Strengthening Information Security Management, Human Capital Capabilities and Technology Enhancement Towards Business Excellence: New Strategy for Post-COVID 19 Era


Dr Fazlida Mohd Razali


Prof. Dr Jamaliah Said


Dr Salwa Zolkaflil


Dr Afzal Izzaz Zahari


Dr Muhamad Khairulnizam Zaini


Zulaikha Amirah Johari

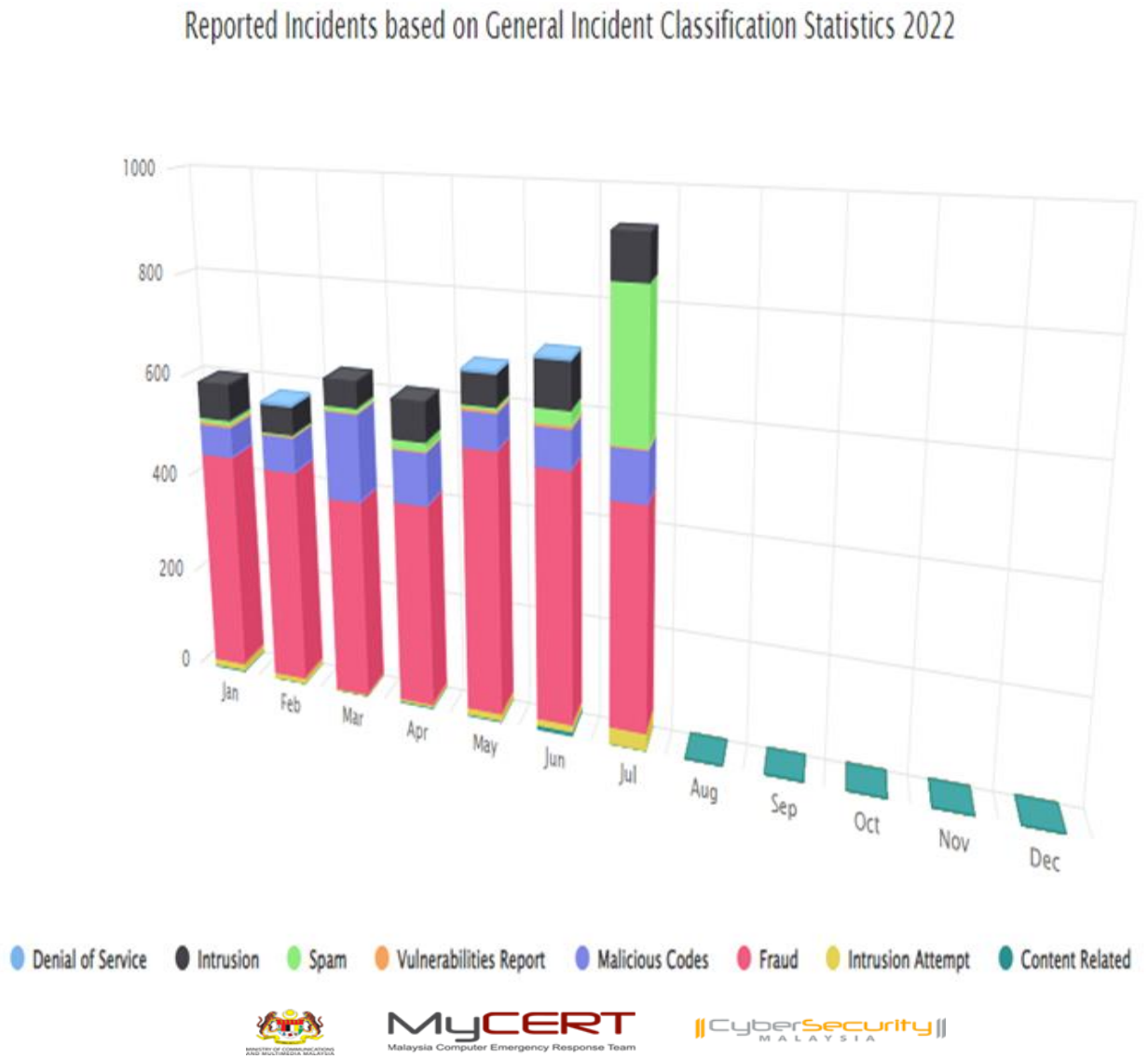
Research Symposium 2022:

"Towards an Inclusive Malaysia: Research Insights on the Implications of Digital Communications on Society"

Introduction

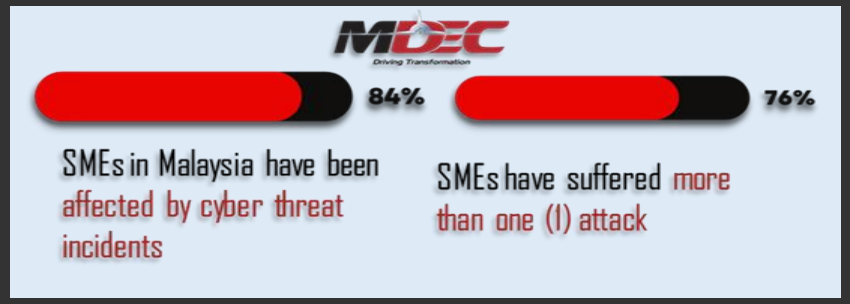
- COVID-I9 has changed the way businesses are conducted.
- When most business activities were conducted via online organizations' data were exposed to **Information Security Risk (ISR)** susceptibility (Wahab, 2022).
- In Malaysia, a total of 838 incidents of cybersecurity was reported to CyberSecurity Malaysia between the start of the Movement Control Order (MCO) on March 18 to April 7 (Keng,2020).
- Southeast Asian countries are still lagging in the cybersecurity area thus being targeted for cyber-attacks; with Indonesia, **Malaysia**, and Vietnam serving as global launchpads for malware attacks (CCM, 2021).

UNIVERSITI TEKNOLOGI MARA | Institut Penyelidikan Perakaunan | MCMC | DSRG DIGITAL SOCIETY RESEARCH GRANT



Introduction

- SMEs are badly affected by the pandemic COVID 19, thus, requires urgent need for digital adoption in order to sustain.
- Digitalization and transformation expose SMEs to information security threats such as malicious emails, phishing attacks, fraud and malware (Wahab, 2022).
- Based on recent studies among the SME sectors in Malaysia, 84% of SMEs are affected by cyber incident and 76% have suffered more than one cyberattacks.



WHY SMEs??

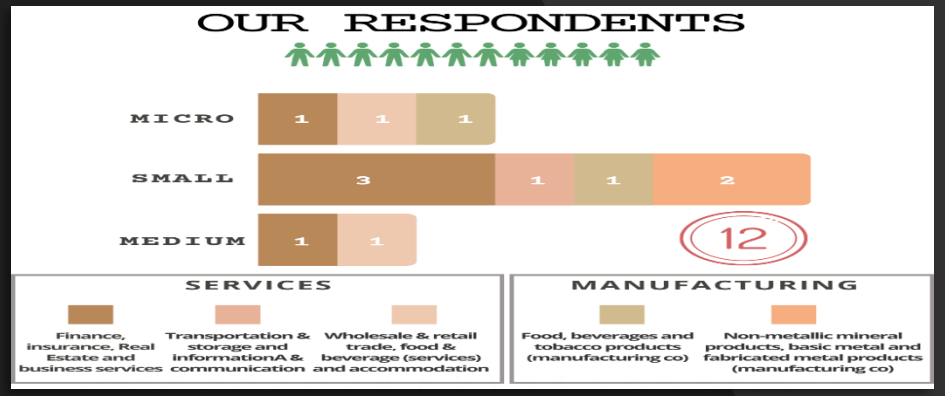
- ❑ SMEs are basically still using outdated technology defense.
- ❑ Lack of good or sound policy or guidelines
- ❑ Lack awareness and training on cybersecurity competency
- ❑ Giving less time and resources to incorporate investment in cybersecurity.

