CyberSecurity MALAYSIA

AN agency under MOSTI

Information Security
Guidelines for
Small & Medium Enterprises (SMEs)

Mohd Nazer Apau
Sabariah Ahmad

COPYRIGHT

NO ENDORSEMENT

Products and manufacturers discussed or referred to in this document, if any, are presented for informational purposes only and do not in any way constitute product approval or endorsement by CyberSecurity Malaysia.

Registered office:
CyberSecurity Malaysia,
Level 7, Block A, Mines Waterfront Business Park,
No 3, Jalan Tasik, The Mines Resort City,
43300 Seri Kembangan, Selangor, Malaysia
Phone: +603 - 8992 6888
Fax: +603 - 8945 3205
Web : http://www.cybersecurity.my

TRADEMARKS

All terms mentioned in this document that are known to be trademarks or service marks have been appropriately capitalised. CyberSecurity Malaysia cannot attest to the accuracy of this information. Use of a term in this document should not be regarded as affecting the validity of any trademark or service mark.

WARNING AND DISCLAIMER

Every effort has been made to make this document as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on “as is” basis. The authors and CyberSecurity Malaysia shall have neither liability nor responsibility to any person or entity with respect to any losses or damages arising from the reliance to the information contained in this document.

ACKNOWLEDGEMENT

CyberSecurity Malaysia wishes to express gratitude to the contributors who may directly or indirectly contribute to the completion of this guideline. In addition, we wish to thank the panel of reviewers (Internal & External) who reviewed the drafts of this guideline.

Contributors

1.	Tengku Azmi Tengku Majid	Malaysia Productivity Corporation (MPC)
2.	Mohd Zaihasry Zainal	Internal Audit, Private Hospital
3.	Norazman Kassim	SK Excel Sdn. Bhd.
4.	Azah Anir Norman	University of Malaya
5.	Mohd Azlan Mohammad	BETANEXUS (M) Sdn Bhd
6.	Yuzida Md Yazid	Knowledge Management (Library)

Internal Reviewers

1. Lee Hwee Hsiung
2. Maslina Daud
3. Lt Col Asmuni Yusof (Retired)
4. Noor Aida Idris
5. Nazhalina Dato' Nazri
6. Ida Rajimee Ramlee

External Reviewers

1.	Tengku Azmi Tengku Majid	Malaysia Productivity Corporation (MPC)
2.	Azah Anir Norman	University of Malaya
3.	Haslizah Husin	Export-Import Bank of Malaysia
4.	Mokhzamir Aznan Mohamed Hassan	Bank Pembangunan Malaysia Berhad
5.	Abdul Razak Hussin	SME Bank Malaysia
6.	Azlan Mohamed Ghazali	iPerintis Sdn Bhd

Table of Contents

EXECUTIVE SUMMARY

It is a fact that in this increasingly “inter-connected” world demanding a perfect security framework would be close to impossible to ask for and no measures can be implemented in any organisation to achieve such perfection. Nevertheless, something needs to be done in order to achieve complete and effective control. The risks and threats are inevitable hence these uncertainties must be managed correctly and carefully. There are information security incidences involving large organisation which failed to manage their information security concerns and cost them huge financial losses.

The same could happen to any organisation including Small and Medium Enterprises (SMEs) if the entrepreneur or the SME business owner did not adopt a serious stance on information security concerns. For SMEs to survive and sustain in the domestic and global market, entrepreneurs must consider Information, Communication and Technology (ICT) as the platform to grow and not shunned due to the emerging threats and risks. The Malaysian government encourages SMEs and entrepreneurs to leverage their businesses on the current ICT infrastructure that is available.

Traditionally, protecting physical assets would be much easier as it involves tangible items. For example, SMEs could hire more security personnel within their premises in order to protect machines and equipments or even cash. Those are no longer considered practical options since most SMEs are dealing with digital information as well. Digital information is considered to be intangible asset. It consists of Intellectual Property (IP), copyrights, trade secrets, business strategies and any other information that are deemed valuable to the organisation. These valuable data must be reasonably protected to avoid risks associated with its loss or leakage due to physical and logical attacks like stolen assets, Distributed Denial of Services (DDOS), malwares like Trojan Horse attacks, viruses, worms and many other types of cyber attacks. Furthermore, the existence of SMEs is justified based on the profit that they are making. Hence, SMEs must acknowledge the reasons why information as an asset needs to be protected.

This guideline serves to inculcate awareness, the understanding and guidance for SMEs in relation to information security and the way forward in managing it.

1 QUICK ASSESSMENT CHECKLIST

Appendix A in this guideline (1PAGE ASSESSMENT – FOR SMALL & MEDIUM ENTERPRISES) contains a set of 30 questions measuring information security readiness and implementation within your company. Additionally, by responding to the questions, it would test your basic awareness of information security. The checklist was designed to be answered by SMEs' managers and/or individuals who can make decisions relating to enterprise business directions and its operations.

You should respond to the questions listed sincerely and analyse the outcome prior to reading this material in complete. If you can achieve 200 marks with reasonable effort, you can skip reading the entire guideline if you want to. Nonetheless, it is essential to read the entire guideline in order to assist you in answering the questions from the checklist.

