above simple explanation, data masking is also referred to as data scrambling and data anonymization. The process involves substituting sensitive information obtained from production databases and replacing it in non-production databases with realistic data

that has been scrambled according to masking rules [3]. Data masking proves to be an optimal solution in instances where confidential or regulated data need to be shared with non-production users. These include internal users e.g. application developers or external business partners such as vendors, customers and suppliers. These categories of users require access to certain original data but do not need complete visibility into every column of every table. This scenario is most appropriate when the information that needs to be retrieved is protected by certain regulations.

In general, there are two main categories of data masking i.e. static and dynamic data masking.

i. Static data masking permanently replaces sensitive data by altering data at rest for instance when data items are masked in the original database. Static data masking is done on a copy of production databases.

ii. Dynamic data masking uses automation and rules to secure data in real-time or on the fly (with data masked in an application's memory). This occurs when sensitive data in transit is replaced leaving the original data-at-rest intact and unaltered.

Data masking is also known as data obfuscation, enabling organizations to generate authentic and fully functional data that exhibits characteristics similar to the original data. However, this is contrary to data encryption where the latter simply hides data, but the data can still be retrieved with appropriate access or key [3]. With data masking, the original sensitive data remains beyond reach and inaccessible.

Why Data Masking?

The main purpose of data masking is to protect sensitive, private information in situations where organizations need to share data with third parties (e.g., developers, software houses, etc.), especially for the purpose of doing data analytics and testing. Data masking will **help organizations meet all levels of compliance, and run constantly, consistently, and efficiently.** Here are several reasons why data masking is essential:

1. Compliance with Legal Requirements

The regulatory environments surrounding the duties and obligations of a data holder to protect the information they maintain are becoming increasingly rigorous in just about every jurisdiction [4]. There are four main legal frameworks that set guidelines for data protection and data privacy i.e., the General Data Protection Guideline (GDPR), the California Consumer Privacy Act (CCPA) and the Health Insurance Portability and Accountability Act (HIPAA), and Payment Card Industry Data Security Standard (PCI DSS) [5]. Data masking helps organizations comply with these regulations by safeguarding sensitive data and ensuring that only authorized individuals can access personally identifiable information.

2. Safeguarding Against Data Breaches

Data breaches can result in severe financial and reputational damage to organizations. By implementing data masking techniques, such as data obfuscation or encryption, organizations can limit access to sensitive data and minimize the risk of unauthorized access, even in the event of a breach.

3. Accidental Exposure

Creating realistic test environments is crucial for software development and quality assurance. However, using actual sensitive data exposes organizations to unnecessary risks. Data masking allows organizations to replace sensitive information with realistic but fictitious data, enabling safer and more compliant testing procedures, outsourcing and collaboration.
When collaborating with external vendors or outsourcing certain operations, sharing sensitive data becomes a necessity. Data masking ensures that shared data does not compromise security or confidentiality, minimizing the risk of data leaks and unauthorized access to allow a more secure testing environment.

4. Facilitate Data Sharing

In organisations, data sharing is essential especially when involving third parties in any outsourced projects or collaboration. Data masking makes data sharing easier as it streamlines the sharing process with larger groups of users which allows access to information while protecting sensitive data. This allows users to use the data without necessarily meddling with the authentic data.

Techniques of Data Masking

The common techniques of data masking are shown in the following diagram

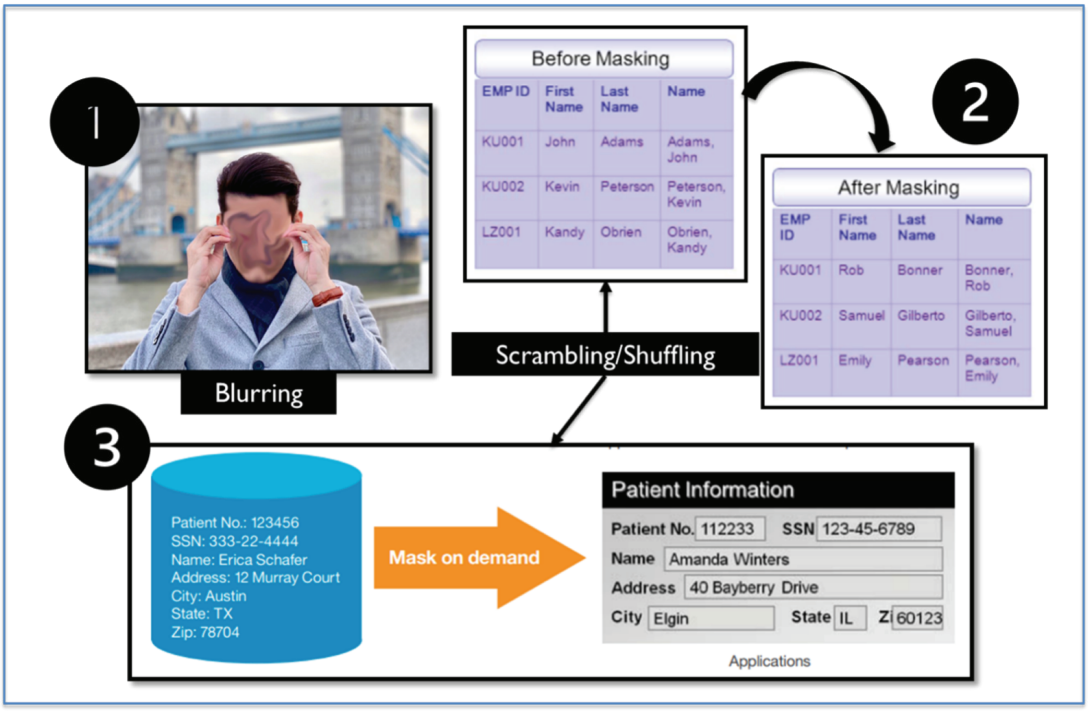


Figure 2: Technique Data Masking Technique

A variety of data management techniques can be used to mask PII and other sensitive data depending on the data type. The primary goal of data masking is to create a version of the data that can be used for development, testing, or analysis purposes while ensuring that sensitive information remains secure and private. In the data masking process, the following are common techniques used.

1. Blurring

Blurring is the process of decreasing precision in order to reduce the potential for data identification. The data can be blurred in a number of ways, such as by breaking it up into smaller categories, distributing the data fields, or incorporating noise into the data records [6]. Consider a scenario when the application uses user age. We can use a numeric blurring algorithm to fill the age field with, for instance, realistic-looking ages by generating random noise within a certain range of ages. The data masking technique of blurring can be applied to safeguard a range of sensitive data. Data can be obscured in this way effectively without becoming meaningless.

2. Shuffling

An algorithm is used to randomly reorganize values inside a column, such as username [5]. For instance, the results will appear accurate, but will not expose any personal information if customer's usernames are mixed together. However, it is essential to prevent the masking process from being reverse engineered. Shuffling is an ideal technique when data links, changes, or statistics must be preserved while still maintaining data privacy and security. This technique is often used for preserving uniqueness, such as email addresses and phone numbers.

3. Substitution

One of the most common techniques for masking sensitive data is substitution, whereby the technique replaces a column of data with similar but unrelated data. Substitution masking is used to replace production data with realistic test data [7]. By replacing one value with another, data is often disguised by changing its meaning—for example, by changing someone's first name from "Kevin" to "James"—while still appearing to be a legitimate data entry. It is important to note that the substitution technique does not expose any personal information or affect data privacy and security.

4. Encryption

Through encryption, the original data is converted into an unreadable ciphertext using complex algorithm. In technical terms, it is the process of converting human-readable plaintext to incomprehensible text, also known as ciphertext [8]. Sensitive data is commonly

protected by encryption from hackers. This technique is suitable for securing data in transit when real-time data usability is not necessary.

1. Tokenization

Tokenization is a procedure that substitutes randomly generated alphanumeric values for the original value. Whenever a user application requests for the original data, the system investigates the token value in the token database retrieves and replaces it [9]. It is one of the ways to ensure data security. Outside the system that produces them, tokens have no significance and do not connect to any other data. Tokenization is commonly used for securing credit card numbers.

Data Masking Best Practices

Ready to start masking your data? Below are some best practices to follow:

i. **Identify data** – Identifying and classifying the types of data that may be sensitive. This action is often carried out by a business or security analyst who is responsible for monitoring a comprehensive listing of organization data elements.

ii. **Assess the situation** – The security administrator is responsible for determining if sensitive information is present, data location and the ideal data masking technique.

iii. **Implement masking technique** – Implementation must take into account architecture, proper planning and future organization needs. Be mindful that it is not feasible for large organizations to assume that a single data masking tool can be used across the entire organization.

iv. **Test data masking results** – Quality assurance and testing are essential to ensure that masking configurations produce the desired results. If not, the database administrator will restore the database to the pre-masked state, modify the masking algorithms and repeat the data masking process once more.

Conclusion

There are a variety of methods that can be used to protect sensitive information. There is no one-size-fits-all solution that can be implemented for all types of data. Therefore, the most appropriate method must be identified to suit the type of data to be protected. Protecting sensitive information is the responsibility of both organizations and individuals.

Incorporating data masking techniques with other data protection security controls is an effective step to intensify your data security efforts. However, it is important to assess your risk and data sensitivity for each data element before selecting the appropriate masking technique and level. With the right approach, data masking can protect an organization from data loss, account compromise, data breach prevention from unintentional or deliberate employee actions, insecure interfaces, data exfiltration or malicious usage of data and therefore, making corporate data more secure.

Reference

1. ISO/IEC 27002:2022 - Information security, cybersecurity, and privacy protection — Information security controls
2. https://www.bmc.com/blogs/data-masking/What's Data Masking?
3. https://docs.oracle.com/database/121/DMKSB/data_masking.htm#DMKSB-GUID-2B0418D5-0D85-4F9B-9A7F-53665681BE25
4. Data Masking: Need, Techniques & Solutions: https://www.academia.edu/19666359/Data_Masking_Need_Techniques_and_Solutions
5. https://www.techtarget.com/searchsecurity/definition/data-masking
6. http://dx.doi.org/10.18608/jla.2016.31.8
De-identification in learning analytics. Journal of Learning Analytics, 3(1), Mohammad Khalil, Martin Ebner (2016). 129–138.
7. https://docs.informatica.com/data-integration/powercenter/10-4-0/transformation-guide/data-masking-transformation/substitution-masking.html
8. https://www.cloudflare.com/learning/ssl/what-is-encryption/
9. https://www.geeksforgeeks.org/difference-between-tokenization-and-masking/
10. https://www.dot-anonymizer.com/resources/infographic/an-introduction-to-data-masking-infographic/
11. https://www.makeuseof.com/what-is-data-masking-and-what-are-its-benefits/
12. https://www.ibm.com/downloads/cas/JGE5XOYY
13. https://www.k2view.com/blog/data-masking-techniques

Engaging Mobile Recovery Services: Safeguarding Your Data And Device Resilience

By | Muhammad Ikhwan Bin Mohammad Faisal

1.0 Introduction

In today's highly inter-connected world, our phones and tablets are like an extension of ourselves. They hold our memories, work records, and messages. But sometimes when things go awry in the digital world, we could lose literally everything from our devices. That's when mobile recovery becomes critical – basically engaging professionals who can help recover lost data from our phones and tablets. Since gadgets have become indispensable in our lives, it is helpful to know the trends in mobile recovery and why so many people need such service.

Our everyday lives and devices are now inextricably intertwined. But occasionally, due to human error, we could lose our valuables such as data. Mobile recovery is like a white knight that saves our day by recovering our lost property. As devices get more sophisticated, data recovery also becomes smarter. Most devices now use biometrics to unlock, so mobile recovery experts need to find smarter ways to circumvent these security features while keeping our secrets safe. Super-fast 5G technology also adds to the complexity of data recovery.

Our world is changing fast, and we rely heavily on our mobile phones and tablets for just about everything – from work to social interaction. Because of this, more people need help to get their lost data from their memorable pictures, important documents, to personal information on their devices. Hence, backing up data is no longer an option.

In this article, we explore the world of mobile device data recovery. We will learn the intricacies of data recovery and why such service is essential. Through such discovery, we can be better prepared to keep our precious data safe.

2.0 Definition and Importance of Mobile Recovery Services

Mobile recovery is a vital process encompassing the retrieval and restoration of lost or inaccessible data from smartphones and tablets. As our handheld devices have evolved into essential extensions of our lives, housing irreplaceable memories, critical work documents, and vital communications, mobile recovery emerges as a vital solution to address unexpected data loss. This intricate process involves employing a range of cutting-edge techniques, including software-based recovery to address software glitches and data-related issues, as well as hardware-based recovery to repair or replace physical components that may have been compromised. The goal of mobile recovery is to ensure a seamless retrieval of valuable data, thereby safeguarding our digital footprints and maintaining continuity of our digital experiences.

Mobile devices contain a vast amount of personal data, including contacts, messages, photos, videos, app data, and more. When a user experiences data loss due to a device malfunction, accidental deletion, or other issues, data preservation ensures the user can recover and continue using their device seamlessly. It prevents disruption in their daily life and preserves user experience. Data preservation in mobile recovery refers to the process of safeguarding and retaining user data from a mobile device to prevent its loss or destruction during the recovery process. When a mobile device encounters issues such as hardware failure, software glitches, accidental deletion, or any other form of damage, data preservation becomes critical to ensure that the user's valuable information remains intact and accessible after the recovery is complete.

It is important to note that not all device issues can be resolved through device functionality restoration. In some cases, severe hardware damage or certain software-related issues may require specialized repair services or, in extreme cases, device replacement. The ultimate goal of device functionality restoration is to bring the mobile device back to its intended working condition, allowing users to use it effectively for their daily tasks, communication, productivity, and entertainment. Mobile recovery professionals or authorized service centers like MyCyberSecurity Clinic (MyCSC), service

provided by CyberSecurity Malaysia, frequently handle device functionality restoration, utilizing their knowledge and experience to provide accurate diagnostics and ensure successful recovery process.

At MyCSC, access to recovery features, backups, and restored data is typically protected by strong authentication mechanisms. Only authorized users could access the data and perform recovery actions. Backup data is stored in secure environments, such as encrypted Network Attached Storage (NAS), servers and local, password-protected devices. These storage locations are intended to prevent unauthorized access. Mobile recovery solutions typically store only the necessary data required for recovery process, reducing exposure of other sensitive information. Furthermore, MyCSC has formulated clear privacy policies that outline how user data is handled, who has access to it, and how they are protected from unauthorized use or disclosure. MyCSC adheres to ISO27001 and ISO17025 in terms of data protection regulations and industry lab standards, ensuring that user data is handled in accordance with applicable laws. All mobile recovery centers should also conduct regular security audits and assessments to identify and address potential vulnerabilities or weaknesses in their systems.

While the above practices are generally followed by reputable mobile recovery solutions, it is also essential for users to choose reliable and trusted providers to ensure data security and privacy. Reading reviews, checking the reputation of the provider, and verifying their security measures are essential steps to seeking a secure mobile recovery solution.

3.0 Type of Mobile Recovery

Software-Based Mobile Recovery is a type of mobile recovery that focuses on resolving issues related to the software and operating system of mobile devices. It involves processes like data backup, data restoration, firmware updates, operating system reinstallation, and app reinstallation. Updating the mobile device's firmware and operating system to the latest versions can help address known issues, bugs, and security vulnerabilities. These updates often include bug fixes and performance enhancements that can improve the overall stability and functionality of a device. Software-based mobile recovery solutions also employ data recovery tools to retrieve accidentally deleted files or recover data from corrupted storage. The recovery is intended to bring the device back to a functional state by addressing software glitches, bugs, or corruption. It could further involve security checks and other procedures to find and mitigate malware or other potential security risks that have affected the device's performance. It is important to note that while software-based mobile recovery can address many issues, it may not be effective if the problem is primarily hardware-related. In such situations, hardware-based mobile recovery or professional device repair becomes necessary.

Hardware-based mobile recovery refers to the process of recovering a mobile device's functionality by addressing issues related to its physical hardware components. This type of recovery is necessary when the device experiences malfunctions, failures, or damage caused by hardware-related problems. It involves repairing or replacing damaged hardware components to restore the device functionality. This type of recovery is typically performed by trained technicians and may require specific tools and equipment. Unlike software-based recovery, which focuses on resolving software glitches and data-related issues, hardware-based recovery deals with physical repairs, replacements, and adjustments of the device hardware components. For instance, the motherboard is a critical component of any mobile device. If it malfunctions due to damage by water, overheating, or other issues, hardware-based recovery entails repairs or replacements of faulty motherboard components. A hardware-based recovery for water or liquid damage involves cleaning and fixing the broken parts to get it working again. It is important to note that hardware-based mobile recovery may incur extra fees, especially if the device is out of its warranty validity period. Users may occasionally need to decide whether repairing of cost-effective compared to buying a new gadget, depending on the severity damage and the condition of the other parts.

4.0 Common Cases That Warrant Mobile Recovery Services

To minimize the risk of data loss, maintain device functionality, and ensure the security of your personal information, best practices in mobile recovery are essential. Here is a brief overview of such best practices.