Datuk Dr Amiruddin Abdul Wahab
Chief Executive Officer
Cybersecurity Malaysia (CSM)

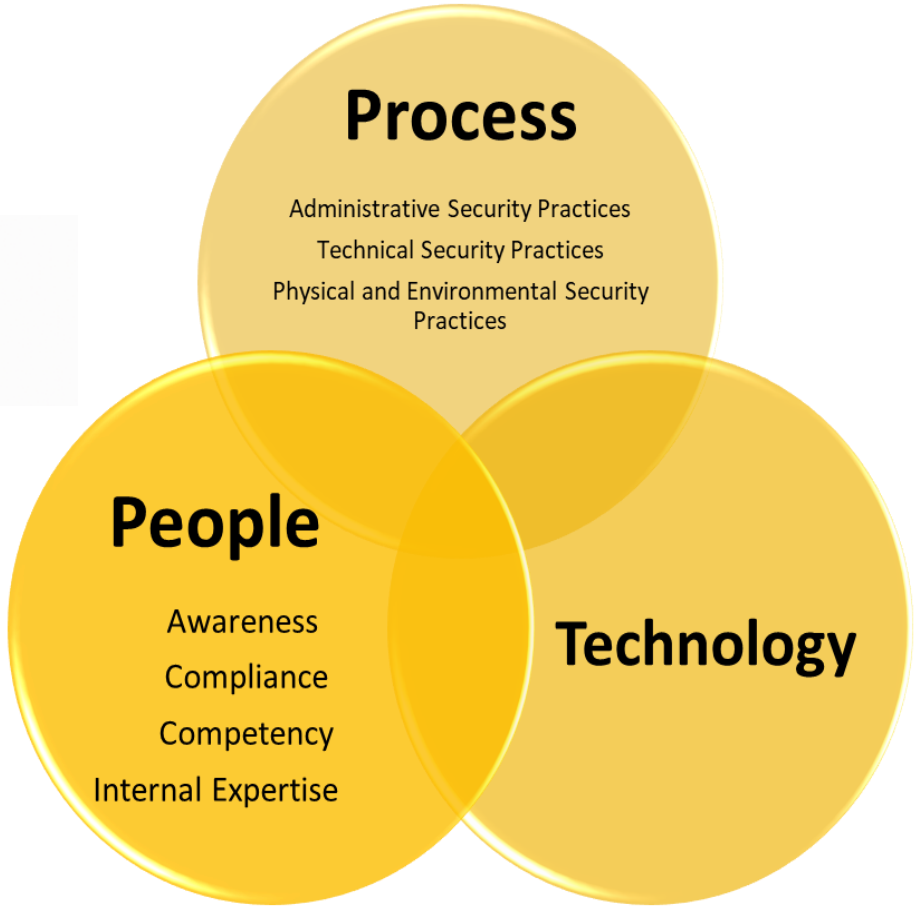
Introduction

Observing the vulnerability of information security threat on SMEs this study aims to:

1) To investigate the level of SMEs' readiness in managing information security risk.
2) To explore the challenges faced by the SMEs in managing information security risk.
3) To investigate the impact of information security threats on SMEs' business agility



Institut Penyelidikan Perakaunan
MCMC
DSRG
DIGITAL SOCIETY RESEARCH GRANT

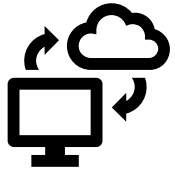


Dynamic Capabilities

FINDINGS : READINESS (RO1)

- Lack readiness in **Administrative Security Practices (ASP)** - No formal policy on Information Security.
- Dealing with the “cyber threat incident” on a case-by-case basis.
- Did not impose any regulation on data security to counterparts.
- Lack readiness in **Technical Security Practices (TSP)** - over-reliance on the Cloud provider to back up the enterprises’ information assets.
- In the WFH setting, SMEs faced Access Control and Password difficulties, especially when the staff used their own device.