2 TERMS & DEFINITIONS

For the purposes of this Guideline, the following terms and definitions apply.

Assets	Anything that has value to the organisation[1].
Tangible assets	Cash, equipment, machinery, plant, property or anything that has long-term physical existence or is acquired for use in the operations of the business and not for sale to customers. In the balance sheet of the business, such assets are listed under the heading Plant and equipment or Plant, property, and equipment. Tangible assets, unlike intangible ones, can be destroyed by fire, hurricane, or other disasters or accidents. However, they can be used as collateral to raise loans, and can be more readily sold to raise cash in emergencies[2].
Intangible assets	Intangible assets are non-physical resources and rights that have a reputation, name recognition, and intellectual property values such as knowledge and know-how. Intangible assets are generally classified into two broad categories: (1) Limited-life intangible assets, such as patents, copyrights, and goodwill, and (2) Unlimited-life intangible assets, such as trademarks[3].
Threats	A potential for violation of security, which exists when there is a circumstance, capability, action, or an event that could breach security and cause harm[4].
Incidents	An incident the likes of an adverse network event in an information system or network or the threat of the occurrence of such event[5].
Vulnerability	The state of being vulnerable or exposed; susceptibility to injury or attack[6].
Malware	A generic term for a number of different types of malicious codes[7].
Virus	A programme or piece of code that is loaded onto your computer without your knowledge and runs against your wishes. Viruses can also replicate themselves. All computer viruses are man-made. A simple virus that can make a copy of itself over and over again is relatively easy to produce. Even such a simple virus is dangerous because it will quickly use all available memory and bring a system to a halt. An even more dangerous type of virus is one capable of transmitting itself across networks and bypassing security systems[8].
Worm	A programme or algorithm that replicates itself over a computer network and usually performs malicious actions, such as using up resources and possibly shutting the system down[9].
Trojan Horse	A computer programme that appears to have a useful function, but also has hidden and potentially malicious functions that evades security mechanisms, sometimes by exploiting legitimate authorisations of a system entity that invokes the programme[10].
Exposure	A threat action resulting in sensitive data directly being released to an unauthorised entity[11].

[1] ISO/IEC 27001:2005
[2] http://www.businessdictionary.com/definition
[3] http://www.businessdictionary.com/definition
[4] http://www.sans.org
[5] http://www.sans.org
[6] http://www.webster-dictionary.org/definition
[7] http://www.sans.org
[8] http://www.cert.org
[9] http://www.cert.org
[10] http://www.sans.org

Intellectual property (IP)	Documented or undocumented knowledge, creative ideas, or expressions of the human mind that have commercial (monetary) value and are protectable under copyright, patent, service mark, trademark, or trade secret laws from imitation, infringement, and dilution. Intellectual property includes brand names, discoveries, formulas, inventions, know-how, registered designs, software, and artistic works, literary, or musical in nature. It is one of the most readily tradable properties on the Internet (digital) marketplace[12].
Data leakages	The unauthorised transfers of classified information from a computer or data centre to the outside world. Data leakage can be accomplished by simply remembering what was seen, by physical removal of tapes, disks and reports or by subtle means such as data hiding[13].
Hackers	Person who illegally gains access to and sometimes tampers with information in a computer system[14].
Authentication	Authentication is the process of confirming the correctness of the claimed identity[15].
Due Care	Degree of care that an ordinary and reasonable person would normally exercise, over his or her own property or under precarious circumstances. The concept of due care is used as a test of liability for negligence[16].
Due Diligence	the care that a reasonable person exercises to avoid harm to another or their property[17]
Cloud Services	Services delivered / offered over the Internet[18]
Social Engineering	Social engineering is essentially the art of gaining access to buildings, systems or data by exploiting human psychology, rather than by breaking in or using technical hacking techniques. For example, instead of trying to find software vulnerability, a social engineer might call an employee and pose as an IT support person, trying to trick the employee into divulging his password[19].
Drive by Download	When programmes are installed on an online computer without the user's knowledge[20].

[11] http://www.cert.org
[12] http://www.businessdictionary.com/definition
[13] http://www.pcmag.com/encyclopedia_term
[14] http://www.merriam-webster.com/dictionary
[15] http://www.sans.org
[16] http://www.businessdictionary.com/definition
[17] http://www.merriam-webster.com
[18] http://searchcloudcomputing.techtarget.com/definition/cloud-computing
[19] http://www.csoonline.com/article/514063/social-engineering-the-basics#1
[20] http://www.macmillandictionary.com/buzzword/entries/drive-by-download.html

3 ACRONYMS AND ABBREVIATIONS

Selected acronyms and abbreviations used in the Guideline are defined below.

ERP Enterprise Resource Planning
USB Universal Serial Bus
ICT Information, Communication and Technology
ROI Return on Investment
CIA Confidentiality, Integrity, Availability
CMMI Capability Maturity Model Integration

4 INTRODUCTION

The Small and Medium Enterprises (SMEs) account for about 99 percent of Malaysia's total business establishments and contribute over 31 percent of the nation's Gross Domestic Product (GDP). SMEs' shares to total employment and exports of the country are at 56 percent and 19 percent respectively[21]. Based on the industry's contribution to the country's GDP and employment opportunities, it is very important to recognise the pivotal role that SMEs play in our economy. The significance of the SMEs contribution to the nation's economy drew the government's attention to support them through the Multimedia Development Corp (MDeC) and the SME development agency (SME Corp Malaysia) initiative by promoting the MDEX e-commerce platform. The MDEX is a platform for SMEs to handle online business-to-business transactions with their buyers and suppliers. This would potentially help narrow the SME digital divide as well[22].