Accidental deletion of important data, formatting a device without backup, or data corruption can

lead to data loss on a mobile device. Mobile recovery services can employ specialized tools and techniques to recover lost or inaccessible data from the device storage. If your mobile device has been exposed to water or other liquids, it can result in damage to the internal components. Water damage can also cause the device to malfunction or even render it completely inoperable. Furthermore, accidental drop, unintended impact, or other physical incidents can cause damage to a mobile device. It can result in a cracked screen, damaged buttons, or internal components. Mobile recovery services can assess the extent of any physical damage and perform necessary repairs or replacements.

Software-related issues can cause a mobile device to become unresponsive, freeze, or continuously crash, leading to a need for mobile recovery services. Your mobile device could also experience performance problems, data breaches, or unauthorized access to sensitive data if infected by malware or viruses. Mobile recovery services can assist in eradicating harmful software, restoring the device's security, and ensuring the security of your personal data. However, be mindful that during the process of updating an operating system or firmware of a mobile device, errors can occur that would render the device unstable or unusable. Mobile recovery services can also assist in recovering from failed system updates and restore the device to a functional state. A mobile device's failure to start up normally or remain in a boot loop may be an indication of hardware or software issues. Mobile recovery can help identify he problem and take the necessary action to fix the booting issue.

The above can be considered among the more common situations in which mobile recovery services is necessary. Every situation is different, and exactly what services are required will depend on the type of problem and device model. It is recommended that you consult experts or licensed service providers for an accurate diagnosis and effective recovery options.

5.0 Mobile Device Best Practices

One of the best practices to avoid data loss is to routinely backup data on your mobile device. Data loss may be caused by unforeseen hardware failures, software bugs, theft, loss, or damage to the device. When you have a backup, your essential data could be retrieved if needed. Having a backup could also prevent you from having to compensate cybercriminals due to malware or ransomware.

There are several ways to back up your data. Most mobile operating systems come with built-in cloud backup features. Examples include Google Drive for Android smartphones and iCloud for Apple devices. These services enable you to recover your data on a new device and automatically back it up. Additionally, you may transfer your data to an external hard drive or other storage media by connecting your mobile device to a computer. Enable automatic backups if at all possible. This ensures that your data is frequently backed up without needing to remember it yourself. Maintaining numerous backup copies in various locations is most crucial. Consider having both an external hard drive backup and a cloud backup. It protects against the potential for total data loss in the event that one backup process fails.

One of the best practices for handling data on mobile devices is to encrypt the data. Your data is encoded throughout the encryption process so that it can only be accessed with the right encryption key. It adds an additional layer of protection to your data, making sure that even if someone obtains access to your device or files without your permission, they won't be able to read or interpret the information.

Most of the latest mobile devices include a feature to encrypt the entire data. All your data, applications, settings, and files are included in this. To activate complete device encryption, check the device's security settings. For complete device encryption to be effective, make sure you use a strong passcode or biometric authentication (such fingerprints or face recognition) to unlock your smartphone. This guarantees that the decryption key is only accessible by you. For confidential communication, use end-to-end encrypted messaging services. For apps such as WhatsApp and Facebook, do make sure that nobody except you and the intended receiver could view the content, not even the service provider. You may add a strong layer of protection to your mobile device and any sensitive data it contains by adhering to these recommendations and encrypting them. By doing so, you can keep your information safe and private.

Lastly, take comfort that our data can still be retrieved although the mobile device is no longer functional or not been used. With the ever-increasing volume of sensitive information stored on various devices and platforms, the importance of securely erasing data before disposal, resale, or reuse cannot be overemphasized. Ensuring that confidential business data, personal information, and

proprietary content are irreversibly removed helps mitigate the risk of unauthorized access and identity theft. The Data Sanitization Service offered by CyberSecurity Malaysia addresses the need for safe and secure deletion of data from storage devices that are to be retired, upgraded or reallocated. With information security at the core of its service and being the national cyber security specialist agency, MyCSC's effective and trustworthy data sanitization service via multiple customer engagement. Services provided are based on the type of digital storage device, state of the data and level of data sanitization required. The levels of data sanitization span from Logical Sanitization, Digital Sanitization to Analogue Sanitization.

6.0 Conclusion

In a world where our digital lives are deeply intertwined with our mobile devices, mobile recovery becomes critical. The digital realm is not immune to mishaps such as the potential loss of critical data. Mobile data recovery ensures that our lost data can be recovered and restored. It is not just a technical process, but a pragmatic solution that safeguards our digital assets. As devices become more advanced, recovery techniques become more complex involving cloud-based methods and biometric security features. As reliance on mobile devices for work, communication, and leisure deepens, demand for mobile recovery services has skyrocketed. Losing data can drastically disrupt one's life.

In this article, we journeyed through the dynamic world of mobile recovery. We have explored its importance, the types of recovery – whether software or hardware-based – and common scenarios that require mobile recovery services. By understanding key aspects of mobile recovery, we could navigate the digital landscape with more confidence, knowing that our data is recoverable and our digital lives would not be disrupted.

In the ever-evolving digital realm, mobile device best practices from backing up data, protecting against malware to encryption are all essential steps that fortify our data security. Through such practices, we could better protect our digital memories, preserve our vital information, and ensure our mobile devices continue to serve as faithful companions on our journey through digital life.

7.0 Citation

1. Kaluri, Rajesh, et al. "A Structured Analysis and Design of a Mobile Repair Development System Using a Grady Booch Approach." IEEE Xplore, 1 Feb. 2020, ieeexplore.ieee.org/abstract/document/9077793.Accessed 30 June. 2023.

2. Paige, Carl. "Global | Revolutionizing Mobile Repairs: How Technology Is Improving Services." Www.carlcare.com, 23 Mar. 2023, www.carlcare.com/global/tips-detail/role-of-technology-in-mobile-repair-services/. Accessed 5 June. 2023.

3. Rouse, Margaret. "Mobile Recovery." Techopedia, 1 Apr. 2014, www.techopedia.com/definition/29966/mobile-recovery#:~:text=Mobile%20recovery%20is%20the%20process. Accessed 5 June 2023.

4. "Securing Mobile Devices with Mobile Encryption." SecurityMetrics, https://www.securitymetrics.com/blog/securing-mobile-devices-mobile-encryption. Accessed 10 june 2023.

5. Shank, Stefanie. "How to Secure Your Mobile Device in Six Steps | Tripwire." Www.tripwire.com, 28 Mar. 2023, www.tripwire.com/state-of-security/secure-mobile-device-six-steps.

6. "DATA SANITISATION SERVICES." MyCSC, 1 June 2020, mycsc.cybersecurity.my/data-sanitisation-services. Accessed 25 July. 2023.

FAQ On TikTok Concerns Raised In Malaysia

By | Nur Qurratu' Aini Rohizan, Kilausuria Abdullah, and Lukman Hakim Abd Rahman

Governments and organisations in the UK, US, Canada, New Zealand, and the European Commission have banned TikTok on work devices due to security and privacy risks. This FAQ feature concerns raised in Malaysia on TikTok:

Questions:

1. What is your expert opinion on the potential threat that TikTok poses to national security?

There are several potential threats that TikTok poses:

Malicious Content: As with any social media platform, there is a risk of malicious content, such as scams, phishing attacks, and malware, being spread on TikTok. Users may be tricked into clicking links that lead to malicious websites or downloading apps containing malware.

Contribute to spreading harmful or inappropriate content, including hate speech, misinformation, and content unsuitable for all ages. This includes provocative hate speech and sensitivity to royals, religion and race.

Cyberbullying and Grooming: TikTok has a young user base, and there is a risk of cyberbullying and grooming on the app. Cyberbullies may target users with hurtful comments, while groomers may try to establish relationships with minors for harmful purposes.

Exposure to Inappropriate Content: TikTok's algorithmic recommendation system may expose users to inappropriate content, such as violence, sexual content, or extremist content.

Vulnerabilities in the App: As with any software, there is a risk of vulnerabilities in the TikTok app that could be exploited by attackers to gain access to user data or carry out other malicious activities.

Data Breaches: There is always a risk of data breaches on any platform that collects user data, and TikTok is no exception. If a data breach were to occur, it could expose sensitive user information, such as usernames, passwords, and personal information.

2. What is the nature of the threat to Malaysians?

(For example, an intriguing conspiracy theory that suggests TikTok—which an expert in the US calls "digital opium"—exists to make people outside of China dumber while the domestic version—Douyin—is intended to make domestic users smarter.)

We will not comment on the "digital opium" term used by some parties. Overall, the nature of the threat that TikTok poses to Malaysians is similar to those faced in other countries.

However, there may be some specific concerns relevant to the Malaysian context.

a. Privacy and security concerns
b. Inappropriate content
c. Addiction and mental health
d. Cultural concerns related to 3R issues (Race, Religion, Royalty)
e. Misinformation and propaganda
f. Fake news especially related to 3R

TikTok users must be aware of these potential threats and take preventive measures to protect their privacy and well-being while using the app. This may include adjusting privacy settings, limiting time spent on the app, and being mindful of the content they consume and share. It is also important for regulators and policymakers to take steps to ensure that the app is being used responsibly and ethically.

3. Are the concerns (cited by the countries above) in banning TikTok valid? Or is it largely due to "distrust of China and awareness of Chinese espionage has increased"?

How do you perceive these concerns? Are these something Malaysia or countries in the region should be concerned about?

The concerns on banning TikTok are complex and there are arguments both for and against such a ban, including:

a. freedom of expression
b. economic impact
c. impact on users
d. national security concerns
e. risk of retaliation

Overall, while there are valid concerns on both sides of the debate, it is important to consider the potential consequences of banning TikTok carefully. Proper analysis of the risks and benefits should be done while the potential impact on individuals, communities, and the wider economy should also be considered.

4. How does the cybersecurity risk associated with TikTok differ from that of other social media platforms like Facebook, Instagram, Twitter or other China-based apps like Shein?

While other social media platforms such as Facebook, Instagram, and Twitter have also faced data privacy and security concerns, they are not specifically tied to a foreign government. Additionally, these platforms have a more extensive user base, which may make them more attractive targets for hackers.

Secondly, TikTok's algorithmic recommendation system and data collection practices have also been scrutinised. The app collects vast amounts of user data, including location data, device information, and browsing history, which it uses to personalize its recommendations to users. This has raised concerns about how this data is being used and whether it could be accessed by third parties.

Other social media platforms also collect user data, but TikTok's algorithmic recommendation system is unique and has faced scrutiny due to concerns about the potential for algorithmic bias and the amplification of harmful content.

5. What does TikTok actually know about its users? What kind of personal information does TikTok collect from its users, and how is it being used?

Before downloading and installing TikTok, user can read what kind of personal information will be collected. This is available under Data Safety at Google Play Store and App Privacy at the Apple App Store, respectively.

TikTok collects a significant amount of personal information from its users, including:

a. Account Information: This includes a user's name, username, email address, and password.
b. Device Information: TikTok collects device information such as the user's device type, operating system, and network information.
c. Location Information: TikTok collects location information, which includes the user's precise location data, as well as IP address and GPS data.
d. User Content: TikTok collects the content users post on the app, including videos, comments, and likes.
e. Usage Information: TikTok collects information about how users interact with the app, including how long they spend on the app, what videos they watch, and what kind of content they engage with.
f. Other Information: TikTok also collects information from third-party services, such as social media platforms, if a user connects their TikTok account to those services.

TikTok uses this data to personalize the user experience and to serve relevant content. The app's algorithm uses this data to recommend videos that the user may be interested in based on their viewing history and other interactions on the app. TikTok also uses this data for advertising purposes, showing users ads that are relevant to their interests.

6. Are there any other security concerns related to the app?

Yes, there are several other security concerns related to TikTok which is similar to question number 1.

- Malicious Content,
- Contribute to spreading harmful or inappropriate content

- Exposure to Inappropriate Content
- Vulnerabilities in the App
- Data Breaches

7. Is deleting TikTok the best course of action for individuals concerned about their privacy and cybersecurity? How can users protect themselves from potential security risks while using TikTok?

Be vigilant of the potential threats and adhere to security best practices while using TikTok. It is also essential to stay informed about the latest security and privacy risks associated with TikTok and other social media platforms and to take appropriate action to protect sensitive information. Regular patches and upgrades must also be put in place to prevent potential cyber-attacks on official devices. In addition, the TikTok account must be protected by adhering to a strict password management policy. It may be helpful to have regular communication with the local TikTok Provider on any concerns of TikTok and report any suspicious activities concerning TikTok.

8. Is banning Tik Tok from government offices, state offices, as well as campuses a good idea to protect our national security and private information?

Government offices could implement policies and procedures on social media apps usage like TikTok on official devices to mitigate these concerns. This could include restrictions on which devices can be used to access the app, guidelines on what types of content can be posted or viewed, and regular security training for employees. In addition, it would be helpful to inculcate user awareness for employees and publish advisories and best practices to guide employees on engaging with TikTok ethically and responsibly.

9. What are the risks and costs of a ban?

Banning builds up distrust among countries and companies. Other countries may retaliate by banning U.S. companies and the situation could rapidly spiral. There might be some impact on people who make income from TikTok, such as content providers or those selling goods via TikTok. The risk of a ban significantly impact politics, the economy and society.

10. What impact could a TikTok ban have on human rights issues?

A TikTok ban could impact human rights issues both positively and negatively. On the one hand, a ban could limit the amount of personal information collected and shared by the app, which is a positive step for user privacy. On the other hand, a ban could limit the ability of marginalised communities to share their stories and connect with others who have had similar experiences. Additionally, TikTok has been used as a tool for activism and advocacy on a range of human rights issues, and a ban could limit the ability of activists and advocates to raise awareness and mobilize support for their causes. The impact of a TikTok ban on human rights would depend on the specific circumstances and implementation of the ban. But banning apps is an extreme measure that does not meet international human rights standards. It is because under international human rights law, blocking an entire service or application is not regarded as necessary and has even been declared unlawful in several instances.

11. What are some alternative approaches to a TikTok ban that policymakers could consider?

Instead of implementing a TikTok ban, policymakers could consider alternative approaches such as increased regulation and oversight, promoting competition in the social media industry, and incentivising companies to prioritise user privacy and data protection. Another approach could be to address the underlying concerns around national security and data privacy through diplomatic negotiations with China, where TikTok's parent company is based. By pursuing these alternatives, policymakers could mitigate the potential negative consequences of a TikTok ban while addressing the concerns around the app's impact on national security and user data privacy.

12. How can governments balance the need for cybersecurity and privacy with the potential impact of a TikTok ban on individuals and businesses?

Governments can balance the need for cybersecurity and privacy with the potential impact of a TikTok ban on individuals and businesses by implementing a targeted and evidence-based approach to policy-making. This can involve conducting thorough risk assessments to identify specific security threats and taking measures to mitigate them, while also considering the potential economic and social impacts of a TikTok ban. Governments can also work with businesses and industry experts to develop alternative solutions that address security concerns while still allowing individuals and businesses to access the app's benefits. By taking a measured and balanced approach, governments can protect national security and individual privacy while minimising the negative impact of a TikTok ban on individuals and businesses.

13. How can individuals, universities, businesses better regulate and control the use of their personal information on social media platforms?

Individuals, universities, and businesses can take several steps to regulate better and control personal information on social media platforms. These include understanding privacy policies, using privacy settings, limiting personal information sharing, being cautious of third-party apps, educating employees and students, and regularly reviewing and updating privacy settings. By taking these measures, they can better protect their personal information.

8. Is banning Tik Tok from government offices, state offices, as well as campuses a good idea to protect our national security and private information?

Government offices could implement policies and procedures on social media apps usage like TikTok on official devices to mitigate these concerns. This could include restrictions on which devices can be used to access the app, guidelines on what types of content can be posted or viewed, and regular security training for employees. In addition, it would be helpful to inculcate user awareness for employees and publish advisories and best practices to guide employees on engaging with TikTok ethically and responsibly.

Summary

Users must be vigilant of potential threats that TikTok may present and also take active steps to protect their privacy and well-being while using the platform. This may include adjusting privacy settings, limiting time spent on the app, and being mindful of the content they consume and share.

References

1. https://www.bbc.com/news/technology-64797355

2. https://www.nst.com.my/world/world/2023/03/891472/dutch-officials-told-not-install-tiktok?utm_source=nst&utm_medium=mostpoplatest

3. https://www.reuters.com/technology/fbi-chief-says-tiktok-screams-us-national-security-concerns-2023-03-08

4. https://www.nst.com.my/world/world/2023/03/891470/italy-orders-probe-tiktok-over-dangerous-content?utm_source=nst&utm_medium=mostpoplatest

5. https://usa.kaspersky.com/resource-center/preemptive-safety/is-tiktok-safe

How To Build Secure Software: Best Practices In Software Development

By | Izzatul Hazirah Binti Ishak, Nur Syahidah Binti Yunos, Muhammad Imran Bin Mohamad Fauzi

Introduction

As the world becomes more digitalised, the number of cyber-attacks has skyrocketed. The scenario is true in Malaysia, where cyberattacks have been an increasing threat in recent years. According to a CyberSecurity Malaysia study, 9,045 cybersecurity incidents were recorded in 2020, representing a 22.50% increase over the previous year.