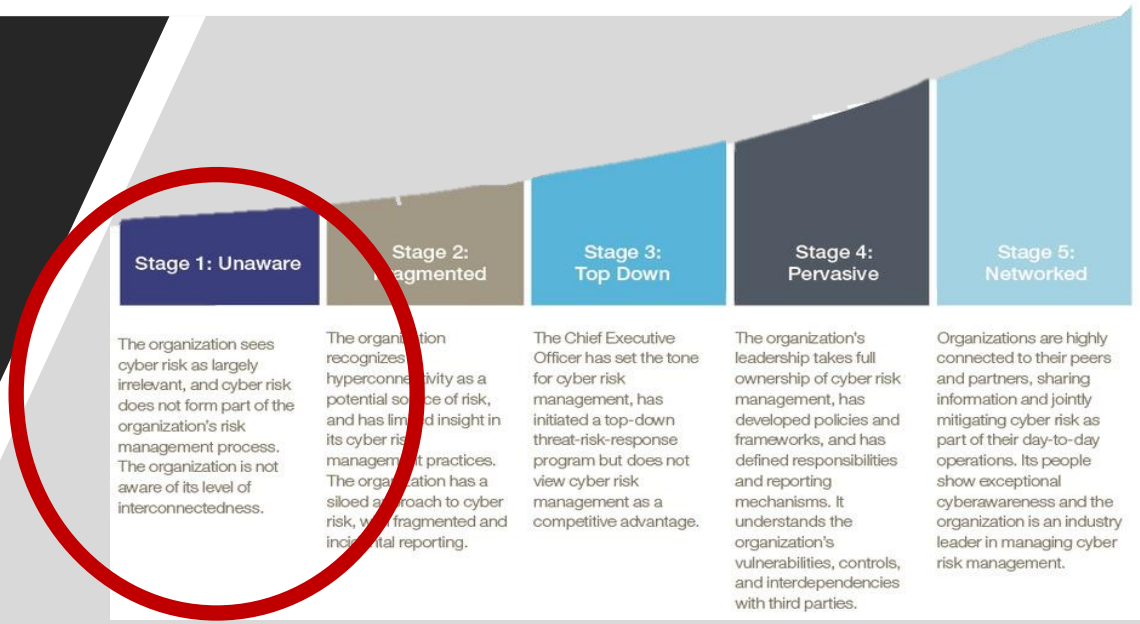
- **Awareness** - Basic awareness of information security threats - depend on key personnel who possess an IT background as the center of reference.
- **Competency** - All SMEs have at least basic knowledge of information security.
- **Internal Competencies** - highly dependent on one person in charge (PIC), which oversees admin-related matters.
- **Tone at the top** play crucial role in initiative to create awareness and increase competencies in organization.



- Using standard **Microsoft Windows Defender** and opined that the current control is sufficient.
- SMEs prefer to outsource internal applications to **Application Services Provider (ASP).**
- SMEs use software and media platforms readily available in the market.
- Most SMEs opined that investment in more advanced technology would be made once **fully integrated systems** are implemented in-house.

FINDINGS : READINESS (RO1)

- SMEs should clearly define their information asset and establish proper security control.
- Specifically, micro-companies under review own “Intellectual Property (documented or undocumented knowledge, creative ideas, or expressions of the human mind that have commercial (monetary value), which is insufficiently documented and protected from internal and external threat.
- SMEs to refer to “Information Security Guidelines for Small and Medium Enterprises” issued by Cybersecurity Malaysia to start implementing Information Security Practices at their enterprise.
- SMEs to participate in online free training/webinar/awareness sessions widely available to better understand and obtain necessary information security skills.



World Economic Forum’s maturity levels of cyber security”

Micro and a few small enterprises can be categorized under “**Stage 1: Unaware**”. Specifically, the enterprises see cyber risk as largely irrelevant, and cyber risk does not form part of the enterprise’s risk management process.