On the other hand, SMEs are perceived as lacking in information security awareness which results in the haphazard management of their information and digital assets. Furthermore, SMEs recognise the fact that managing information as an asset is relatively costly and procrastinate on the need for investments to build and maintain reliable information security processes and systems. They do not see the benefits of doing so and how it can assist them in generating revenue for their companies. While it may seems that Internet enabled service serves as an excellent medium for communications and promotions (marketing) among SMEs, but the potential risks and threats posed by the Internet has caused SMEs to lose faith, trusts and confidence to leveraging it.

Most corporate organisations are considered mature in managing information security; but SMEs are still far behind in their quest towards that desired level of maturity. There are tasks that can be carried out within the SME industry in order to achieve reasonable control in the area of information security. This guideline presents several suggestions of Knowledge Practices for SMEs to become accustomed with and exercise it within their controlled environment.

[21] SME Annual Report 2009/10
[22] http://techcentral.my/news/story.aspx?file=/2010/6/15/it_news/20100615114625&sec=it_news

4.1 Objective

The objective of this guideline is to provide awareness, basic understanding, and guidance on information security. SMEs might be fully aware on how they are protecting their physical assets but the conscious state in the sense of protecting the information as an asset is still low. Through the Knowledge Practices suggested in this document, it will ensure that SMEs are capable to manage their assets (information) appropriately. It should be noted that this guideline does not in any way address the overall management of information security for SMEs (if currently available), and it is not intended to replace or supersede any best practices, standards and guidelines produced by any associations, institutions, and/or regulators.

The use of this guideline can differ according to size, nature and the complexity of the current establishment within a particular SME. This guideline can be used to compliment the best practices, standards and guidelines that have been adopted within the enterprise. Knowledge Practices from this guideline can be applied to SMEs in maximising productivity through effective and efficient controls in protecting information as an asset. Subsequently, it can yield more profit by minimising asset losses.

4.2 Scope

This guideline outlines the basic principles of implementing information security through the exercise of the six Knowledge Practices. Each Knowledge Practice will further explain on the relevant action and awareness that needs to be taken to protect the business environment and relevant assets of an SME.

4.3 Target Audience

This Guideline is recommended for the following audience:-

- Entrepreneurs
- SME owners
- Individuals who work in SMEs
- Organisation and individuals who are keen to understand SMEs and possess the desire to promote information security and controls while taking it to the next level

4.4 Document Structure

This Guideline is structured as follows:

Section 1:	Quick Assessment Checklist
Section 2:	Defines some of the Terms and Definitions used in this guideline
Section 3:	List of relevant Acronyms and Abbreviations used in this guideline
Section 4:	Highlights on the introduction of the guideline and begin with the objectives, scope and target audience for this guideline
Section 5:	Knowledge Practice #1 – discusses the necessary “due care” and “due diligence” that needs to be taken in order to demonstrate asset protection (i.e. Protection, Detection, Response, Documentation and Prevention)
	Knowledge Practice #2 – describes the protection of information (asset) and why it is not supposed to be considered as technology alone but must be seen as a business issue as well
	Knowledge Practice #3 – discusses on managing information security and why it is unique based on People, Process and Technology components
	Knowledge Practice #4 – briefly explains protection of an asset (information) that must be based on identified risks
	Knowledge Practice #5 – discusses the necessity to have an appointed or dedicated staff to handle information security and its concerns
	Knowledge Practice #6 – provides a simple rationale on the needs of information security awareness for SMEs
Section 6:	Concludes all listed Knowledge Practices with S.E.C.U.R.E M.E (S-ME)
Appendix A:	Quick Assessment Checklist (1Page Assessment for SMEs)
Appendix B:	Highlights on the classification of SMEs in Malaysia
Appendix C:	Highlights how information is considered as an asset and how it is different from one SME to another
Appendix D:	Highlights several information security risks faced by SMEs
Appendix E:	Template on Incident Handling Response and Strategy
Appendix F:	Presents the Source of References for this guideline

5 KNOWLEDGE PRACTICE

The six Knowledge Practices recommended will enlighten SMEs on the relevant areas of information security and its required needs. Those who are not familiar with Security Risks, Threats and Vulnerabilities within the SME environment should read the entire section in Appendix D. It elaborates on the necessity for entrepreneurs and SME owners in adopting a serious stand on information security and embraces the suggested Knowledge Practices. Therefore, by applying the knowledge at hand, potential security threats can be minimised and the risks involved reduced and consequently creates a culture of excellence among SMEs in Malaysia in information security.