Web attacks can have a crippling effect on both individuals and corporations, resulting in reputational and financial losses. To reduce the risk of attacks, developers are compelled to implement best practices and strategies to develop secure software. By the end of this article, developers will acquire a better understanding of the challenges in protecting against web attacks and necessary steps to create secure software to realise a more secure digital environment in Malaysia.

Challenges

Building a completely secure software is a formidable challenge considering developers must contend with a variety of complex and dynamic factors that can undermine software security. Here are some of the most significant challenges that developers face when attempting to build secure software:

1. **Addressing Vulnerabilities in Legacy Systems:** Many organizations still rely on legacy systems developed before implementation of modern security standards. These systems can be particularly challenging to secure, as they are built with inherent vulnerabilities that are difficult to detect and remediate.

2. **Time and Budget Constraints:** Another significant challenge is time and budget constraints. In today's fast-paced business environment, organizations come under immense pressure to deliver software solutions quickly and efficiently, often at the expense of security. However, prioritizing speed and cost savings over security could result in severe consequences, including data breaches and other security incidents.

3. **Complexity of Modern Software Systems:** The complexity of modern software systems is another challenge that developers face when building secure software. With a multitude of components and technologies that must work seamlessly together, it can be difficult to identify and mitigate potential security vulnerabilities. This is especially so in large, distributed software systems where there are many attack vectors and vulnerabilities to protect.

4. **Evolving Threat Landscape:** Another challenge in building secure software is keeping up with an evolving threat landscape. Cyber threats are constantly evolving, and attackers are always looking for new ways to exploit software vulnerabilities. This means developers must stay up to date with the latest threats and attack techniques and adapt their software accordingly to ensure they remain secure.

5. **Lack of Security Training:** More critically, a lack of security training for developers can pose a significant challenge to building secure software. Many developers may not have received sufficient training in secure coding practices or are aware of the latest security best practices. This can lead to vulnerabilities being introduced into the software unintentionally.

Building secure software is a multifaceted challenge that requires significant expertise, resources, and diligence. The challenges outlined above are just a few of the many obstacles that developers face when attempting to build secure software. However, by adopting best practices and prioritizing security throughout the development process, organizations can mitigate the risks of cyber-attacks and safeguard sensitive data of their users. We will now discuss some of the best practices which developers can implement to build more secure software.

Best Practices

1. Perform Regular Security Audits: Organizations may perform regular security audits to identify security flaws in legacy systems and rank the flaws according to their severity. They should also think about upgrading old systems to more current versions with greater security features.

2. **Prioritize Security:** Organizations should adopt a secure software development life cycle that prioritizes security from the initial software development stage notwithstanding time and financial constraints. This includes performing penetration testing, code review, and threat modelling. By prioritizing security throughout the development process, organizations could avoid expensive and time-consuming security issues later in the future

3**. Secure Code Best Practices:** Developers should follow secure coding best practices, such as input validation, error handling, and proper encryption, to reduce security risks in complex software systems. In order to identify possible threats and take prompt action, they could also employ monitoring and logging systems.

4. **Staying Current in Cybersecurity:** By constantly participating in cybersecurity training, reading cybersecurity blogs and forums, and attending cybersecurity conferences, developers are able to keep up with the most recent threats and attack techniques. Additionally, they ought to apply security patches and updates as soon as they become available.

5. **Providing Ongoing Security Training for Developers:** To keep developers updated with the most recent cybersecurity best practices, organizations should provide their developers with regular security training regularly such as online courses, seminars, and conferences. To enhance their knowledge of security vulnerabilities and mitigation, developers should be encouraged to participate in bug bounty programs and ethical hacking events.

Conclusion

In conclusion, developing secure software plays an essential role in creating a safer digital world, especially in Malaysia, where cyberattacks are on the rise. Developers could significantly improve the security of their software and protect sensitive user data by following the best practices in software development and prioritizing security throughout the development process.

The difficulties developers encounter, such as dealing with vulnerabilities in legacy systems, time and budget restrictions, the complexity of current software systems, an expanding threat landscape, and a lack of security training, underscore the importance of implementing proactive security measures. Developers can reduce the risks of cyberattacks and protect their consumers' valuable digital assets by identifying these problems early and applying suitable security practices.

As security remains a constant challenge, developers must keep abreast of the newest security trends, vulnerabilities, and mitigation strategies in order to react to the ever-changing threat landscape. By prioritizing security in software development, developers play an important role in fostering user trust and confidence, resulting in a more secure digital environment in Malaysia.

Ultimately, the objective is to nurture a security-first culture in software development, whereby secure coding practices, frequent security audits, continuous training, and staying updated about cybersecurity are an integral development process. Only by so doing, developers can realise a better and more secure digital future.

References

1. 5 key challenges of building a security training program - Avatao. (2022, July 13). Avatao. https://avatao.com/blog-5-key-challenges-when-building-a-security-training-program/

2. Galdino, G. (2022, June 21). How to deal with security challenges in software development? Conviso AppSec. https://blog.convisoappsec.com/en/developers-how-to-deal-with-some-of-the-biggest-security-challenges-during-software-development/

3. Tran, D. (2023, March 31). Best Practices For Secure Software Development. Perforce Software. https://www.perforce.com/blog/sca/best-practices-secure-software-development

4. Team, H. (2022, April 28). Secure Software Development: Best Practices, Frameworks, and Resources. Hyperproof. https://hyperproof.io/resource/secure-software-development-best-practices/

5. Waitt, T. (2019, December 8). Secure Software Development: Challenges and Considerations - American Security Today. American Security Today. https://americansecuritytoday.com/secure-software-development-challenges-and-considerations/

Massive Campaign On Stolen Mobile Bank Credentials Via Malicious Mobile APK

By | Kilausuria Abdullah, Lukman Hakim Abd Rahman, Nur Qurratu' Aini Rohizan, Kamarul Bahrin Khalid, and Shaikh Abdul Fikri Bin Shaikh Abdul Hamid.

Introduction

Today, billions of people across the world use smartphones, computers, and tablets in their daily lives. These devices run various software applications that provide utility and convenience to us. While there are literally thousands of useful applications that benefit us, cybercriminals have also developed their own versions of mobile-friendly application programs known as mobile APK.

Mobile APK is a malicious software specifically designed to target mobile devices, such as smartphones and tablets, with a single goal of gaining access to credentials and private data.

Although mobile APK is currently not as pervasive as other malwares, it is a growing threat as many companies are now allowing employees to access corporate networks using their personal devices. Even public users who use their smart phones could potentially bring unknown threats into a environment.

Therefore, it is highly recommended that users protect their applications to minimize the impact of stolen credentials and finances.

The threat of mobile APK could just be a click away where all the money from a victim's bank account could be lost after filling in sensitive banking credentials.

What is the modus operandi of a malicious APK Campaign? This article surveys the current landscape of mobile APK Campaigns targeting bank credentials based on incident reports received from Cyber999 service and best practice against such threat.

Statistics of Android Trojans

The Overall incidents reported to Cyber999 services on Malicious APK from 2022 to July 2023.

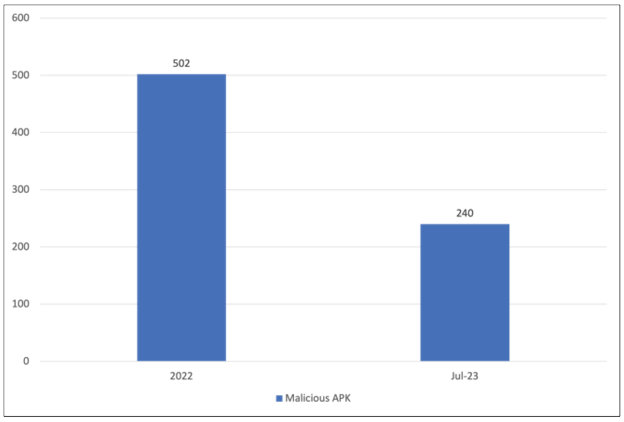


Figure 1: Malicious APK Incidents Reported to Cyber999 in Year 2022 vs July 2023.

Referring to **Figure 1** above, a total of 502 malicious APKs were reported in year 2022. On the other hand, 240 malicious APK incidents have already been reported for year 2023 up to July.

The rapid rise in reported malicious APK incidents is a clear indicator of the evolving tactics used by cybercriminals to target mobile users. The rise from 502 incidents across previous years to 240 incidents in the first half of 2023 alone underscores the urgency of addressing this threat. As technology advances and connectivity deepens, attackers find new and innovative ways to exploit vulnerabilities in mobile platforms, necessitating stronger countermeasures.

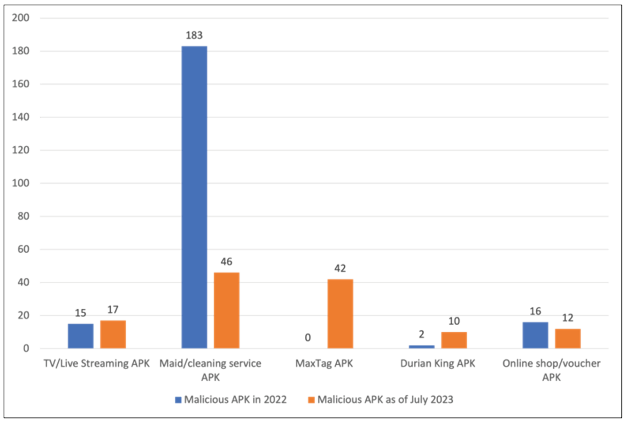


Figure 2: Top 5 Malicious APK Incidents Reported to Cyber999 in Year 2022 vs as of up to July 2023.

The statistics in Figure 2 reflect a range of reported incidents involving different types of malicious APKs, offering insights into emerging trends and potential areas of concern within the realm of mobile applications.

1. TV/Live Streaming Malicious APKs:

In 2022, there were 15 reported incidents related to TV/Live Streaming malicious APKs. By July 2023, the number of incidents rose to 17, suggesting a continued focus on TV/Live Streaming malicious APKs among threat actors.

2. Maid/Cleaning APKs:

2022 saw a substantial 183 reported incidents involving maid/cleaning malicious APKs, underscoring the popularity of the service.
The number of incidents dropped significantly to 46 up to July 2023, probably due to increased awareness.

3. Maxtag APKs:

Interestingly, there were no reported incidents involving MaxTag malicious APKs in 2022. However, the situation took a turn, with 42 reported incidents by July 2023, highlighting a sudden emergence of security concerns related to this specific type of malicious APK.

4. Durian King APKs:

The increase in reported incidents in 2023 for Durian King malicious APKs could signify a growing interest among threat actors to exploit this service during durian season.

5. Online shop/voucher APKs:

While the overall number of reported incidents for online shop/voucher malicious APKs has decreased slightly, the fact that they continue to be targeted suggests that attackers still view these services as potential avenues for exploitation.

Types of Massive Campaign

There are various malicious mobile APK campaigns reported within the past few years, mostly in the form of a phishing or financial fraud attempts targeting internet banking details. Some of the top 3 examples are as follows:

1. Maid cleaning services

In this campaign, threat actors attempt to steal financial credentials by using fake websites that pose as legitimate services, some replicating an original outright. In their effort, threat actors employ Facebook adverts to persuade potential victims to download Android malware from a malicious website. All eight websites impersonated services only in Malaysia. The seven websites provide cleaning services: Grabmaid, Maria's Cleaning, Maid4u, YourMaid, Maideasy, MaidACall and MyMaidKL. The eighth website is a pet store called PetsMore. To tempt potential victims, threat actors set up these websites using domain names similar to their original counterparts.

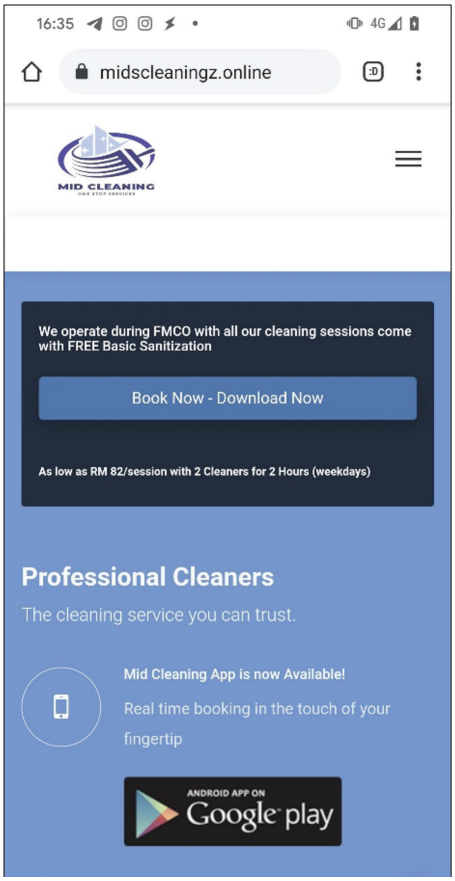


Figure 2: Top 5 Malicious APK Incidents Reported to Cyber999 in Year 2022 vs as of up to July 2023.

2. MaxTag

In May 2023, several threat actor groups impersonated MaxTag, a SmartTAG toll payment device seller to target victims and steal their financial credentials through a fake website. The fake website mimics the original website almost entirely, luring victims to enter credentials in the fake payment gateway form that sends the data to a C2 (Command & Control) server managed by threat actors.

3. E-Wedding Card

In light of recent malicious APK, cybercriminals had exploited a malicious android application in a "Wedding Invitation" or “Jemputan Majlis Perkahwinan” malware campaign targeting internet users in Malaysia. The Wedding Invitation Scam preys on people's excitement about wedding invitations. Cybercriminals use text messages sent via instant messaging apps such as WhatsApp to trick victims into installing a malicious APK on their devices that can steal their personal information.

Modus Operandi of Massive Mobile APK Campaign

The Massive malicious APK campaign that stole mobile bank credentials of target naive users all have very similar TTPs. The details of TTPs for these types of massive campaign are shown in the table below.

Type of massive campaign	Medium Advertisements	Modus Operandi
Cleaning Services, And MaxTag	Facebook and Instagram	1. Threat actors use fake websites that pose as legitimate services. 2. Threat actors employ Facebook and Instagram adverts to persuade potential victims to download Android malware from a fake website. 3. To tempt potential victims, threat actors set up these websites using domain names similar to their impersonating services. 4. Potential victims are required to enter credentials via a fake payment gateway form that sends data to a C2 (Command & Control) server which is managed by threat actors.
E-Wedding Card	WhatsApp	

Effects of Mobile Malware Malicious APK

The effects of mobile malware vary depending on the type of malware, its capabilities, and the intentions of the attacker. Major consequences can be classified into a several categories:

1. **Data theft**

   Mobile malware can steal sensitive data such as personal data, login credential and credit card number. The stolen data may be sold to 3rd parties that could harm the user in terms of financial, privacy and safety.

2. **Financial loss**

   The TAC numbers could be stolen from users' mobile phones using the APK files, thereby allowing the attacker to receive a TAC number through SMS. This will enable the attacker to perform unauthorized financial transactions.

3. **Privacy Invasion**

   Malware can access user device's microphone and camera, giving attackers the ability to secretly record sounds, take pictures, and even observe your keystroke or steal from web browser's cache.

Best Practices in Mobile Security

A mobile application is meant to manage information and perform tasks in victim's phone. However, such features could be used for other malicious purpose. As best practices to prevent such incidents, we would highly recommend the following:

- Verify an application permission and the application author or publisher before installing it.
- Avoid side loading (installing from non-official sources) whenever possible. If you need to install Android software from a source, other than the trusted marketplace, ensure it is coming from a reputable source.
- Do not click on adware or suspicious URL sent through SMS/messaging services.
- Malicious program could be attached to collect user's information.
- Always install a reputable anti-virus on your smartphone/mobile devices and keep it up to date regularly.
- Update the operating system and applications on smartphone/tablet, including the browser, to avoid any malicious exploits of security holes in outdated versions.
- Do not root or 'Jailbreak' your phone.
- Please ensure to turn off the "Unknown Source" option in the Security Settings page.
- Contact relevant authorities such as Cyber999 for any inquiries and assistance related to this threat.

Summary

Malicious mobile APKs are a growing threat to mobile users. These apps can steal personal information, install malware, or even take control of a device. Therefore, the need for enhanced mobile security measures is unquestionable. To protect yourself from malicious APKs, it is important to only download apps from trusted sources, such as the Google Play Store or the Apple App Store, be wary of apps that ask for excessive permissions, keep your mobile operating system and apps up to date and use a mobile security app to scan for malware.

If you think you have downloaded a malicious APK, uninstall it immediately and contact your device manufacturer or mobile carrier for assistance.

References

1. https://www.makeuseof.com/what-are-android-banking-trojans/

2. https://www.mycert.org.my/portal/details?menu=431fab9c-d24c-4a27-ba93-e92edafdefa5&id=1d7aff3a-492f-435a-9d2c-f5d2dc5bc8af

3. https://www.bleepingcomputer.com/news/security/malicious-android-app-steals-malaysian-bank-credentials-mfa-codes/

4. https://www.mycert.org.my/portal/advisory?id=MA-834.052022

Wedding Invitation 'Jemputan Majlis Perkahwinan' Malicious APK

By | Lukman Hakim Bin Abd Rahman, Nur Qurratu 'Aini Binti Rohizan, Shaikh Abdul Fikri Bin Shaikh Abdul Hamid, Ahmad Rabbani Bin Omar, Syafiq Iskandar Bin Sham Suri

Introduction

Today's digital landscape is experiencing an alarming surge in persistent threat of malicious APK attacks. These attacks pose a significant danger to both individuals and organizations. Recently, the wedding invitation scam has gained significant traction on social media in Malaysia, emerging as a new and concerning trend. Scammers employ tactics such as contacting their targets via WhatsApp and deceitfully sending an APK file disguised as a wedding invitation.