FINDINGS 2: READINESS OF SMEs (RO1) - cont'

- The SMEs recognise digitalisation has a potential risk, but they have limited insights into its information security risk management practices.
- Despite the inexistence of formal policy, the enterprises have a practice in place but prefer to handle incidents on a case-by-case basis.
- As SMEs under this category have future planning on "fully automated systems", it is suggested that SMEs take the initial initiative to formalize the information security practices based on ISO/IEC 27001:2013 standards.

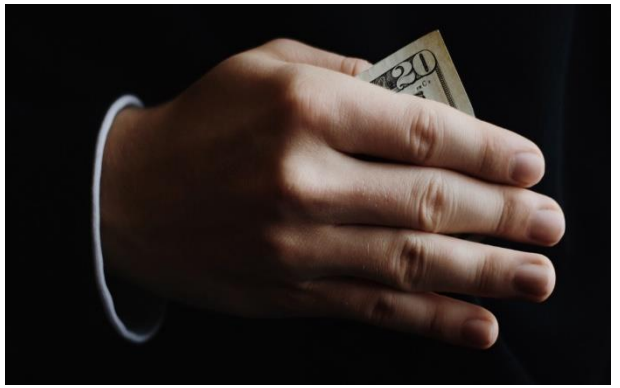
World Economic Forum's maturity levels of cyber security"

The remaining SMEs under review are still at the 2- stage, which is **fragmented**.

FINDINGS 2:
CHALLENGES FACE BY SMEs (RO2)

Lack Management Buy-in

- Data was not sensitive.
- No urgency on having proper Information Security Practices.
- Insignificant financial implication and severe business disruptions.
- Investment does not contribute to Return on Investment .



Limited Resources

- Limited financial resources - priority for operation.
- Limited internal expertise - No specific staff overseeing InfoSec.
- Highly dependent on key person -

Limited Knowledge

- Difficulty to keep the staff updated on evolving risk of cybercrime and finding a way to manage it competently.
- Lack of knowledge on the best technology and supplier that can best meet the need of SMEs.

RECOMMENDATION:

INFORMATION SECURITY PRACTICES

- SMEs can refer to “Information Security Guidelines for Small and Medium Enterprises” issued by Cybersecurity Malaysia to get started on implementing Information Security Practices at their organisation.
- Management commitments and assistance from related authorities, such as SME Corps, MDEC, Cybersecurity Malaysia, to create awareness on the importance of implementing InfoSec management practices for their business.
- SMEs to work with MDEC, SME Corp and NACSA to be part of the “Matrix Collaboration Programme” to get more information on solutions provided by this programme to manage cybersecurity challenges faced by SMEs with affordable packages.
- Stakeholders (i.e., SME Corp, MDEC etc.) work together with the media to create awareness among SMEs on cybersecurity threats and their consequences on businesses and how they would affect agility.

RECOMMENDATION:

INFORMATION SECURITY PRACTICES

- SMEs should establish a “Bring Your Own Device (BYOD)” policy to compel employees, especially those working with official and critical data, to safeguard the information asset.
- Specifically, CyberSecurity Malaysia could provide a specific guideline on best practices for working from home setting and avoiding cybersecurity crimes. For further outreach, SME Corp can collaborate with CSM Malaysia to create awareness on the information security risk when working from home.
- Third-party service providers (i.e., Telecommunication Companies, Financial Services Companies, or Consulting Companies) should include cybersecurity features in their package.

RECOMMENDATION:

HUMAN CAPITAL CAPABILITIES

- The tone at the top is crucial to inculcate awareness and compliance on Information Security. SME's top management, particularly the owners, should exercise due care and due diligence in protecting their information assets.
- SMEs should also emphasise Security Education, Training & Awareness (SETA) to increase staff's competencies and awareness.
- It is suggested that SMEs participate in online free training/webinar/awareness sessions that are widely available.
- SMEs should establish a "Community of Practice (CoP)" as a platform for sharing best practices and experiences related to information security.
- Upskilling and Reskilling are vital for SMEs to survive in the digital business ecosystems when they know how they can handle security issues accordingly.