#1: "Due Care" & "Due Diligence"

> SMEs' owners and entrepreneurs MUST perform and exercise "due care" and "due diligence" on protecting their assets (information)

There are several SMEs practicing information security as an integral part of their governance and operation processess. For a listed company, it is a regulatory requirement to exercise internal auditing. Hence, information security governance and processes exist involuntarily. However, SMEs are not being pressured to have all sorts of information security governance exercises by regulators and/or any agencies. It is therefore critical for SMEs to perform and exercise "due care" and "due diligence" in protecting their assets in order to sustain profits and market challenges.

In the case of SMEs, the respectful parties to empower due care and due diligence are the owners or entrepreneurs themselves since they are generally the sole decision maker for their organisations.

It is important for SMEs to know their assets well in order to better manage and protect it. The five pillars on information security are relevant for SMEs to practice and inculcate at their organisations in order to demonstrate the urgency of asset (information) protection. At the same time, it shows that information security's "due care" and "due diligence" are basically being practiced within SMEs. These pillars are as follows:-

i. Asset Protection
ii. Incident Detection
iii. Incident Response
iv. Documentation
v. Prevention

i. Asset Protection

Once assets have been identified, SMEs must know "what" to secure and must know precisely "what" to protect. They also must know "how" well the information at stake is needed for protection. Securing assets by obscurity is not effective and enterprises could end up wasting resources if the protection mechanisms or the security implementation is not proper. At the same time, the cost of implementing such protection should not exceed the value of the asset that is being protected.

More often than not, SMEs own machines, equipments, raw materials, finish goods and other properties that need protection. These are all tangible items that can be physically touched, feel, and sensed. A reasonable work space, warehouse and/or shop-lot are used to store these items. Additionally, hiring security guards and installing an alarm system is needed to guard these physical assets.

The same protective measures must be in place if we are to refer to the information as asset protection. Information as an asset must be protected from potential damage by malware like viruses, Trojan Horse attacks, and worms. Apart from that, a sense of protection must be in place to avoid internal and external attackers stealing enterprise information. The defence mechanisms involved can be physical and logical in their approach as it depends on the subject requires protection. Since SMEs varies from one type to another, the approach would definitely depend on their physical and logical layout. Nevertheless, almost every SMEs store their information in their notebooks, desktops, servers and thumb drives. A few sophisticated ones, subscribe to "cloud services". As information (data) travels from one point to another, usage of the network, be it internal (Local Area Network) or external (Internet) is inevitable. Microsoft[23] is suggesting seven (7) steps which SMEs can adopt to demonstrate asset protection. Actions are summarised as per Table-1.

Steps	Actions
Step 1: Protect Your Desktops and Laptops	• Regular update on the software patches. • At a minimum, install reputable anti-virus software. • Ensure only legal (authorised) software are installed. • Setup firewalls. For Small and Micro enterprises, the least that these organisations should do is to have a standard Windows firewall activated.
Step 2: Keep Your Data Safe	• Make a regular backup of your data and don't forget to carry out restorations (tests) regularly. Backup data is not guaranteed to be available when needed in the event that a restoration process fails or was never tested. • Establish proper permissions to those who want or needs access to the data.
Step 3: Use Internet Safely	• Start creating your own Internet Policy. • Inculcate safe browsing principles i.e. delete temporary Internet files, cookies, histories, surf only known websites, etc[24].
Step 4: Protect Your Network	• Do not Allow Remote Access. However, if it is critical for business operations and support, use a strong password and encryption technology. • Enforce Wi-Fi protection i.e. WPA-2[25].
Step 5: Protect Your Servers	• Servers must be physically located in a restricted area. • Allow only authorised staff to access the restricted area. • Not all staff should be granted access to the restricted area. • Users who have logical access to the servers must be given the "Least Privilege" access. • System administrators who need to perform administration duties must be given necessary or relevant access to perform those duties.
Step 6: Secure Line of Business Application	• SMEs that practically use any applications or ERP systems, a user access. Controls must be enforced wisely. Users are not supposed to have all access but limited to what they "need to have" for their job operations.
Step 7: Manage Computers from Servers	• Centralise the management of computer related machines through updates and monitoring from servers. This would ensure that all computers connected to the network adopts uniform patches and the latest updates. • Managing user's access should be from the central location i.e. servers. • Actions related to this area are relevant to the establishment of multiple servers and workstations. For small and micro SMEs with no multiple servers and workstations, they can subscribe to mailing lists (i.e. Microsoft Security Mailing List) and activate auto updates to ensure their machines are updated with the latest patches.

Table-1: Asset Protection

[23] Security Guide for Small Business: Microsoft Small Business Team (2005)
[24] Detail can be viewed from the "Web Browsing – Play It Smart, Don't be Played". (http://www.cybersafe.my/download/guidelines/Safe_Web_Browsing.pdf)
[25] Detail can be viewed from the Wireless Local Area Network (LAN) Security guideline. (http://www.cybersafe.my/download/guidelines/CSM_Guideline_Book_Wireless.pdf)

There are numerous instances which we can relate to on asset protection. But, the point that we desire to stress here is on the importance and the need for protecting the asset (information) for business endurance.

ii. Incident Detection

SMEs should know that if the protection measures taken seem to be very strong but remains at an “un-alert” stage, then it will become useless. This is due to the fact that the chances of assets being stolen or security being breached will always be there/possible. Incidents could also be from internal and external threats as well. After all, there is no 100 percent guarantee of impenetrable security.