SMS Trojan/Spyware

This article focuses mainly on malicious APK that uses SMS Trojan or spyware. The purpose of this attack is to get information from Short Message/ Messaging Service (SMS) in compromised device. This stolen information may be used for a variety of illegal activities, including financial fraud, identity theft, and unlawful access to accounts that require two-factor authentication.

Non-technical Summary

CyberSecurity Malaysia carried out an investigation to analyze in detail the behaviours of the malicious Android application so that we can ascertain how victims of scams are compromised, or "hacked," using such Android application installed in the victim's phone. After being installed, the malicious software will be able to send SMS to the phone and read all the victims' SMS content. The program could provide scammers or hackers access to the victim's SMS inbox.

Technical Summary

A malicious Android Package Kit (APK) sample that uses a wedding invitation theme as its operating principle was recently discovered by the MyCERT Team. The threat actor used WhatsApp to spread this malicious Android software, sending victims messages containing a wedding invitation and an APK file that must be downloaded to view the invitation card.

Additionally, once installed on the victim's Android device, the malicious APK starts stealing all incoming SMS messages. The threat actor can monitor a victim's SMS content via phishing approach and SMS theft methodology used by the Android application. This stolen information might be used for nefarious purposes, such as gaining access to online banking data or other services that employ SMS authentication.

The MyCERT malware analysts have also spotted clues that could point to an Indonesian origin for the attacker of this campaign. These concerns are sparked by the discovery of Indonesian phone numbers within the code as well as the use of Indonesian terminology in the malware's command and control system.

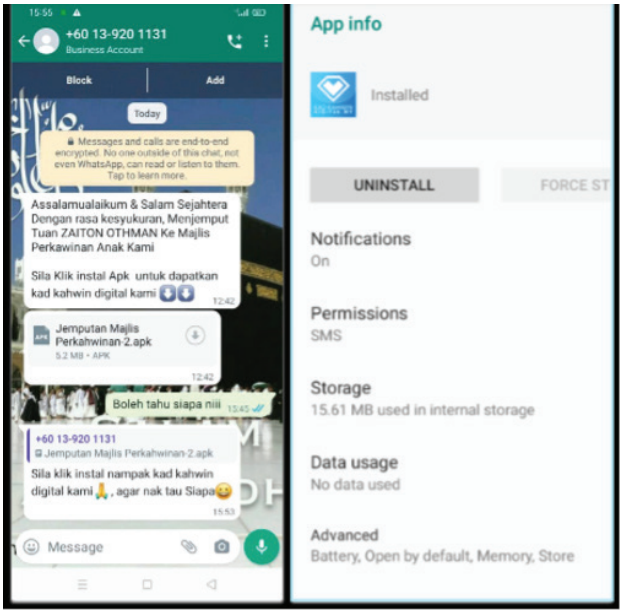


Figure 1: WhatsApp conversation (credit to owner) and installed the malicious APK which does not have a name.

Graph Flow

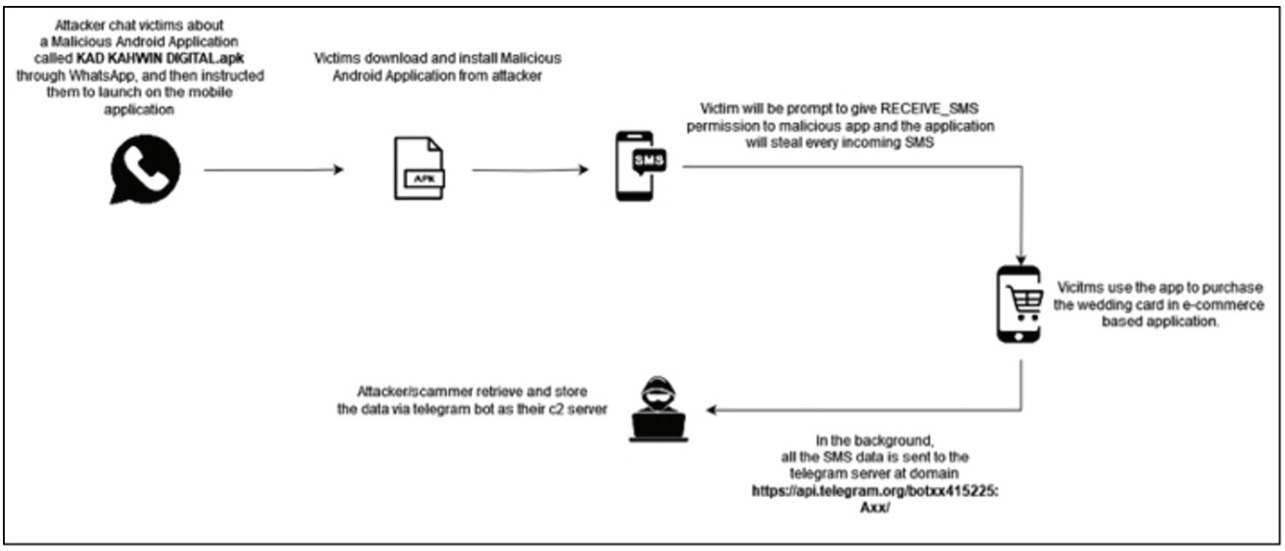


Figure 2: Graph Flow of the modus operandi by DetecX team of Netbytesec.

Modus Operandi

A new scam tactic has been making waves on social media, targeting WhatsApp users through the disguise of wedding invitation cards sent via APK file.

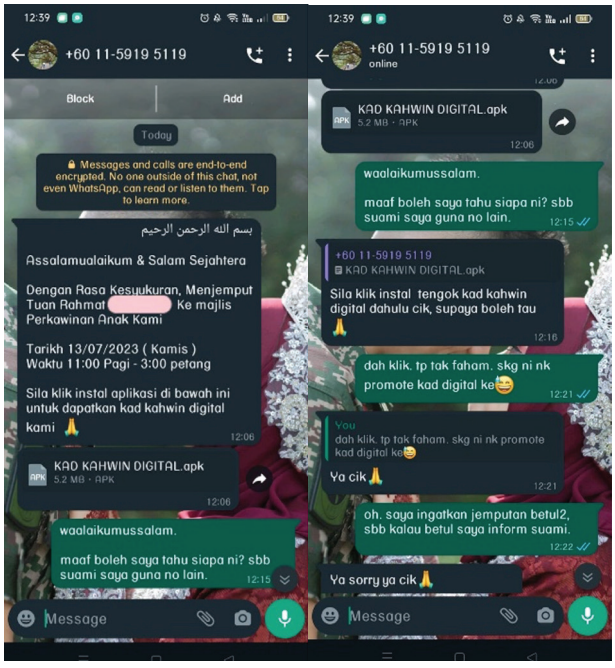


Figure 3: The conversation (credit to owner) between the victim and the scammer.

The attacker creates a seemingly legitimate wedding invitation app, which can be downloaded and installed on Android devices. The attacker could send unsolicited messages to individuals or groups on WhatsApp, pretending to be a friend or family member inviting them to a wedding. They may use persuasive language or emotional appeal to entice recipients to click on a link or download the APK. They could claim that it contains important wedding details or exclusive content related to the event.

Unsuspecting recipients may download and install the malicious app on their Android devices, believing it to be a genuine wedding invitation.

Once installed, a permission will pop up to allow receive SMS which the application will steal every incoming SMS, including from the victim's device without his or her knowledge.

Recommendation

To protect against malicious APK attacks, individuals and organizations should prioritize the following:

- Verify an application permission and the application author or publisher before installing it.
- Avoid side loading (installing from non-official sources) whenever possible. If you do need to install Android software from a source other than the trusted marketplace, be sure that it is coming from a reputable source.
- Do not click on adware or suspicious URL sent through SMS/messaging services.
- Malicious program could be attached to collect user's information.

- Always run a reputable anti-virus on your smartphone/mobile devices and keep it up to date regularly.
- Update the operating system and applications on smartphone/tablet, including the browser, to avoid any malicious exploits of security holes in outdated versions.
- Do not root or 'Jailbreak' your phone.
- Ensure to turn off the “Unknown Source” option in the Security Settings page.
- Contact relevant authorities such as Cyber999 for any inquiries and assistance needed related to this threat.

Conclusion

In conclusion, malicious APK attacks represent a growing and persistent threat in today's digital landscape. These attacks underscore the need for heightened awareness, robust cybersecurity practices, and proactive measures to safeguard both personal and organizational data. The consequences of falling victim to such attacks can be severe, ranging from compromised privacy to financial loss and even reputational damage. As the sophistication and diversity of malicious APKs continue to evolve, it is imperative for users and organizations to stay informed, adopt best practices, and leverage advanced security solutions to mitigate these threats effectively.

References

1. https://www.mycert.org.my/portal/details?menu=431fab9c-d24c-4a27-ba93-e92edafdefa5&id=1d7aff3a-492f-435a-9d2c-f5d2dc5bc8af

2. https://www.bleepingcomputer.com/news/security/malicious-android-app-steals-malaysian-bank-credentials-mfa-codes/

3. https://notes.netbytesec.com/2023/06/kahwin-sms-stealer-target-Malaysia.html?m=1

4. https://www.virustotal.com/gui/file/982b360b0cf8fcd0dec00f233cdeeb191876d4301dd8e62e75ff2909a5b03cfc

5. https://www.facebook.com/story.php?story_fbid=pfbid02Zv4AUVmd6UnoT9KSRMbRqpGqPiDctoiFadW8Gj1AXVUSuKy5as7tdxPoLyBUc8yhl&id=100069476666645&mibextid=Nif5oz

Understanding Computer Security Incident Response Team (CSIRT)

By | Sharifah Roziah Binti Mohd Kassim, Ahmad Rabbani Bin Omar, Kilausuria Binti Abdullah, Syafiq Iskandar Bin Sham Suri, Shaikh Abdul Fikri Bin Shaikh Abdul Hamid

1.0 Background

Preventive measures against security incidents such as applying security updates, performing backups, and regular network security inspections are important. However, it is not sufficient to rely solely on them. Some widely used technologies, such as intrusion detection systems (IDS), cannot respond and handle incidents but only detect and provide alerts about possible cyber-attacks [1]. Rather, efficient responses to computer security incidents have become more important now [2].].

Researchers have emphasised that security by prevention is no longer sufficient; rather, having appropriate response mechanisms to respond to computer security incidents is necessary [3]. Computer security incidents normally occur under considerable time pressure when organisations are under immense pressure due to information overload, information diversity and task uncertainty requiring people, processes, and technology to collectively respond. While protection of systems is almost all technology-based, detection requires equal proportions of people, processes, and technology with critical proportion coming from the process and technology [4]. Schneier, 2014 said that one could not automate incident response as it needs people and thinking. The "people" component of incident response, highlighted by Schneier, 2014 is made up of a "computer security incident response team" (CSIRT) who collectively respond to security incidents as a team.

Bruce Schneier (2014) has pointed out that computer security incident response needs people to perform the tasks in responding to incidents [4]. This claim is supported by a recent empirical study conducted as part of this research, with 17 national CSIRTs, found that manual approaches are predominantly used in 14 out of 17 national CSIRTs incident responses [5].

This finding is consistent with Bruce Schneier (2014), which shows incident response depends largely on manual approaches that need people, often in groups or teams, called an incident response team or Computer Security Incident Response Team (CSIRT).

2.0 Origin and Types of CSIRTs

The concept of CSIRTs first emerged from team efforts and experiences handling the first ever 'Internet worm' incident, which hit the Internet in November 1988, the Morris Worm attack [6]. This established the first CSIRT— the CERT/CC, under Carnegie Mellon University, USA [7], after realising the urgent need for a specialised team to respond to incidents. It should be noted that CERT/CC is now called the CERT Division of the Software Engineering Institute (SEI) of Carnegie Mellon University in the USA. Since the establishment of the first CSIRT, CSIRTs have gained attention in the realm of cyber security for their significant role in responding to and mitigating security incidents. Interestingly, many early CSIRTs were established by academic communities, for example, in the setup of CERT/CC of Carnegie Mellon University in 1988 and the Australian Computer Emergency Response Team (AusCERT), established in the University of Queensland, Australia in 1993.

The increasing need for incident response expanded the establishment of CSIRTs to various sectors both public and private. Over time, CSIRTs flourished worldwide, expanding to organisational, national (national CSIRTs) and regional levels. In the broader Internet community, CSIRTs from a diverse group of organisations and sectors, such as critical infrastructure, government, industry, and academia form a "global network" [8]. Today, CSIRTs have been widely established within regions, countries, governments, the military, academics, products and businesses [9]. While national CSIRTs address issues on the national level, sector-specific CIRTs address cyber security needs of a specific sector, such as health, transport, telecommunication, and utilities. Other types of CSIRTs serve multinational companies, large companies, and private universities. Organisational CSIRTs or Internal CSIRTs (sometimes referred to as "enterprise"

CSIRTs) operate at an organisations' levels such as a private company, enterprise or businesses.

A list of different types of CSIRTs is summarised in Table 1.

Types of CSIRTs	Constituency Served
Regional CSIRTs	A region, e.g., Asia Pacific, Europe
National CSIRTs	A country
Public Sector CSIRTs	A county, a locality
Governmental CSIRTs	State Government
Organisational CSIRTs	Any organisation
Product CSIRTs	Respond to product vulnerabilities, e.g., CISCO, Microsoft CSIRTs
Sector CSIRTs	A particular sector, e.g., Energy Sector CSIRT
Commercial CSIRTs	A commercial entity

Table 1: Types of CSIRTs

3.0 CSIRTs Functions and Services

A CSIRT is responsible for receiving, reviewing, and responding to security incident reports and activities. It consists of a "group of experts within an organisation which is responsible for handling incidents related to IT security issues" [10]. The ISO/IEC 27000:2018 standard defined an "Information Security Incident Response Team" as appropriately skilled and trusted organisation with members that handle information security incidents during an incident's life cycle. Generally known as computer security incident response team (CSIRT), an incident response team is also called a computer emergency response (or readiness) team (CERT), or a cyber (or computer) incident response (or readiness) team (CIRT). The ISO/IEC270351:2023 uses the term Incident Response Team (IRT) defined as a team of appropriately skilled and trusted members of an organisation that responds to and resolves cyber incidents in a coordinated way.

Notably, ISO/IEC27035-1:2023 also clarified that Computer Emergency Response Team (CERT) and Computer Security Incident Response Team (CSIRT) are specific examples of IRTs in organisations and sectorial, regional, and national entities wanting to coordinate their response to large-scale ICT and cybersecurity incidents.

ISO/IEC 27035-1:2023 recommends having a permanent incident response team (IRT) for respective constituencies. Establishing CSIRT ensures a team trained and experienced in resolving incidents and coordinating with internal and external stakeholders on incidents. Such a CSIRT normally responds to cyber incidents following an established standard operating procedure (SOP) [11]. This SOP is mainly adapted from the guidelines defined by standardisation in cyber security, such as the "Computer Security Incident Handling Guide" defined by the NIST in the US [12], in Figure 1, the International Standard Organisation – ISO/IEC 27002:2013 and the SANS Institute of the USA, in Figure 2.

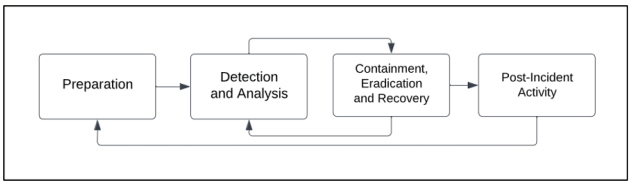


Figure 1: Computer Security Incident handling Guide by NIST

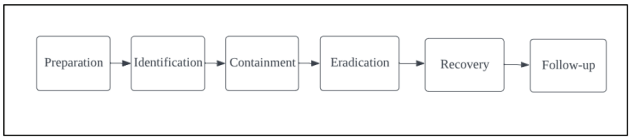


Figure 2: Computer Security Incident Handling Steps by SANS Institute

In principle, CSIRTs' services consist of reactive nature [4]7 such as incident management, incident response, and incident handling or either proactive such as monitoring, vulnerability handling and information sharing within the team [13]. A number of CSIRTs provide a combination of reactive (i.e., incident response and intrusion detection) and pro-active services (i.e., vulnerability management, risk assessments, security consulting, and penetration testing) while other CSIRTs focus on providing reactive services only. CSIRTs perform these services based on their mission, scope, expertise, and constituent requirements. In addition to the above services, CSIRTs participate in national and international research initiatives related to cyber security on identifying methods for detecting security incidents [14]. A full description of the work of CSIRTs can be found in RFC 2350, Internet Engineering Task Force, 1998.