RECOMMENDATION:

HUMAN CAPITAL CAPABILITIES

- Authority to continuously provide SETA for SMEs to establish security awareness, competencies, and culture.
- MCMC could provide a specific guideline on best practices, for example, the “Klik Dengan Bijak” awareness campaign
- NGOs or professional bodies may also conduct webinars or share short videos on cyber security and information security information. This will be a good initiative to create an effective cyber resilient society. The videos will not only help SMEs but the public at large.
- To establish dedicated website on cybersecurity awareness that will share information related to cyber security and provide a one-stop center for SMEs to find solutions for any problem about cyber security.
- Related agencies could provide short modules on information security through social media such as Youtube for references and self-learning.

RECOMMENDATION:

HUMAN CAPITAL CAPABILITIES

- SMEs should establish proper “Information Security Governance” to have clear authority and responsibility in managing information security.
- Establishing the formal policy on information security could help SMEs segregate the duties on information security (i.e., who to handle incidents) to avoid over-reliance on key personnel. By having a clear guideline, the person in charge may not necessarily be an IT expert.
- The fact that information security has gained attention, relevant government agencies should upgrade the competencies of existing cybersecurity practitioners and nurture a new generation of credible cybersecurity practitioners.

RECOMMENDATION:

TECHNOLOGY

- SMEs to initiate the acquisitions of cost-effective security technology, tools, and technical services to ensure that all information assets residing in the SMEs' information systems can be safeguarded, thus reducing the probability of facing business disruptions due to security incidents.
- SMEs to work with MDEC, SME Corp and NACSA to be part of the "Matrix Collaboration Programme" to get more information on solutions provided by this programme to manage cybersecurity challenges faced by SMEs with affordable packages.
- Cybersecurity services providers have less interest to promote their services to SMEs due to the low rate of return. Agencies like SME Corp should facilitate the arrangement to get the best deal from the cybersecurity service providers.
- Partnership programmes on assessing InfoSec related matters could be held between SME owners, associations, and government agencies.
- Information security promotion through events, such as SME Day, SME conventions, and SME exhibitions, should be further enhanced.

FINDINGS 3: BUSINESS AGILITY (RO3)

Mostly all SMEs has experiences cybersecurity threats, but it has no significant impact on business agility.
.

Human capital capability contributes a lot in ensuring the business agility during COVID-19.

Majority of the company put effort in digitalizing their business process by hiring third party since they aware of the benefit of digitalizing the process which in turn affect their business agility and competitive advantage.
.

Support needed for agility include financial assistance in the form of grant and solutions that best fit their nature of business
.

Technology enhancement does have big contribution on ensuring the survival and agility of micro enterprise.

CONCLUSION

- To sustain and stay competitive in the post-COVID period, information security risk, particularly cybersecurity, must be addressed and mitigated efficiently.

- To survive, SMEs need to strategize on optimizing their “Dynamic Capabilities” specifically “process (Information Security Practices), people (human capital capability), and technology” to create a competitive advantage.

- Since SME main obstacles to implement sound information security practices is lack of management buy-in and financial constraint, they must have the ability to integrate, build and coordinated internal and external competencies to combat rapidly evolving information security threat.

- Clearly, to survive and create a competitive advantage, the ability to exploit an existing opportunity, create opportunity and ability to foresee emerging threats is crucial (Hussain Shah, Ahmad, Maynard, & Naseer, 2019).

THANK YOU

- Dr Fazlida Mohd Razali, CA(M), AIIA (M)
- Accounting Research Institute (ARI) UITM
- Area of Research: Audit, Governance, Risk Management, Forensic Accounting Information Security
- Email: fazlida@uitm.edu.my
- H/p: 0126520452