Protecting information (asset) is required but it is not effective if the protection mechanism in place failed to detect security breaches and failed to react toward untoward incidents. For tangible assets, it is usually buildings or business premises that are used to protect it. The premises are well-equipped with the fire detection and alarm systems. The same mechanism should be in place for intangible assets. Alerts and notifications must be triggered to the respective parties for immediate action to avoid further damage and any recurrence of such incidences. If intrusions are detected at the early stages, SMEs would have sufficient time to take the necessary actions and put proper measures in place to prevent such incidents in the future.

It is a challenging effort for the owners in small and micro/medium enterprises to justify investments in relevant technologies. They normally could not afford to deploy tools like Intrusion Prevention System (IPS) and the Intrusion Detection System (IDS) due to financial constraints. Nonetheless, taking into consideration that most enterprise based organisations are using windows based systems, they could at least subscribe to Microsoft security bulletins and mailing lists for advisory services to ensure that they are aware of the latest service patch requirements and updated with the latest database on security threats and risks. In addition, practicing some kind of ad-hoc and scheduled audit would be beneficial to the organisation as well. SME owners can assign trusted individuals to audit their current privilege access to critical or to sensitive business processes. By adopting that approach, SMEs can detect violations of information security and fraud related matters within their enterprises.

SMEs with enough money to spend on technology investments should install IDS and IPS. The latter is most recommended as it can prevent for the most part network attacks. These tools may not be cheap but it is worth to have them installed as it can assist SMEs to detect and prevent alarming attacks to the network. However, the tools need to be handled by personnel who understand and know these products well. For that matter, finding a good technical or solution partner is relevant and essential to assist the enterprise in detecting intrusions and breaches.

iii. Incident Response

Detections should trigger reactions. It is meaningless if the tools that you have installed or processes that you have established are not escalating security breaches once detected. It might be too late by the time you discovered the breach if it is not promptly triggered. Responses (reactions) are important as it portrays how you to react to incidents. The SANS Reading Room through a write up from Terry Morreale provide six steps to ease SMEs into reacting towards security incidents. The steps consist of Preparation, Identification, Containment, Eradication, Recovery and Lessons Learnt which were summarised as per Table-2. Nonetheless, in order to perform these tasks effectively, organisations should first establish a team that coordinates and are directly involved in the incident handling process. The team should consist of people from various relevant departments (e.g. technical support and operations) and most importantly, representatives from the management team.

Steps	Actions Needed
1: Preparation	• Knowing who to assign or who to handle the incident. • Develop incident handling instructions where it contains Call Lists, Initial Response, Response Strategies, Recovery and Lessons Learnt Reports. • A call list consisting of contacts of people that needs to be involved or notified if an incident takes place. • Initial response and strategy will ensure employees know what to do next when referring to the handling instruction guide. • Organisations with multiple critical servers and are capable (affordable) in purchasing tools should consider to have Event Logs, Network-based Intrusion Detection Systems, Host-based Intrusion Detection Systems, and firewalls. These tools could assist in providing analysis reports when handling or facing with incidents. It will prove to be a valuable addition to incident handlers.
2: Identification	• Determine who to identify and decide on the definition and classification of an incident. • Suspected incidents are analysed and determined whether such incidents are really happening. • Respected parties involved must calmly assess the situation and be ready to communicate with each other if an incident really occurs. • If external parties (i.e. law enforcement agencies) need to be notified, the senior management / SME owners need to be informed first.
3: Containment	• During this phase, incident handlers must react immediately to prevent further damage. • Incident handlers must possess basic technical knowledge or SMEs should engage with solution / technical partners to assist them. • The goal of this step is to make sure no new compromises using the same vulnerabilities occurs again.
4: Eradication	• Similar to the previous steps, incident handlers or the solution / technical partners must know how to remove malicious codes or rectify damages due to an incident. • In order to completely remove the damage inflicted, the cause of the incident must firstly be determined. • The primary goal is to ensure that no new occurrence / compromise happen again with the same vulnerabilities (in addition to contain the incident from getting worse).
5: Recovery	• Recovery processes should be carried out by trained staff or the solution/technical partners. • Representatives of SMEs must verify that all systems that are rebuilt measure up to the requirements for operations and making sure the restorations does not include compromise data / software / applications.
6: Lessons Learnt	• Incidents should be well documented in order for SMEs to learn from previous mistakes. • It is advisable to conduct the “lessons learnt” (port mortem) sessions within 24 hours after the incidents are over and get it documented within a month for future references.

Table-2: Incidents Response Steps

Appendix E provides a good template for SMEs to use whenever they encounter security incidents. In addition, Malaysia’s renowned agency, CyberSecurity Malaysia through The Malaysian Computer Emergency Response Team (MYCERT) provides advice to SMEs in handling security incidents and formulate proper responses towards it. SMEs, particularly micro-enterprise and enterprises which do not have a formal process in their operational plan, can seek assistance from MYCERT-Cyber999 Hotline (1300-88-2999) and obtain further instructions on managing and reacting towards incidents.

iv. Documentation

Documentation is another important aspect but it is always not being given enough attention and adherence. In this regard, it is not only limited to SMEs, but most non-SMEs and bigger organisations as well. People do not know what to do and how to react when there is no documented procedures and actionable tasks to refer to if an incident occurs. The same documentation could also be used for future references as mentioned in the "lessons learnt" from the incident handling steps.