4.0 Conclusion

In a nutshell, it is clear that CSIRTs play a prominent role in the overall response to security incidents. In view of the current threat landscape, the frequency of occurrences and the seriousness of security incidents or incidents or cyber-attacks, the responsibility to respond to and mitigate the incidents therefore lies in the hands of CSIRTs, depending on the constituents' requirements. A much bigger responsibility is crucial at national levels to ensure the entire cyberspace of a nation is safeguarded, of which the responsibility often lies on national CSIRTs

5.0 References

1. Sayed Hadi Hashemi, Mohammad Babaeizadeh, Mohsen Nowruzi, Hossein Hadian Jazi, Mohammad Shahmoradi, and Elaheh Biglar Beigi Samani. 2012. A Comprehensive Semi-automated Incident Handling Workflow. In Proceedings of the 6th International Symposium on Telecommunications. IEEE, 1065–1070.

2. Erka Koivunen. 2010. "Why Wasn't I Notified?": Information Security Incident Reporting Demystified. In Information Security Technology for Applications: 15th Nordic Conference on Secure IT Systems, NordSec 2010, Espoo, Finland, October 27-29, 2010, Revised Selected Papers (Lecture Notes in Computer Science, Vol. 7127). Springer, 55–70.

3. Robin Ruefle, Audrey Dorofee, David Mundie, Allen D. Householder, Michael Murray, and Samuel J. Perl. 2014. Computer Security Incident Response Team Development and Evolution. IEEE Security & Privacy 12, 5 (2014), 16–26.

4. Bruce Schneier. 2014. The Future of Incident Response. IEEE Security & Privacy 12, 5 (2014), 96–96.

5. Sharifah Roziah Binti Mohd Kassim, Shujun Li, and Budi Arief. 2022. Incident Response Practices Across National CSIRTs: Results from an Online Survey. OIC-CERT Journal of Cyber Security 4, 1 (2022), 63–80.

6. Eugene H. Spafford. 1989. The Internet worm program: An analysis. ACM SIGCOMM Computer Communication Review 19, 1 (1989), 17–57.

7. Y. M. Wara and D. Singh. 2015. A Guide to Establishing Computer Security Incident Response Team (CSIRT) for National Research and Education Network (NREN). African Journal of Computing & ICT 8, 2 (2015), 1–8.

8. Software Engineering Institute, Carnegie Mellon University. [n.d.]. National Computer Security Incident Response Teams (CSIRTs). web page. https://www.sei.cmu.edu/our-work/cybersecurity-center-development/index.cfm

9. Rahayu Azlina Ahmad and Mohd Shamir Hashim. 2011. The Organisation of Islamic Conference-Computer Emergency Response Team(OIC-CERT): Answering Cross Border Cooperation. In Proceedings of the 2011 2nd Worldwide Cybersecurity Summit. IEEE, 5 pages.

10. Muhammad Haidar, Yudho Giri Sucahyo, Teddy Sukardi, and Arfive Gandhi. 2021. Analysis of CSIRT Services in Facing Cyber Security Challenges in Indonesia. In 2021 4th International Conference on Information and Communications Technology (ICOIACT). IEEE, 154–159.[7]

11. Sharifah Roziah Binti Mohd Kassim, Solahuddin Bin Shamsuddin, Shujun Li, and Budi Arief. 2022. How National CSIRTs Operate: Personal Observations and Opinions from MyCERT. In Proceedings of the 2022 IEEE Conference on Dependable and Secure Computing. IEEE, 2 pages.

12. Paul Cichonski, Tom Millar, Tim Grance, and Karen Scarfone. 2012. Computer Security Incident Handling Guide. Technical Report 800-61 Revision 2. National Institute of Standards and Technology, U.S. Department of Commerce.

13. Robin Ruefle, Audrey Dorofee, David Mundie, Allen D. Householder, Michael Murray, and Samuel J. Perl. 2014. Computer Security Incident Response Team Development and Evolution. IEEE Security & Privacy 12, 5 (2014), 16–26.

14. Monika Nowikowska. 2022. The Main Tasks of the Network of Computer Security Incident Response Teams in the Light of the Act on the National Cybersecurity System in Poland. In Cybersecurity in Poland. Springer, 223–241.

AKSA MYSEAL 2.0: Repository of Libraries and APIs

By | Nurul Amiera Sakinah Binti Abdul Jamal & Chan Yen Yee

Introduction

In the world of digital security, there is an unsung hero that is working quietly in the background to keep our data safe. The hero is none other than cryptographic algorithms, a powerful lock that safeguards our online communications and sensitive information. A world without it is akin to leaving our front door at home wide open. MySEAL project was initiated to ensure that these algorithms are strong and trustworthy.

The Story Begins: Birth of MySEAL

MySEAL
Senarai Algoritma Kriptografi Terpercaya Negara

MySEAL, which stands for **Se**narai **Al**goritma Kriptografi Terpercaya Negara is Malaysia's National Trusted Cryptographic Algorithm List. A mission was set in motion in 2016 to create a list of cryptographic algorithms that is trusted and reliable, to be known as AKSA MySEAL. The algorithms chosen as candidates for AKSA MySEAL were not just any algorithms. They were selected from various important standards like NIST-FIPS, ISO/IEC, IEEE, and other cryptographic algorithm listing projects (i.e. CRYPTREC, NESSIE, eSTREAM). It was as if a team of best of breed algorithms was assembled from different parts of the world. These algorithms were then put to the test by local and international experts in the field of cryptography. These experts verified if the selected algorithms meet predetermined criteria and requirements during the first and second phase of AKSA MySEAL evaluation to ensure that these digital guards were up to the task.

This careful selection process was conducted between April and November 2017, resulting in a list of 58 cryptographic algorithms (as presented in Table 1). The selected algorithms can be categorised into six groups. Each of these groups represents different structures and designs in cryptographic primitives as well as different functionalities:

- **Symmetric Block Cipher:** 12 algorithms (take count of the cipher variants) are involved, 9 general block ciphers, and 3 lightweight block ciphers, respectively.
- **Symmetric Stream Cipher:** 3 algorithms are included.
- **Asymmetric Cryptographic:** Categorised into 3 subgroups: Digital Signature Scheme (3 ciphers), Asymmetric Encryption Scheme (6 ciphers) and key agreement scheme (2 ciphers).
- **Prime Number Generators:** 3 primitives included.
- **Deterministic Random Bit Generator:** 9 primitives involved.
- **Cryptographic Hash Function:** Categorised into 2 subgroups, namely general hash functions (10 ciphers, **take count of the cipher variants**) and lightweight cryptographic hash functions (10 ciphers) respectively.

Cryptographic Primitives	Number of algorithms (with variants)	Algorithms & Variants
Symmetric Block Cipher	12	Block Cipher: 1. AES-128, AES-192, AES-256 2. Camellia-128, Camellia-192, Camellia-256 3. CLEFIA-128, CLEFIA-192, CLEFIA-256 Lightweight Block Cipher: 1. PRESENT-80, PRESENT-128 2. HIGHT

Symmetric Stream Cipher	3	1. ChaCha20-256 2. KCipher-2 3. Rabbit
Asymmetric Cryptographic	11	Digital Signature Scheme: 1. DSA 2. ECDSA 3. RSA-PSS Asymmetric Encryption Scheme: 1. PSEC-KEM 2. RSA-KEM 3. ACE-KEM 4. ECIES-KEM 5. RSA-OAEP 6. NTRU Key Agreement Scheme: 1. ECDH 2. DH
Prime Number Generators	3	1. Miller-Rabin Primality Test 2. Elliptic curve Primality Certificate 3. Shawe-Taylor's Algorithm
Deterministic Random Bit Generator	9	1. HMAC-SHA-384-DRBG, HMAC-SHA-512-DRBG 2. SHA-512/224-DRBG, SHA-512/256-DRBG5, SHA-384-DRBG, SHA-512-DRBG 3. AES-128-CTR-DRBG, AES-192-CTR-DRBG, 3-Key-TDEA-CTR-DRBG
Cryptographic Hash Function	20	Hash Function: 1. SHA-384, SHA-512, SHA-512/224, SHA-512/256 2. SHA3-224, SHA3-256, SHA3-384, SHA3-512, SHAKE128, SHAKE256 Lightweight Hash Function: 1. SPONGENT-88, SPONGENT-128, SPONGENT-160, SPONGENT-224, SPONGENT-256 2. PHOTON-80/20/16, PHOTON-128/16/16, PHOTON-160/36/36, PHOTON-224/32/32, PHOTON-256/32/32

Table 1. AKSA MySEAL Algorithms

Dawn of A New Chapter: Why AKSA MYSEAL 2.0 Matters

Time progression is lightning fast in the world of digital security. After five years since its first selection testing, the algorithms listed in AKSA MySEAL need to be re-evaluated, and hence AKSA MySEAL 2.0 was initiated. Started in April 2023, AKSA MySEAL 2.0 is expected to conclude by January 2024. AKSA MySEAL 2.0 is akin to a 'training camp' for the algorithms. It is not just about reviewing old ones – but welcoming new "recruits". The evaluation process of AKSA MySEAL 2.0 involved 29 new algorithms, in addition to the existing algorithms listed in AKSA MySEAL. The candidates presented in Table 2 underwent a process similar to the AKSA MySEAL evaluation, albeit with higher standards.

How significant is the inclusion of these algorithms like Bouncy Castle, OpenSSL, and others in cryptographic libraries and APIs? An analogy would be like a champion being invited to a big

tournament. It means it is acknowledged as strong and skilled. Similarly, when an algorithm is included in these popular libraries and APIs, it means experts and programmers trust them enough to use them in their own projects. This trust is a testament of the algorithm's reliability and functionality. It is a seal of approval from the cryptographic as well as the cybersecurity community.

Cryptographic Primitives	Number of algorithms (with variants)	Algorithms & Variants
Symmetric Block Cipher	4	Block Cipher: 1. SEED Lightweight Block Cipher: 2. MISTY1
Symmetric Stream Cipher	7	1. MUGI 2. TRIVIUM 3. SNOW 2.O 4. DECIMv2 5. Salsa20/12 (SW) 6. HC-128 7. Grain-V1
Asymmetric Cryptographic	10	Digital Signature Schemes: 1. RSA 2. SDSA 3. ECSDSA 4. BLS 5. SM2 6. SM9 7. RSASSA-PKCS1-v1_5 Stateful hash-based signature schemes: 1. LMS-HSS 2. XMSS 3. XMSSMT
Prime Number Generators	4	1. Pocklington Primality Test 2. Deterministic Lucas Primality Test (Lucas-Lehmer) 3. Probabilistic Lucas Primality Test 3. Brillhart-Lehmer-Selfridge Primality Test
Cryptographic Hash Function	4	Hash Function: 1. Whirlpool 2. Streebog 3. SM3 Lightweight Hash Function: 1. Lesamnta-LW

Table 2. AKSA MySEAL 2.0 Evaluating Algorithms

Table 3 to Table 9 presents the validation status of listed algorithm candidates in AKSA MySEAL 2.0 (categorised into the six main groups) within 7 widely used cryptographic libraries or APIs:

1. Bouncy Castle
2. OpenSSL
3. Crypto++,
4. Microsoft Cryptographic API,
5. WolfCrypt,
6. Java Classes
7. Vitis Security Library

	Bouncy Castle	OpenSSL	Crypto++	Microsoft API	WolfCrypt	Java Classes	Vitis Security Library
AES-128, AES-192, AES-256	√	√	√	√	√		
Camellia-128, Camellia-192, Camellia-256	√	√	√		√		
HIGHT			√				
SEED	√	√	√				

Table 3. Symmetric Block Cipher

	Bouncy Castle	OpenSSL	Crypto++	Microsoft API	WolfCrypt	Java Classes	Vitis Security Library
ChaCha20 -256	√	√	√		√		
DECIMv2			√				
Salsa20/12 (SW)	√		√				
HC-128	√		√				
Grain-V1	√						
Rabbit			√				

Table 4. Symmetric Stream Cipher

	Bouncy Castle	OpenSSL	Crypto++	Microsoft API	WolfCrypt	Java Classes	Vitis Security Library
DSA	√	√	√	√	√		
RSA	√	√	√	√	√		
ECDSA	√	√	√	√			
RSA-PSS	√	√					
RSASSA-PKCS1-v1_5	√	√	√	√			
SM2	√	√			√		

Table 5. Asymmetric Digital Signature

	Bouncy Castle	OpenSSL	Crypto++	Microsoft API	WolfCrypt	Java Classes	Vitis Security Library
RSA-KEM	√						
ECIES-KEM	√						
RSA-OAEP	√	√	√	√			
NTRU							
ECDH	√	√	√	√			
DH	√	√	√	√			

Table 6. Asymmetric Key Agreement Schemes & Encryption Schemes

	Bouncy Castle	OpenSSL	Crypto++	Microsoft API	WolfCrypt	Java Classes	Vitis Security Library
Miller-Rabin Primality Test	√						
Elliptic curve Primality Certificate		√		√			
Shawe-Taylor's Algorithm	√						

Table 7. Prime Number Generators

	Bouncy Castle	OpenSSL	Crypto++	Microsoft API	WolfCrypt	Java Classes	Vitis Security Library
HMAC-SHA-384-DRBG	√	√		√		√	√
HMAC-SHA-512-DRBG	√	√		√		√	√
SHA-512/224-DRBG	√	√				√	
SHA-512/256-DRBG5	√	√				√	
SHA-384-DRBG	√	√				√	
SHA-512-DRBG	√	√				√	
3-Key-TDEA-CTR-DRBG	√	√					√
AES-128-CTR-DRBG	√	√					√
AES-192-CTR-DRBG	√	√					√

Table 8. Deterministic Random Bit Generator

	Bouncy Castle	OpenSSL	Crypto++	Microsoft API	WolfCrypt	Java Classes	Vitis Security Library
Whirlpool	√	√	√			√	√
SHA-224	√	√	√	√	√	√	√
SHA-256	√	√	√	√	√	√	√
SHA-384	√	√	√	√	√	√	√
SHA-512	√	√	√	√	√	√	√
SHA-512/224						√	√
SHA-512/256						√	√
SHA3-224	√	√	√		√	√	√

SHA3-256	√	√	√	√	√	√	√
SHA3-384	√	√	√	√	√	√	√
SHA3-512	√	√	√	√	√	√	√
SHAKE128	√	√		√	√	√	√
SHAKE256	√	√		√	√	√	√
SM3	√		√				

Table 9. Cryptographic Hash Function

Some of the candidate algorithms listed in AKSA MySEAL 2.0 are not yet supported in the aforementioned 7 libraries/APIs. However, there are implementations available in other cryptographic projects and repositories. The main reason for their exclusion is that these ciphers are relatively new, even if they hold potential.

Below is a list of algorithms that have not yet been listed in any of the widely used cryptographic libraries or APIs as mentioned.

1. Symmetric Block Cipher: CLEFIA (all variants), PRESENT (all variants) & MISTY1
2. Symmetric Stream Cipher: KCipher-2, MUGI, Trivium & SNOW 2.0
3. Asymmetric Digital Signature: SM9, SDSA, ECSDSA & BLS
4. Asymmetric Key Agreement Schemes & Encryption Schemes: PSEC-KEM, ACE-KEM &NTRU
5. Prime Number Generators: Pocklington Primality Test, Probabilistic Lucas Primality Test, Deterministic Lucas Primality Test (Lucas-Lehmer) & Brillhart-Lehmer-Selfridge Primality Test
6. Deterministic Random Bit Generator: Streebog (all variants), Lesamnta, SPONGENT (all variants) & PHOTON (all variants)

Conclusion: Stronger Together

MySEAL 2.0 was initiated to ensure that the pre-qualified digital guardians are in tip-top condition. By reassessing the existing primitives, recruiting new algorithms, and ensuring their current maturity and popularity in real-world applications, AKSA MySEAL 2.0 is intended to continue protecting our digital lives. The next time you send a message or make an online transaction, remember the unsung heroes working behind the scenes to keep your data safe and sound.

Insider Threats In Organizations

By | Mohd Sharulnizam Kamarulzaman

In today's contemporary era characterized by the prevalence of information, the utilization of information technology (IT) is specifically tailored to incorporate a human-computer interface. This enables retrieval and utilization of data storage, be it for legitimate or unethical reasons. The perpetration of immoral activities involving information technology (IT) is frequently carried out by individuals within an organization (Crossler et al., 2013). These insiders often engage in such actions intentionally and with malevolent intent, hence presenting a significant security concern (Haines and Leonard, 2007; Liang and Xue, 2010). Examples of insider information leak include the illicit acquisition of personally identifiable information with the intention of engaging in fraudulent activities, misappropriation of intellectual property, or the illegal disclosure of sensitive or classified information by an insider to third parties without proper authorization (Greitzer and Frincke, 2010; Huth et al., 2013). The acts of theft and leakages are normally deliberate and malevolent in nature. According to Da Veiga and Eloff (2010), it is essential for an organization to prioritize employee behaviour while addressing information security concerns. The unethical and immoral use of computers and information systems is a matter of great significance, as highlighted by Kajzer et al. (2014). Cheng et al. (2013) further emphasize that individuals can be the most vulnerable element in terms of information system security. According to Willison and Warkentin (2013), this particular insight possesses the highest likelihood of causing significant harm and detriment to the employer. Therefore, it can be argued that insider activities and behaviour in information handling presents a significant impediment to information security within a business (Okere et al., 2012). Such assertion is supported by empirical research findings that establish the potential risks posed by individuals with privileged access to information systems (Da Veiga and Eloff, 2010; Omar, 2015; Rhee et al., 2009; Stanton et al., 2005). Insider risks are commonly associated with the human-computer interaction in relation to of permitted or illegal access. Furthermore, it is important to note that security mishaps can be attributed to poor insider attitude and a lack of awareness regarding security issues (Endsley, 1995; Greitzer et al., 2014; Greitzer et al., 2014). One crucial strategy in addressing these concerns involves implementing security awareness programs aimed at enhancing the knowledge and understanding of internal personnel on potential internal threats within an organization. Such knowledge empowers employees to take proactive measures in safeguarding valuable information assets (AlHogail and Mirza, 2014; Da Veiga and Eloff, 2010).