Unfortunately, SMEs are always depending on limited resources and putting too much dependency on a single person to attend a unique task in dire situations. If the said staff resigns, this will impair the hand-over tasks and disrupt the continued security processes and might cause it not be executed properly. The worst case is when key employees are absent during critical or emergency periods and the ones who are available could not do anything or will be having a difficult time performing the urgent tasks at hand due to unavailable references.

SMEs will not be able to manage information security without proper processes in place. No doubt, in order to establish the desired processes, it will take a certain amount of time and cost. This is where the desired processes which have been practiced before must be documented and updated from time to time. However, it is a daunting task to get SMEs to have all the relevant documents in place since SMEs normally consists of a very small group of people. But, there is no other alternative in "not to document" the organisation's processes if there is a desire to manage information security. This is where SMEs should start documenting their appropriate processes for effectively managing information security. These documented processes are normally termed as Policy, Procedure and Guidelines (PPG). The good practice that SMEs should adopt is to "Document what you do, and do what you document". Without proper process, SMEs cannot measure their competencies. Once organisational competencies cannot be measured, it is hard to control the enterprise business direction.

v. Prevention

Most SMEs often overlook preventive measures even though many believe that "prevention is better than cure". Data collection of incidents should be documented and analysed and this includes the ways assets are being protected, incidents being detected, and the ways staff reacts towards incidents. The problems that SMEs face are normally resolved on an ad-hoc basis. There are no formal studies or Root-Cause-Analysis (RCA) being done. Even if there were, the analysis is not formal and it is not documented for future references.

It is very imperative for any enterprise to ensure that the necessary processes are in place and documented for smooth operations. Furthermore, enterprises cannot be improved and prevention cannot effectively be formulated if the processes are not available. Within the available documented processes, enterprises can review and revise for better practices and achievements. The Security Incident Handling steps can be a good start for SMEs to formulate preventive actions. Tools like IDS and IPS could assist SMEs to prevent the occurrence of security incidents.

#2: "It's a Business Issue"

> Protecting an asset (information) is not about technology or a technical issue alone. SMEs must be aware that protecting the information as an asset is a business issue as well

For SMEs to explore further on the limitless potential of ICT, it would require time and strong support from both the management and owners. SMEs possess this tendency to believe that information security (information asset protection) is all about technical matters and they are unwilling to accept information security as part of their operational and business strategy requirements.

Noticeably, protecting an asset is the main reason of having information security governance and processes in place. Organisations would be assured that their profits are not affected if the asset value is not being compromised. To a certain extent, SME's suppliers and SME's customers will have more trust and confidence dealing with a business that promotes information security governance and processes. Hence, SMEs must change the above negative perception as information security is not only about technical issues but encompass business and operational aspects as well.

Furthermore, Malaysian SMEs are far behind, in terms of innovation as compared to advancing Asian economies like South Korea, Taiwan and Singapore. The setting up of the Cradle Fund and the Cradle Investment Programme provide an incentive for Malaysian SMEs to further enhance their technological capabilities and commercialisation to compete in the global technology environment[26]. By seriously looking at technology as part of organisational strategy, it may assist SMEs to get a new source of funding through the Cradle Fund (http://www.cradle.com.my/cms/home.jsp) from the Cradle Investment Programme, which is a government initiative.

[26] http://www.malaysiansme.com.my/2011/03/malaysian-smes-external-and-internal.html

#3: “It’s unique for each enterprise”

> SMEs must be aware that managing information security is unique for each enterprise. The way assets are being protected must fit into the needs of an enterprise. There is no silver bullet in handling information security issues where Integrating People, Process, and Technology is extremely crucial

Managing information security requires good understanding on existing resources, processes and technologies. Additionally, deciding the best options (new processes and new technologies) to fit into an organisation’s need is important as well. Undoubtedly, there is no single solution able to suit multiple organisations due to “People”, “Process” and “Technology” (PPT) differences. The type of people in terms of their educational background, experiences and skills are always diverse from one organisation to another.

Generally, for SMEs, all processes adopted are unique to its own nature of existence. There are no processes which are similar even though they are in the same sector and category or even if they produce the same products or outputs. For the large and medium enterprise, they may adopt industry standards like the CMMI level, 6 Sigma and ISO (International Organisation for Standardisation), but the processes that are defined within the CMMI standards are tailored specifically to its own environment.

Technology plays an important role in benefiting or enabling business objectives. However, deployment of such technologies varies between enterprises. SMEs must become conscious on the different classes and categories composed of different types of people, process and technology. It is the same like technology adoption where Information security cannot be easily “copied” from other organisations’ practices. SMEs must perform preliminary studies and due diligence to customise their own specific needs prior to implementation.

#4: "It must be based on Risk Perspective"

> SMEs must implement information security based on the identified risks

Information security is composed of assets, threats and vulnerabilities. If one of these components is irrelevant, then there is no risk encounter[27]. Thus, protecting information must come from the risk perspective by implementing information security based on risk identification. There are many approaches in managing the information risk involved. However, SMEs must at least know how to implement the phases of risk assessment[28] as laid out in Table-3 below.

Phase1: Threat Identification	Identify all relevant threats
Phase2: Threat Categorisation	Determine the impact and likelihood of the relevant threats
Phase3: Exposure Assessment	Identify the vulnerability of the assets
Phase4: Risk Categorisation	Determine the risk and evaluate the impact to the business

Table-3: Information Risk Assessment Phases

Without careful and proper risk assessment, SMEs may wastefully deploy or mitigate risks that are unlikely to occur or will never materialise.

[27] Risk Assessment and Risk Management Methods: Information Packages for SMEs v.1.0 (ENISA)

[28] Risk Assessment and Risk Management Methods: Information Packages for SMEs v.1.0 (ENISA)

#5: “Dedicated staff or formally appointed”

> SMEs should have appointed a dedicated team of staff who look into information security matters. Knowing the nature of SMEs with being a flat organisational structure, (the least) a non-full time information security personnel is essential

Local SMEs are always faced with the constraint of hiring experts in ICT and particularly Information Security personnel. SMEs normally have flat organisational structure where a single person can be entrusted with multiple functions or roles. More than often, the people who are sought after to work in the SME sector are hired due to their specific skills related to a specific operational domain. Even though he or she is hired for ICT related tasks, it may not be his or her only job. For example, a person who assumes the position of a system administrator will take charge of everything related to ICT.

Furthermore, SMEs are with no structured unit and dedicated security departments unlike that of the big corporations. Employing a specific ICT person will cost them too much and that may affect their financial standings. Several SMEs will outsource their ICT related tasks to external parties particularly the micro and small enterprises. The medium sized SMEs might be having a formal IT department and treating information security differently. However, there are possibilities that no absolute job segregations in place to perform the required ICT duties. It is important to note that implementing segregation of duties can reduce internal attacks especially from disgruntle employees.

Hence, it is crucial for SMEs’ owners to appoint dedicated staff to be responsible in related areas of information security. If this is not done, no one will take the initiative to manage incidents and be the “champions” on the subject matter.

#6: "Continuous Awareness on Information Security"

> Awareness on Information Security is important among SME owners and staff

SMEs must recognise the importance of information security awareness. Awareness like security acculturation programmes for the staff and management can inculcate the knowledge and practice related to information security. Depending on the budget of an SME, they can produce awareness posters, regular awareness emails to staff and management, and briefings from invited speakers who are familiar with the subject matter. SMEs can also encourage (sponsor) staff for training programmes at expert organisations like CyberSecurity Malaysia. Through its Information Security Professional Development (ISPD), CyberSecurity Malaysia provides a platform to nurture Information Security practitioners and promote knowledge sharing sessions with leading industry experts and academicians as well as fostering local and international collaborations. Awareness training is also provided for those who need basic information security understanding. Further information on the training modules provided can be located at the Cyberguru Portal[29].

Humans tend to forget and prefer convenience rather than complexity. Thus, it is important for SMEs to understand the rationale of having solid information security and controls at their level. If not, convenience is always the preferred option if users are left to decide between the enforcement of security best practices and handiness. Furthermore, human is the weakest link in any security implementation. The most classic example is when a user's password is displayed on the computer screen via a sticky note. That reflects a user's "convenience" in avoiding from forgetting his/her password.

SME owners should realise by now that the greatest threat to their assets is the employees themselves. Employees are the closest to the assets that are being protected and pose the greatest risk since incidents can happen deliberately (attack) or "un-deliberately" (accident). Hence, staff should be reminded on related information security practices in order to minimise the risks of information security violations.

[29] https://www.cyberguru.my/

6 "S-ME: SECURE ME"

S-ME – "S.E.C.U.R.E. M.E."

These Knowledge Practices can be concluded with the S-ME phrase. It stands for "SECURE ME" and further elaborated below.

S	**S**electively identify your Valuable Assets
E	**E**nsure **P**rotection **C**ost should not be more than **A**sset's **V**alue (**PC$** < **AV$**)
C	**C**omprehend your protected area
U	**U**nderstand the risks and plan for mitigation
R	**R**isks that inflict the asset value must be managed correctly
E	**E**nsure that "you document what you do, and do what you document"
M	**M**aking sure business survival in the event of disasters/interruptions
E	**E**valuate People, Process and Technology for continuous improvement

The 1Page Assessment – For Small and Medium Enterprises (available in Appendix A) is a quick checklist designed to measure information security readiness and test your basic awareness on the subject matter. The checklist was designed for SME managers and/or individuals who are able to make decisions related to the enterprise business direction and its operations. The overall scoring result will be represented by excellent, good, fair or poor classifications in the area of information security readiness (implementation) and the awareness level at your organisation. If your score is 140 and below, there is a large amount of effort needed to increase the awareness level and security implementation within your enterprise. Furthermore, "Due Care" and "Due Diligence" might not be sufficiently exercised within your enterprise. For those who fall between the ranking of Good and Excellent, security implementation might be sufficiently implemented and the level of security awareness is adequate. However, from time to time, the implementation must be reviewed and improved upon to ensure the level of asset protection is always relevant and adequate.