Historically, businesses place significant emphasis on safeguarding their physical assets, while neglecting to address the importance of education on acceptable human behaviours necessary to ensure security of information assets (Tseng and Fan, 2011). The lack of knowledge and awareness among individuals could contribute to a significant failure in effectively protecting an organizations' information assets, as reported by InfoWatch in 2016. This failure has subsequently resulted in several incidents of information leak and scandals. A recurring element observed in ethical scandals is the provision of ex post incentives to insiders by external entities (Tan et al., 2016). These individuals who possess privileged access to information are susceptible to various enticements from competitors or other entities, which may lead them to engage in deliberate acts of disruptive, unethical, or unlawful activity. With the lure of personal benefits, their actions result in compromise of sensitive information. The act of divulging confidential organizational information for personal benefit is a deceitful activity that poses a significant threat to the overall welfare of an organization (Omar, 2015). Engaging in such behaviour is considered unethical as it contravenes established organizational norms, as well as official and informal policies, rules, and procedures (Robinson & Bennett, 1995). Hence, it is imperative to allocate greater consideration to ethical concerns in safeguarding information assets, as this will be a prominent subject in information sharing (Da Veiga and Eloff, 2010).

In the contemporary digital landscape within a company's operations, human elements in the context of information leakage is particularly noteworthy since the accessibility and exchange of information are integral components of everyday routines. Regrettably, there is still a lack of comprehensive understanding among businesses on the human elements in information sharing that contribute to both

purposeful and inadvertent information leakage. This knowledge gap might be attributed to minimal study conducted on human factors in this context. Several psychosocial indicators have been identified as potential signs that an individual may be a malicious insider. These symptoms include feelings of disgruntlement, expressing disagreement with criticism, exhibiting rage, showing disengagement, displaying contempt for authority, and experiencing performance challenges (Greitzer & Frincke, 2010). Furthermore, the term "information leakage" can also encompass the unintentional loss of information that occurs when an individual neglects to update their password, fails to log off before departing from their job, or improper discarding of sensitive material such as shredding (McCormick, 2008; Warkentin and Willison, 2009). Interestingly, information leakages could also yield advantages. For example, corporations facilitating dissemination of volunteer information pertaining to a new innovative product or process (Harhoff et al., 2003). Such information leakage or spill could enhance diffusion. However, it is important to note that proprietary information has the potential of being leaked in an unregulated, undesirable, and potentially detrimental manner (Ritala et al., 2015). This would enable competitors to replicate and introduce similar products.

Irrespective of the specific nature and underlying motives of the leaking incidents, the consequences of such insider actions can manifest in financial detriment, organizational disruption, reputational damage, and enduring impact on the overall culture of an organisation. It is worth noting that the potential consequences of an incident is not based on a deliberate act, as even an inadvertent act of information leaks can yield equally detrimental outcomes as that of a deliberate and malevolent attack (Hunker & Probst, 2011). The objective therefore should be to mitigate outcomes irrespective of the underlying incentive (Hunker & Probst, 2011). The negative consequences of information leaking outweigh any potential benefits, making it a counterproductive activity (Marcus et al., 2016). There are strategies available to address such issue including employing mitigation approaches (Hunker and Probst, 2011).

Individuals intent on disclosing sensitive or proprietary information have many dissemination options at their disposal. Multiple methods, such as email, instant messaging, thumb drives, and other contemporary information technology tools, can exfiltrate or replicate gigabytes or larger quantities of data (Greitzer & Hohimer, 2011). The most effective approach to proactively prevent such leak is by doing an analysis on insider behaviour. Analysis could identify indicators and early warning signs that may be indicative of potential insider threat activity (Greitzer & Frincke, 2010). Such phenomenon is frequently detectable on the conduct exhibited prior to the committing an offense. Nevertheless, there may be challenges in distinguishing between what is considered "acceptable" insider behaviour and what is deemed "unacceptable" (Hunker & Probst, 2011).

Acknowledging insider threats as a manifestation of deviant human behaviour serves as a crucial initial step to effectively manage the dissemination of sensitive information, in addition to implementation of pre-existing technological safeguards. Insider threats can be identified when individuals exhibit unusual actions that depart from established policies or accepted norms of behaviour, regardless in these activities are driven by ignorance, malicious intent, or disrespect (Greitzer and Hohimer, 2011; Greitzer et al., 2008). In general, the disclosure of proprietary information is generally regarded as an unfavourable conduct by employees (Ritala et al., 2015). The impact of human behaviour on information sharing can have detrimental effects, whether it is due to deliberate or inadvertent misuse. Such conduct can result in a significant reduction in the value of information for both the organisation providing the information and the receiving organization within the supply chain. Therefore, it is imperative to identify the unique human characteristics associated with insider threats in order to effectively limit the risks. It is imperative for scholars and executives to explore suitable measures of information sharing to mitigate any adverse consequences of information leakage, and uphold integrity.

Organizations face substantial risks from individuals who possess both access to assets and a comprehensive understanding of its mechanisms. Due to the intricate nature, differentiating between the conduct of a typical employee and an atypical one can be challenging. Therefore, anticipating the likelihood of an employee engaging in undesirable behaviour prior to a security failure is of utmost importance. An employee exhibiting a significant level of threat may attempt to exert influence over fellow co-workers, encouraging them to engage in unlawful behaviour that could result in an information security breach. Hence, an in depth review of the interpersonal connections among co-workers and the evaluation of the spread of influence caused by insider threats are crucial in enhancing information security protocols.

References

1. AlHogail, A., & Mirza, A. (2014). Enhancing information security awareness through proper information security training programs. Journal of Information Security, (5), 1-13.
2. Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. Computers & Security, 39, 447-459.
3. Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. Computers & Security, 32, 90-101.
4. Da Veiga, A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. Computers & Security, 29(2), 196-207.
5. Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. Human Factors, 37(1), 32-64.
6. Greitzer, F. L., & Frincke, D. A. (2010). Combining traditional cyber security audit data with psychosocial data: Towards predictive modeling for insider threat mitigation. Insider Threats in Cyber Security, 85-113.
7. Greitzer, F. L., & Hohimer, R. E. (2011). Modeling human behavior to anticipate insider attacks. Journal of Strategic Security, 4(2), 25-48.
8. Greitzer, F. L., Cappelli, D. M., Moore, A. P., Trzeciak, R. F., & Cowley, J. (2008). Combating the insider cyber threat. IEEE Security & Privacy, 6(1), 61-64.
9. Greitzer, F. L., Kangas, L. J., Noonan, C. F., Brown, C., & Ferryman, T. (2014). Psychosocial modeling of insider threat risk based on behavioral and word use analysis. e-Service Journal, 9(2), 106-138.
10. Haines, J. W., & Leonard, L. N. K. (2007). Individual characteristics and ethical decision-making in an IT context. Industrial Management & Data Systems, 107(1), 5-20.
11. Harhoff, D., Henkel, J., & von Hippel, E. (2003). Profiting from voluntary information spillovers: How users benefit by freely revealing their innovations. Research Policy, 32(10), 1753-1769.
12. Hunker, J., & Probst, C. W. (2011). Insiders and insider threats – An overview of definitions and mitigation techniques. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 2(1), 4-27.
13. Huth, C. L., Chadwick, D. W., Claycomb, W. R., & You, I. (2013). Guest editorial: A brief overview of data leakage and insider threats. Information Systems Frontiers, 15(1), 1-4.
14. InfoWatch. (2016). Annual report on data leaks and confidential data theft. InfoWatch Analytical Center.
15. Kajzer, M., D'Arcy, J. P., Crowell, C. R., Striegel, A., & Van Bruggen, D. (2014). An exploratory investigation of message-person congruence in information security awareness campaigns. Computers & Security, 43, 64-76.
16. Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. Journal of the Association for Information Systems, 11(7), 394-413.
17. Marcus, B., Taylor, O. A., Hastings, S. E., Sturm, A., & Weigelt, O. (2016). The structure of counterproductive work behavior: A review, a structural meta-analysis, and a primary study. Journal of Management, 42(1), 203-233.
18. McCormick, W. T. (2008). Insider threat control: Using universal background investigations, behavioral indicators, and personality assessment. Security Journal, 21(4), 248-263.
19. Okere, I., Van Heerden, R., & Leenen, L. (2012). Indicators for insider threats and destructive worms in critical infrastructure networks. 2012 Information Security for South Africa, 1-8.
20. Omar, A. (2015). Mitigating risks of insider threats: Verifying identity, authorizing access, and monitoring behavior. Computer Fraud & Security, 2015(8), 13-18.
21. Rhee, H. S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. Computers & Security, 28(8), 816-826.
22. Ritala, P., Olander, H., Michailova, S., & Husted, K. (2015). Knowledge sharing, knowledge leaking and relative innovation performance: An empirical study. Technovation, 35, 22-31.
23. Robinson, S. L., & Bennett, R. J. (1995). A typology of deviant workplace behaviors: A multidimensional scaling study. Academy of Management Journal, 38(2), 555-572.
24. Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. Computers & Security, 24(2), 124-133.
25. Tan, J., Zhang, H., & Wang, L. (2016). Network analysis of insider trading in corporate information security. Journal of Management Information Systems, 33(4), 1099-1124.
26. Tseng, L. M., & Fan, Y. W. (2011). Exploring the influence of organizational ethical climate on knowledge management. Journal of Business Ethics, 101(2), 325-342.
27. Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: The insider threat. European Journal of Information Systems, 18(2), 101-113.
28. Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. MIS Quarterly, 37(1), 1-20.

IPED Digital Forensics: Unlocking The Power Of Open Source Investigation Tools

By | Aisyah Binti Mohamad Hafizul, Jayhanraaj Al Jeeva, Mohd Izuan Effenddy Bin Yusof, Muhammad Faridzul Bin Sukarni, Ummu Ruzanna Binti Abdul Razak

In today's digitally connected world, advanced digital forensics tools have become indispensable. From criminal investigations to cybersecurity incidents, professionals require reliable software to gather, analyze, and preserve electronic evidence. One such remarkable tool is IPED Digital Forensics, an open-source software solution developed by the Federal Police of Brazil. In this article, we will delve into the world of IPED Digital Forensics, its significance, and how it empowers investigators worldwide.

Understanding Digital Forensics

Before we deep dive into IPED Digital Forensics, let's revisit the fundamental concepts of digital forensics. In essence, digital forensics refers to the art and science of collecting, preserving, and analyzing digital evidence from various sources such as computers, mobile devices, and digital storage media. Such evidence can be crucial in solving crimes, ensuring legal compliance, and enhancing cybersecurity.

What is IPED Digital Forensics?

IPED, or the Integrated Platform for Digital Evidence, is a powerful digital forensics software suite which was developed and maintained by the Federal Police of Brazil in 2012. IPED - Digital Evidence Processor and Indexer (translated from Portuguese) is a tool implemented in java. Although it was developed on open source, its code was officially published only in 2019.

From the onset, the goal of the tool was to achieve efficient data processing and stability. Some key characteristics of the tool are:

- Command line data processing for batch case creation
- Multiplatform support, tested on Windows and Linux systems
- Portable cases without installation, which can be run from any removable drive
- Integrated and intuitive analysis interface
- High multithread performance and support for large cases: up to 400GB/h processing speed using modern hardware and 135 million items in a (multi) case as of 12/12/2019

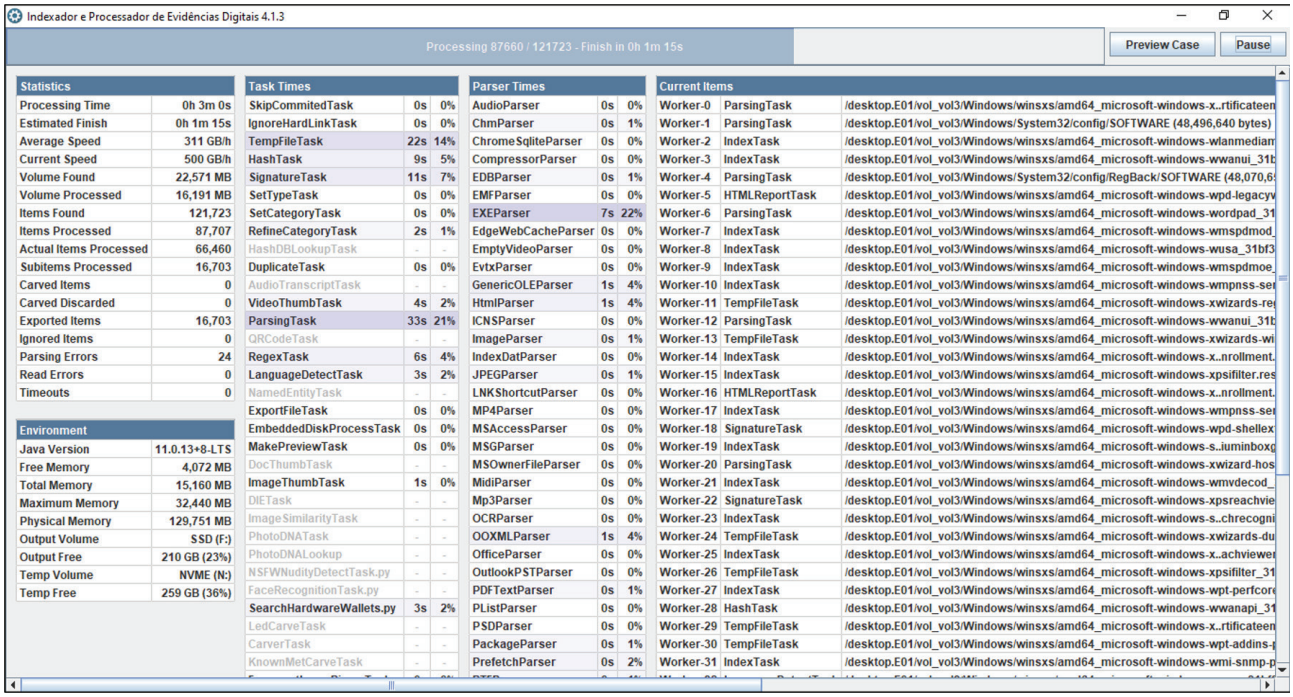


Figure 1.0 Multithread performances

Currently IPED uses the Sleuthkit Library only to decode disk images and file systems, so the same image formats are supported: **RAW/DD, E01, ISO9660, AFF, VHD, VMDK. There is also support for EX01, VHDX, UDF(ISO), AD1 (AccessData) and UFDR (Cellebrite) formats.**

IPED is designed to assist investigators, forensic experts, and law enforcement agencies in effective handling of electronic evidence. What sets IPED apart is its open-source nature, making it accessible to a global community of professionals.

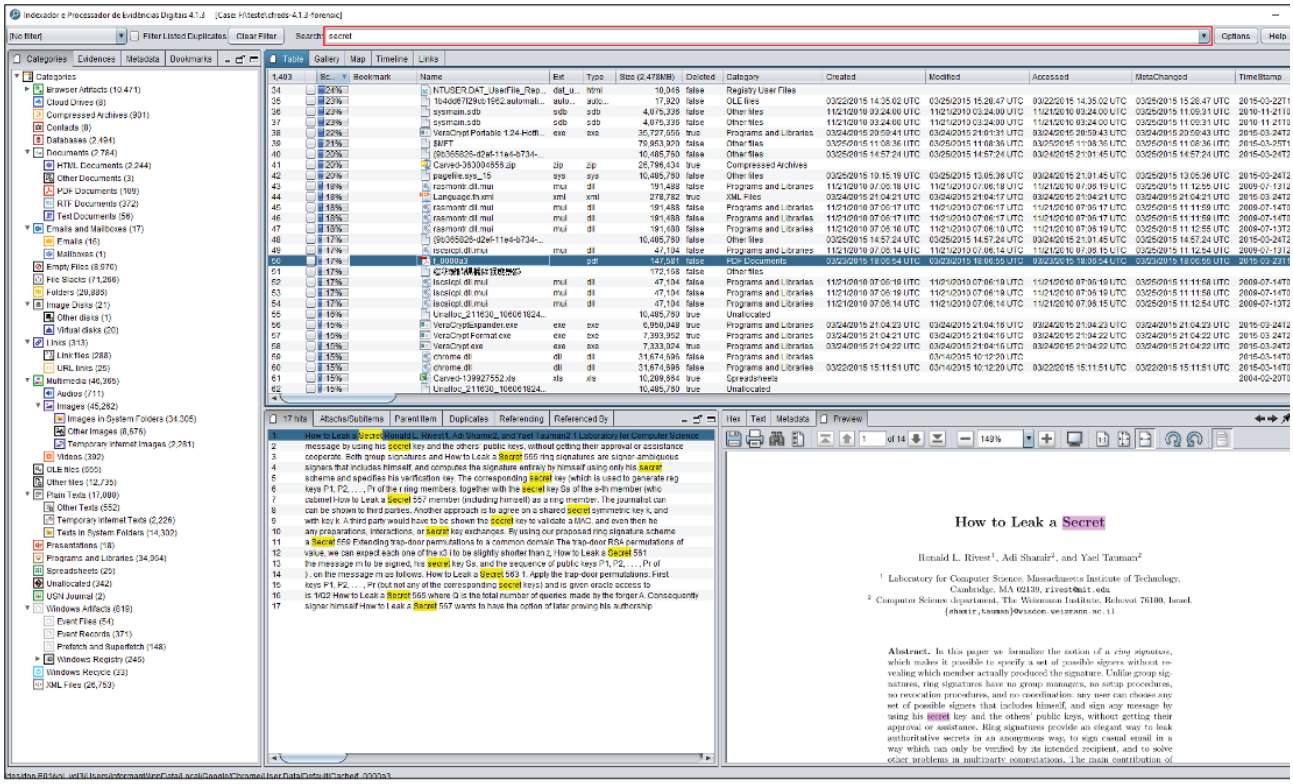


Figure 2.0 Analysis GUI

Power of Open Source

Open-source software, like IPED Digital Forensics, is built on the principles of transparency, collaboration, and accessibility. Here are some key reasons why open source is the future of digital forensics:

1. Collaboration: Open-source projects benefit from contributions made by a diverse community of experts worldwide. This collaborative approach fosters innovation and ensures that the software is continuously improved.

2. Transparency: Users can inspect the source code of open-source software, ensuring that there are no hidden vulnerabilities or backdoors. This transparency enhances trust and security.

3. Cost-Effective: Open-source software is often free to use, eliminating the need for expensive licenses. This makes it accessible to organizations with limited budgets.

4. Flexibility: Users can customize open-source software to suit their specific needs. This adaptability is crucial in the dynamic field of digital forensics.

Key Features of IPED Digital Forensics

Now, let's explore the remarkable features of IPED Digital Forensics that make it an indispensable tool for investigators:

1. Data Collection: IPED allows users to collect digital evidence from a wide range of sources, including computers, smartphones, external drives, and cloud storage. Such versatility is essential in modern investigations that involve diverse range of data types.

2. Data Processing: Once data is collected, IPED provides tools for efficient data processing. This includes data extraction, indexing, and keyword searching, enabling investigators to identify and

access critical information swiftly.

3. Analysis: IPED offers a suite of analytical tools, including timeline analysis, file carving, and the ability to generate detailed forensic reports. These features empower investigators in reconstructing digital events accurately.

4. User-Friendly Interface: Despite its robust capabilities, IPED maintains a user-friendly interface. This ensures that both seasoned professionals and those new to digital forensics can navigate the software effectively.

5. Multilingual Support: IPED supports multiple languages, making it accessible to a global user base. This inclusivity is a testament to the software's international relevance.

Some of IPED's key features include:

- Supported Hashes: IPED supports a variety of hashes, including md5, sha-1, sha-256, sha-512, and edonkey.
- Supported Hash Sets: IPED is compatible with various hash sets, including NIST NSRL, NIST CAID, ProjectVIC, Interpol ICSE, and standard CSV formats.
- Fast Hash Deduplication: IPED offers fast hash deduplication capabilities, streamlining the process of identifying duplicate data.
- Signature Analysis: The software provides signature analysis tools, aiding in the identification of known patterns and file types.
- Categorization: IPED categorizes files by type and properties, making it easier to analyze and prioritize evidence.
- Recursive Container Expansion: It supports the expansion of dozens of file formats within recursive containers, including DD, E01, EX01, VHD, VHDX, VMDK, and differential VMDKs.
- Image and Video Gallery: IPED offers support for hundreds of images and video formats, making it easier to view and analyze multimedia content.
- Georeferencing: It can georeference GPS data using mapping services like Google Maps, Bing, or OpenStreetMaps.
- Regex Searches: IPED allows for regex searches with optional script validation for various data types, including credit cards, emails, URLs, IP and MAC addresses, monetary values, and cryptocurrency wallet addresses (Bitcoin, Ethereum, Monero, Ripple, etc.).
- Embedded Viewers: The software provides embedded hex, Unicode text, metadata, and native viewers for comprehensive analysis.
- Indexing and Fast Searching: IPED supports file content and metadata indexing, enabling fast searching even for unknown files and unallocated space.
- Data Carving Engine: It features an efficient data carving engine that scans a wide range of file formats and is extensible through scripting.
- Optical Character Recognition: Powered by Tesseract 5, IPED offers Optical Character Recognition capabilities.
- Encryption Detection: The software can detect encryption in known formats and using entropy tests.
- Processing Profiles: IPED offers various processing profiles, including forensic, pedo (CSAM), triage, fast mode (preview), and blind (for automatic data extraction).
- Language Detection: It can detect more than 70 languages, enhancing its global usability.

Getting Started with IPED Digital Forensics

If you are eager to explore the world of digital forensics with IPED, here are the essential steps to get started:

1. Download and Installation: Begin by downloading the IPED software from the official repository on GitHub. You can download it via this link: IPED GitHub Repository (https://github.com/sepinf-inc/IPED). Installation is typically straightforward and does not require advanced technical expertise.

2. Training and Education: While IPED's user interface is intuitive, investing time in training and education is crucial. Numerous online resources, tutorials, and courses are available to help you become proficient in digital forensics with IPED.

3. Practical Experience: The more you practise, the better you become. Consider working on simulated cases, participating in digital forensics challenges, or collaborating with peers to gain hands-on experience.

Challenges and Considerations

While IPED Digital Forensics is a powerful tool, it's essential to be cognizant of certain challenges and considerations:

1. Hardware Requirements: Efficient use of IPED may require specific hardware configurations. Ensure that your computer meets the software's requirements to prevent performance issues.

2. **Learning Curve:** Like any professional tool, becoming proficient with IPED may take time. Patience and dedication are key to mastering the intricacies of digital forensics.

3. **Continuous Updates:** Digital forensics tools must stay up-to-date with the latest technologies and threats. Regularly check for updates and improvements in the IPED software.

Global Impact of IPED Digital Forensics

IPED Digital Forensics, with its open-source approach, has left a significant impact on the global digital forensics community. Law enforcement agencies, cybersecurity experts, and legal professionals worldwide have benefited from the software's accessibility and robust features. It has become a valuable tool in solving crimes, ensuring justice, and safeguarding digital assets.

Conclusion

IPED Digital Forensics stands as a shining example of open-source excellence in the field of digital forensics. Developed by the Federal Police of Brazil, this software has democratized access to powerful investigative tools, enabling professionals worldwide to uncover the truth, solve complex cases, and enhance cybersecurity efforts.

As we navigate an increasingly digitalised world, the role of digital forensics is ever more critical. IPED Digital Forensics, with its commitment to open source, collaboration, and transparency, is poised to play a pivotal role in the future of digital investigations. It empowers individuals and organizations to protect their digital assets, ensure justice, and maintain the integrity of digital evidence in an evolving technological landscape.

Reference

1. https://github.com/sepinf-inc/IPED

Cybercrimes: Types & Tips

By | Khairul Akma Mahamad & Raja Nur Zafira Raja Sharudin

Introduction

Rapid development in Internet technology and cyber space have created new opportunities for irresponsible people to exploit internet users. The number of cybercrime cases in Malaysia has been increasing year on year. Despite efforts by various enforcement agencies and government institutions, Malaysia remains a hotspot for cybercrime. The buzzword today is 'scam'. Nearly everyone from kids to the elderly has come to know of it. Yet many are still complacent about their online safety because they feel that they do not own anything of value to steal from. Many people unknowingly believe that their data is safe from cybercriminals if they minimise using the Internet or regularly delete their browsing history after each session. security practices can help minimize those risks. Securities Commission Malaysia has approved four digital asset exchanges (DAX) to operate in Malaysia that include Luno, SINEGY, Tokenize, and MX Global [3]. One of the most popular DAX in Malaysia is Luno which has been a reputable cryptocurrency exchange since 2015. The exchange takes its cyber security very seriously and has implemented various measures to ensure the safety of its user accounts and funds. Luno uses two-factor authentication (2FA) and email confirmation to prevent unauthorized access to user accounts.

Cybercrime and Statistics

According to Wikipedia, cybercrime is a type of crime that involves a computer or a computer network. The computer could be the tool in committing crime or a target of such crime.

Based on statistics by the Malaysia Computer Emergency Response Team (MyCERT), fraud has been consistently the highest incident that is reported every year as shown below in Figure 1.

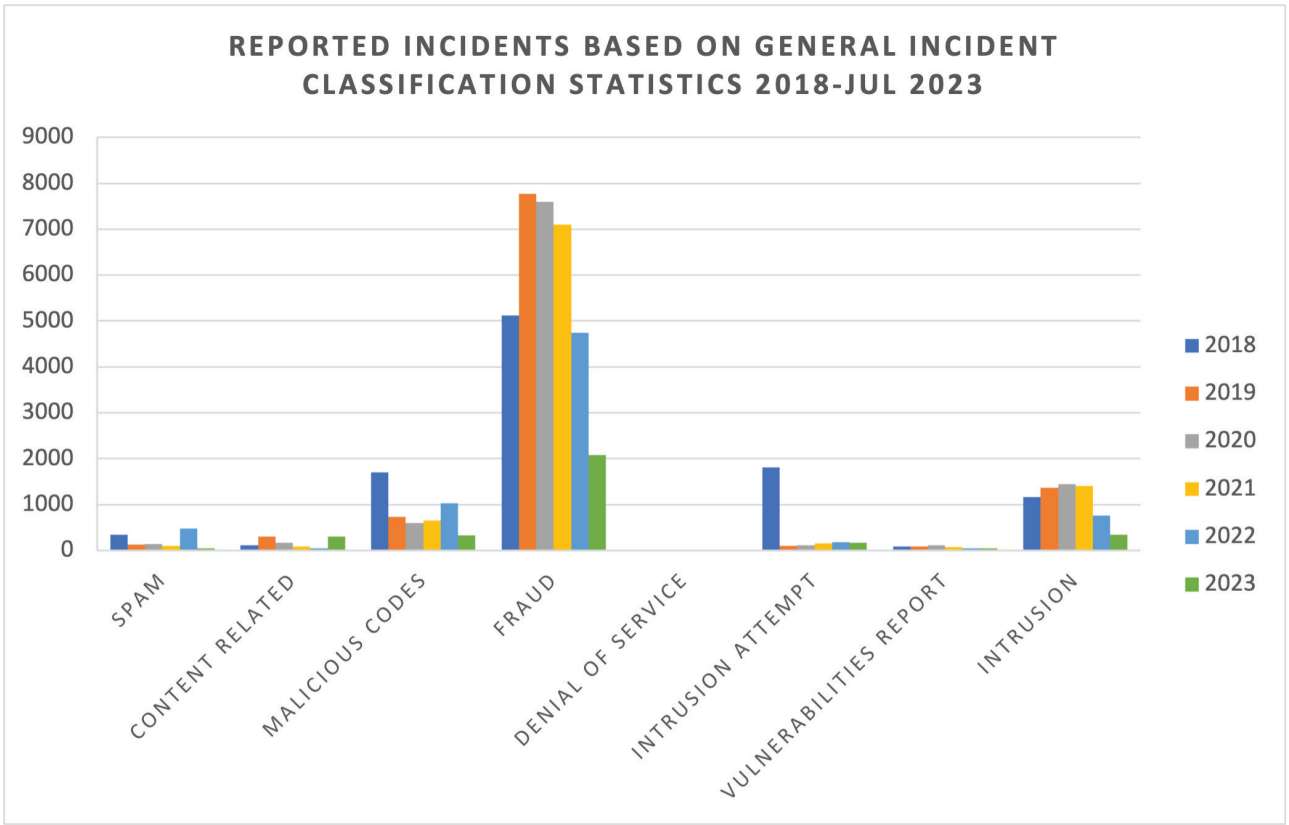


Figure 1 Security Incidents Statistics for year 2018 to Jul 2023 adapted from MyCERT

Types of Cybercrimes

Common types of cybercrime in Malaysia include phishing attacks, online scams, ransomware attacks, hacking, and malicious software distribution. Social engineering techniques, such as impersonation and pretexting, were also prevalent. The cybercriminal will find ways to steal personal information or monies from their victims. The techniques are summarised as follows:

a. Phishing

Victims of phishing often would receive an e-mail or SMS request from a so urce posing as a legitimate entity (e.g. banks, LHDN) to update their internet banking details. Once the attachment or the link in the email is clicked on, the victim will enter banking details such as user ID, password, ATM card number etc. in the phishing website. The suspect will then transfer money from the victim's bank account.

b. Online Fraud

Cyber criminals use e-mails, websites, chat rooms, and social media sites to make connections with victims. By exploiting the victims' trust, criminals deceive and manipulate them into giving up confidential information or even money to them. The types of online frauds include: scams, miracle cures, advance fees for credit cards, parcel scams, shopping and auction sites fraud, mule recruitment, "something is wrong with your PC", fake check scams, identity theft, business opportunities, "relative in distress", sweeps-take offer, foreign lottery, secret shopper, phishing emails, prize winner, charity donation, love scam, and many more.

c. Identity Theft

Cybercriminals steal victims' personal information such as full name, date of birth, or credit card number to commit financial fraud or other crimes, such as entering or exiting a country illegally, laundering money and drug trafficking. The consequences that follow can be detrimental to the victims.

d. E-Commerce fraud

The most popular e-commerce transactions associated with fraud occur in the airline industry, followed by general retail, electronics, ticketing, telecom, money transfers, toys, clothing, etc. Criminals use methods such as phishing and identity theft to facilitate the commission of the crime.

e. Ransomware

This malware can modify or block data on your computer. In order to restore the computer's performance and data, victims have to pay ransom to the cybercriminals. However, experts have warned that access to the blocked data or security of the computer is not guaranteed despite paying the ransom.

f. Botnet

A "bot" is a type of malware that enables an attacker to take control over an affected computer. Botnet is a network of infected machines ranging from a few hundreds to hundreds of thousands stretching across the globe. Many of these computers are infected without their owners' knowledge. Botnets can be used to carry out a variety of automated tasks, including sending spams, viruses, and spyware; steal sensitive information such as credit card numbers, banking credentials, and personal information; DDoS; and Click fraud.

g. Distributed Denial of Service (DDoS)

In a DDoS attack, hundreds or thousands of compromised machines (multiple computers and internet connections) are used to flood the access to a targeted system (this could be a machine, network resource, or website). Victims of a DDoS attack include both the end targeted system and all systems controlled by the hacker in the attack. DDoS attacks are usually distributed via botnets globally.

h. Love Scam

The victims are normally targeted via social media. The suspect will introduce himself as businessman or engineer or maybe pilot from other country. He will use 'charm' tactics such as enticing victim with luxury presents from overseas. The suspect then will ask the victim to make various payment e.g. tax, to claim such gifts. Besides that, suspect may request victim to assist him in paying other party for business purpose or to get inheritance money.

Tips and Advice

It is hard to imagine how much cybercriminals can make from the digital world. From online scams to ransomware, their methods are diverse and increasingly sophisticated. It is therefore crucial to guard against these attackers and prevent them from getting the upper hand on you.

Some tips to help prevent cybercrime:

- Do not share your banking information. A real bank would never ask for your bank account information, your debit card and PIN numbers, or other sensitive information (such as your IC number) via email
- Always double check the site address or email address in the provided link is accurate and genuine site
- Be careful with sales or offers
- Buy from trusted websites and do not compromise on safety features
- Ignore unknown individuals on social media
- Do not easily believe any social media acquaintance

How to Prevent Cybercrime and Challenges

Preventing Cybercrime

Given the constantly evolving nature of technology and cyber threats, cybercrime prevention is a complex and arduous challenge. Below are some key strategies to help prevent cybercrime:

a. Educate and Raise Awareness

Provide regular training and education to users, and general public on cybersecurity best practices. Include topics such as password hygiene, phishing awareness, and safe online behaviour.

b. Implement Strong Security Measures

- Use strong, unique passwords and two-factor authentication (2FA) for all accounts.
- Keep software, operating systems, and applications updated with the latest security patches.
- Employ robust firewalls, intrusion detection systems, and antivirus software.

c. Regular Backups

Maintain regular backups of critical data to ensure that you can restore your systems without paying ransom or losing valuable information in case of a cyber-attack.

d. Threat Intelligence

Stay updated on the latest cyber threats and vulnerabilities through threat intelligence sources to proactively reorganise your defences.

e. Incident Response Plan

- Develop and regularly update a comprehensive incident response plan to effectively manage and mitigate the impact of cyber incidents.
- Report any cyber threats to relevant authorities such as PDRM, KPDNKK, BNM and other relevant enforcement agencies.

Challenges in Preventing Cybercrime

Addressing cybercrime requires a multi-layered and holistic approach that involves technical solutions, policy changes, education, and collaboration. It is an ongoing effort that requires constant vigilance and adaptation to counter the evolving threat landscape.

a. Sophistication of Attacks

Cybercriminals continuously develop advanced attack techniques that can bypass traditional security measures.

b. Human Factor

Social engineering and phishing attacks exploit human behaviour, making it challenging to defend against human error.

c. Technological Evolution

As technology evolves, new vulnerabilities emerge, making it difficult to keep up with securing all aspects of the digital landscape.

d. Attribution and Enforcement

Identifying and prosecuting cybercriminals across international boundaries is complex due to the anonymity and technical expertise they possess.

e. Emerging Technologies

The adoption of new technologies like IoT and AI introduces new attack vectors that need to be addressed.

f. Insider Threats

Malicious or unintentional actions by employees or insiders can pose a significant risk to cybersecurity.

National Scam Response Centre

On 14 October 2022, the Prime Minister's Department announced that the National Scam Response Center (NSRC) has been established as an operational center to coordinate a rapid response to any online financial fraud. The

response includes speedy detection of stolen funds and enforcement action against criminals.

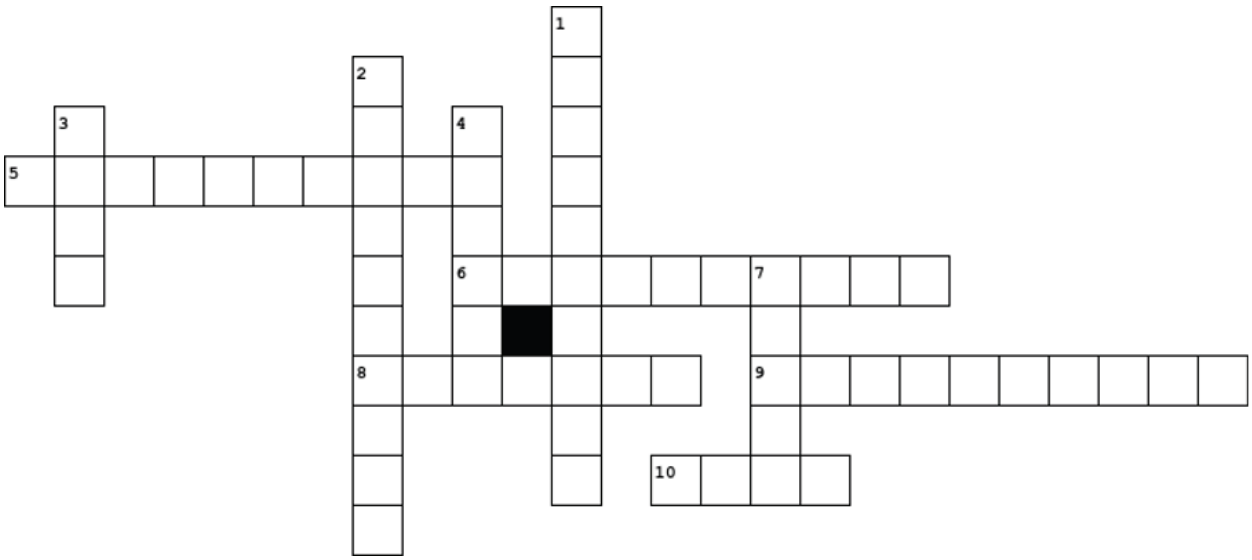
The NSRC is a joint venture between the National Anti-Financial Crime Center (NFCC), the Royal Malaysian Police (PDRM), Bank Negara Malaysia (BNM), the Malaysian Communications and Multimedia Commission (MCMC) as well as financial institutions and the telecommunications industry. The NSRC brings together resources and expertise from all these parties to combat financial fraud more effectively.

References

1. https://www.cybersecurity.my/en/index.html
2. https://www.oic-cert.org/en/index.html
3. https://www.oic-cert.org/en/awards.html
4. https://www.mcmc.gov.my/

Crossword Puzzle: Physical Security

By | Syahran Abdul Halim & Azirawati Abd Rahman



Across

5. Body measurements and calculations related to human characteristics
6. The process of risk assessment is risk _____
8. One of the physical security framework components
9. Physical security threat caused by natural
10. Most common type of physical security surveillance

Down

1. Moving people away from an area where they are in potential danger to a safer location
2. Access control weakness and risk
3. Situation involving exposure to danger
4. One of physical security main objective is to protect _____
7. Physical security risk

1. evacuation · 2. tailgating · 3. risk · 4. assets · 5. biometrics · 6. evaluation · 7. theft · 8. testing · 9. earthquake · 10. cctv ·

Unravelling The Web Of Scams In Malaysia

By | Jazannul Azriq bin Aripin

Scams have become an insidious threat in Malaysia, preying on unsuspecting individuals and causing significant financial and emotional distress. In a digital age where connectivity is constant, scammers have created diverse schemes to exploit people. It is crucial to shed light on the various scams prevalent in Malaysia, understand the tactics employed by scammers, and explore the impacts on victims and society. Additionally, we will delve into the government's response and provide practical tips to help individuals avoid falling prey to these deceptive practices.

Types of Scams in Malaysia

Malaysia faces a myriad of scams, ranging from traditional face-to-face deception to sophisticated online frauds. Online scams, including phishing and identity theft, have surged in recent years, capitalising on the increasing reliance on digital platforms. Phone scams, where scammers pose as authorities or bank officials, are also on the rise, manipulating victims into divulging sensitive information.

Another common type is an investment scam, which promises quick and lucrative returns. Malaysians often fall victim to these schemes due to the allure of easy wealth. Ponzi schemes and fake investment opportunities exploit the trust individuals place in financial ventures, leaving them with substantial losses.

Common Tactics Employed by Scammers

Scammers employ a variety of tactics to deceive their victims. Impersonation is a very prevalent tactic, with scammers posing as government officials, bank representatives, or even relatives in distress. Phishing, where fraudulent emails or messages trick individuals into revealing personal information, is another common tactic. Such scams play on trust and urgency, catching victims off guard.

Another manipulative technique involves creating fake websites or social media accounts to mimic legitimate businesses. Unsuspecting individuals may unknowingly share sensitive details, leading to identity theft or financial loss.

Impact on Victims and Society

The impact of scams extends beyond financial losses, affecting victims emotionally and straining social relationships. Families and communities often bear the brunt of the aftermath, as victims grapple with shame, guilt, and the burden of financial recovery. The elderly, in particular, are vulnerable, facing challenges in adapting to the rapidly evolving landscape of digital scams.

Society, as a whole, suffers from a loss of trust. The prevalence of scams erodes confidence in online transactions and communication, hindering the potential benefits of technological advancements. Addressing this issue is not only about protecting individuals but also about safeguarding the integrity of societal interaction.

Government Initiatives and Response

Recognising the severity of the issue, the Malaysian government has taken several steps to combat scams. Law enforcement agencies have increased efforts to track down and prosecute scammers, aiming to deter potential offenders. Public awareness campaigns have been launched to educate citizens about common scam tactics and how to recognise and avoid them.

Regulatory changes has been implemented to strengthen consumer protection and enhance cybersecurity measures. While these initiatives are steps in the right direction, continuous collaboration between the government, businesses, and the public is essential to stay ahead of the evolving strategies employed by scammers.

In 2023, CyberSecurity Malaysia organised National Anti-Scam Tour. This program was mooted by *Gabungan Bertindak Anti Scam* (GBAS), a coalition of several government agencies, non profit organisations (NGO), private entities, institutions of higher learning and supported by the Ministry of Communications and Digital. The program was organised to educate and enhance public awareness on various types of scams. In 2023, the program was organised at several

states namely Selangor/Wilayah Persekutuan Kuala Lumpur, Perlis, Sabah, Sarawak, Kelantan and also Wilayah Persekutuan Putrajaya.

Tips for Avoiding Scams

Protecting oneself from scams is a proactive effort that requires a combination of scepticism and awareness. Verifying the legitimacy of online transactions is paramount in an era where digital deception is prevalent. Individuals should exercise caution when sharing personal information, as scammers often exploit vulnerabilities through phishing attempts and deceptive tactics. Regularly updating passwords and employing two-factor authentication provide additional layers of security, mitigating the risk of unauthorised access to sensitive accounts. Staying informed about the latest scam tactics is crucial; as awareness empowers individuals to recognise potential threats. Sharing knowledge with friends and family also builds a collective defence within the community against evolving fraudulent activities.

It is essential to be wary of unsolicited messages, emails, or calls, regardless of how urgent they may seem. Verifying the identity of entities before providing any information is a compulsory practice to prevent falling victim to impersonation scams. Educating friends and family about common scams, monitoring social media privacy settings to control the dissemination of personal information, and exercising caution with email attachments are additional steps to enhance overall online security. By staying informed, employing best practices, and actively participating in reporting suspected scams, individuals play a vital role in fostering a safer digital environment for everyone.

Conclusion

In conclusion, understanding and addressing the issue of scams in Malaysia is a shared responsibility. By shedding light on the types of scams, tactics employed by scammers, and the impact on victims and society, would empower individuals to stay vigilant. The government's initiatives, coupled with practical tips for avoiding scams, lays a foundation for concerted effort to curb fraudulent activities. In a technologically connected world, avoiding scams is not only a personal duty but also communal responsibility to create a more stable and resilient society.

References

1. https://newswav.com/article/unravelling-the-scam-epidemic-understanding-and-addressing-scamming-in-mala-A2309_D3njGU

2. https://www.comparehero.my/fraud-scam/articles/how-to-avoid-scams-malaysia

3. https://www.nst.com.my/news/nation/2022/09/834531/online-scam-cases-increasing-malaysia

ChatGPT : Evolusi Kecerdasan Buatan

By | Nur Arafah binti Atan

Apa Itu ChatGPT

ChatGPT adalah sebuah mesin bot sembang (*chatbot*) berdasarkan kecerdasan buatan atau *Artificial Intelligence* (AI). Ia merupakan bot sembang yang mampu menjana sejumlah besar teks respon dari pelbagai bidang dan dalam pelbagai bahasa.

Latar Belakang ChatGPT

Pada November 2022, dunia digemparkan dengan kemunculan satu perkara baharu dalam bidang teknologi yang digelar 'ChatGPT'. Sistem ini dibangunkan oleh sebuah syarikat penyelidikan dan pembangunan AI iaitu OpenAI dan mempunyai pengkalan data (*database*) yang besar bagi penyimpanan maklumat.

Secara istilahnya, Chat bermaksud perbualan atau sembang manakala GPT adalah akronim bagi *Generative Pre-Training Transformer* iaitu model mesin yang menjana teks di alam maya sama seperti pemikiran manusia. Dalam kata lain, ChatGPT merupakan satu kemajuan teknologi bot sembang (*chatbot*) yang telah dicipta sehingga mampu melakukan pelbagai tugasan teks seakan pemikiran manusia. Ianya membantu memudahkan tugasan pengguna seperti pelajar, pekerja dan individu perseorangan. Cara ChatGPT beroperasi adalah mirip format percakapan antara dua individu (yang bertanya dan menjawab soalan).

Sebenarnya sistem bot sembang ini bukanlah sesuatu yang baharu kerana sebelum ini bot sembang telah pun banyak digunakan khususnya yang melibatkan pengurusan pelanggan seperti AirAsia AVA Chatbot, Chat with Shopee dan sebagainya. Walau bagaimanapun, sistem bot sembang ChatGPT adalah berbeza kerana ianya lebih meluas dan mampu memproses sejumlah besar teks respon dalam pelbagai perkara serta pelbagai bahasa melalui satu pelantar (*platform*).

Kelebihan ChatGPT

Penjanaan teks jawapan dan penyediaan informasi: Menerusi pengkalan data yang besar, ChatGPT sudah dilatih untuk menyimpan jutaan teks daripada internet sehingga apa jua maklumat yang diinginkan boleh diperolehi dengan mudah dan cepat. Penerapan kaedah *deep learning* pada ChatGPT mampu menjana teks respon yang lebih meluas merangkumi pelbagai perkara termasuk bidang perkhidmatan, pemasaran, pendidikan, kesihatan, kemahiran, seni dan sebagainya.

Kepelbagaian bahasa: ChatGPT mampu menjana teks respon daripada pelbagai bahasa di dunia dan Bahasa Inggeris merupakan bahasa utama dalam penyampaian maklumat. Penggunaan bahasa yang pelbagai ini mampu memperluaskan penyebaran ilmu dan maklumat kepada pengguna. ChatGPT juga membantu meningkatkan kemahiran berbahasa dan menulis dengan memberikan maklum balas tentang tatabahasa, perbendaharaan kata dan gaya, serta dengan membantu mereka membentuk ayat dan membuat suntingan kandungan bertulis.

Kecekapan masa: ChatGPT mampu mempercepatkan proses pengumpulan maklumat. Jika sebelum ini, sesuatu maklumat diperolehi dari pelbagai sumber dan pelbagai laman sesawang, namun melalui ChatGPT, hanya satu chatbot yang digunakan dan ianya mampu mengurangkan masa pencarian. Kita hanya perlu bertanyakan apa yang kita mahu dan chatbot ini akan menjawab kesemua pertanyaan dalam tempoh masa yang singkat (*in prompt*).

Perlaksaan pelbagai tugas: Kelebihan ChatGPT yang lain adalah kemampuannya dalam melaksanakan pelbagai tugasan berbeza seperti membuat ringkasan dokumen atau artikel yang panjang kepada sebuah ringkasan komprehensif sekaligus memudahkan pembacaan dan pemahaman pengguna. ChatGPT mampu membuat analisa teks, membantu menyelesaikan masalah koding dan sebagainya.

Kelemahan ChatGPT

Pemahaman yang terbatas: Berbeza dengan manusia, ChatGPT mengalami kesulitan dalam memahami sesuatu topik tertentu (specific) yang memerlukan pemahaman yang lebih mendalam, meskipun ChatGPT telah dibina untuk memahami kepelbagaian maklumat bersumberkan internet. Akibatnya, respon yang diberikan adalah berulang-ulang, tidak lengkap, kurang tepat dan tidak konsisten.

Tiada pemahaman emosi: ChatGPT tidak mampu memahami realiti dan emosi pengguna yang bertanyakan soalan. Sistem ini tidak memiliki empati seperti manusia. Oleh demikian, ia cenderung untuk memberikan respon yang terlalu umum dan tidak releven. Selain itu, jawapan yang diberikan juga kadangkala tidak masuk akal dan tidak bersesuaian dengan peringkat usia pengguna.

Penyalahgunaan maklumat: ChatGPT mampu memberi risiko kepada penyalahgunaan maklumat bagi sektor-sektor tertentu seperti berlakunya plagiat yang khususnya dikaitkan dalam bidang pendidikan dan penyelidikan. Selain itu, risiko penyalahgunaan maklumat dan idea yang mampu mendatangkan ancaman keselamatan dan keharmonian negara mungkin akan berlaku.

Memerlukan jaringan internet yang stabil: Untuk mengakses ChatGPT, pengguna memerlukan jaringan internet yang stabil bagi memastikan sistem ini dapat berinteraksi secara maksimum. Sekiranya jaringan internet lemah, maka chatbot ini akan banyak menampilkan *bug* dan tidak boleh memberikan jawapan sesuai seperti yang diharapkan.

Rumusan

Secara umum, kita boleh nyatakan bahawa ChatGPT ini merupakan sebuah sistem atau platform yang mampu memudahkan pengguna untuk mencari maklumat dan informasi yang merangkumi pelbagai bidang dalam pelbagai bahasa pada bila-bila masa. Namun begitu, adalah penting untuk memahami kelemahan yang terdapat pada platform ini. Justeru, pemikiran manusia yang waras dan pemahaman yang tidak terbatas masih diperlukan bagi menganalisis kepelbagaian maklumat yang diberikan oleh ChatGPT. Kebijaksanaan manusia adalah kunci kepada meminimumkan risiko dan memaksimakan manfaat penggunaan platform ChatGPT.

Rujukan

1. Apa Itu ChatGPT Dan Cara Penggunaannya https://www.mysumber.com/chatgpt.html | Mysumber.com

2. ChatGPT dan kesannya terhadap pendidikan anak-anak kita https://berita.mediacorp.sg/komentar/komentar-chatgpt-dan-kesannya-terhadap-pendidikan-anak-anak-kita-750636

3. Cabaran dan kelebihan ChatGPT kepada pendidikan https://www.astroawani.com/berita-malaysia/kolumnis-cabaran-dan-kelebihan-chatgpt-kepada-pendidikan-403854

4. Fenomena ChatGPT, Ketahui Kelebihan dan Kekurangannya https://netciti.co.id/article/fenomena-chatgpt-ketahui-kelebihan-dan-kekurangannya

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

CyberSecurityMalaysia
cybersecuritymy
cybersecuritymy
CyberSecurity Malaysia
cybersecurity_my

MINISTRY OF DIGITAL

ISSN 1985-1995