A APPENDIX:
QUICK ASSESSMENT

[*Please turn over to the next page*]

1 PAGE ASSESSMENT – FOR SMALL & MEDIUM ENTERPRISES					
Please answer ALL 30 questions below accurately and sincerely in order to measure the outcome of Information Security implementation in your company. State YES (√) if you are fully implementing it, state PARTIAL (√) if you are half way to implement it and/or it is already in your plan to implement it and/or the implementation coverage is in partial. State NO (X) if you are not implementing anything and/or do not understand the statements below. Marks are given as below. **REMINDER:** Checklist must be completed by those holding **MANAGERIAL AND ABOVE** only positions. (Answers should **either** be YES, PARTIAL or NO)					
DESCRIPTIONS		Yes = 8 Partial = 4 No = 0	**YES**	**PARTIAL**	**NO**
Knowledge Practice: #1 – Due Care & Due Diligence with Protection, Detection, Response, Documentation and Prevention	1.	Have you identified assets (information) within your enterprise that worth protecting?			
	2.	Have you installed anti-malware (or at least anti-virus) in your PCs and servers?			
	3.	Have you identified physical security perimeter and equipped with the proper control? (i.e. alarm systems, CCTVs, lockers, strong cabinets, etc.)			
	4.	Do you (or your vendor as requested by you) frequently update software patches that are made available?			
	5.	Do you prepare a backup copy and regularly restore (test) your data?			
	6.	Do you advise your staff not to leave sensitive documents on their tables without proper supervision?			
	7.	Do you have an Enterprise Security and an Internet Policy established and well understood by your staff?			
	8.	Have you installed any mechanism/method to detect information security incidents? (i.e. IDS, IPS, etc.)			
	9.	Do you have technical experts within your enterprise? If NO, do you engage with any solution/technical partner to assist your enterprise in technical related matters?			
	10.	Have you managed to ensure your Policy, Procedure and Guideline (PPG) established, reviewed and updated from time to time?			
	11.	Do you analyse the incident occurrences for the root cause analyses and then come up with preventive measures?			
	12.	Do you understand and are you trained in responding to the related security risks and incidents?			
Knowledge Practice: #2 – It's a Business Issue	13.	Does your management / enterprise owner participates, encourages and endorse related information security initiatives?			
	14.	Does the management / enterprise owner participate in decision-making on ICT/security related matters? (i.e. risk assessments, planning, strategy, awareness, etc.)			
	15.	Does the management / enterprise owner demonstrate commitment on the information security measures implemented within the organisation?			
	16.	Do you understand the obligation and/or aware of the local regulatory requirements related to your operations if related information security initiatives are not being implemented?			
Knowledge Practice: #3 – It's Unique for Each Enterprise	17.	Are you of the opinion that your internal processes are effective and you have documented it properly as formal procedures?			
	18.	Does your team conduct studies on requirements and then present the outcome to the management / enterprise owner to decide and adopt any ICT initiative or implementing security measures?			
Knowledge Practice: #4 – It Must be Based on Risk Perspective	19.	Do you understand all information security risks and its consequences towards your enterprise?			
	20.	Do you agree that it is important to know the information security risks and its influence towards your enterprise?			
	21.	Do you practice information security risk management within your enterprise environment?			
Knowledge Practice: #5 – Dedicated Staff or Formally Appointed	22.	Do you assign dedicated personnel to be "Champions" on information security related areas?			
	23.	Have you clearly established the high-level "Dos" and "Don'ts" and ensure your employees understand the necessity to safe keep the enterprise sensitive data? The "Champion" can enforce this checklist in addition to the enterprise policies.			
	24.	Do you assist in giving "mandates" to the "Champions" in order for them to do their tasks related to information security comfortably?			
Knowledge Practice: #6 – Continuous Awareness on Information Security	25.	Do you allow staff to share their ID and passwords among themselves?			
	26.	Do you encourage your staff to use hard-to-guess passwords?			
	27.	Have you observed any of your staff making their passwords noticeable? (i.e. sticky notes @ computer screen/displaying passwords) to others?			
	28.	Do you compel your staff (and yourself) to regularly change passwords? (i.e. every 90 days)			
	29.	Do you keep reminding your staff about information security policies via emails/awareness programmes/ posters/etc.? (continues education and awareness)			
	30.	Do you feel that it is important to implement information security standards within your enterprise?			
Total Number of [YES] [PARTIAL] and [NO]					
Total Number of YES (x8), PARTIAL (x4) and NO (x0)					

POOR (0 - 80)	FAIR (81-140)	GOOD (141 - 199)	EXCELLENT (200)
You must seriously study the current situation and reassess them with the suggested knowledge practices.	SMEs should revisit the identified fragile areas and improve them with the necessary actions / practices.	SMEs should ensure continuous improvements with the current practices and strive in adopting industry best practices.	SMEs should consider adopting ISMS and/ or governance standards i.e. ISO27001, COBIT, ITIL, etc.

B APPENDIX: MALAYSIAN SMEs

SMEs in Malaysia are defined into two broad categories; (1) Manufacturing, Manufacturing-Related Services and Agro-based industries and (2) Services, Primary Agriculture and Information Communication Technology (ICT). These categories normally employ full time people not exceeding 50, or with an annual sales turnover not exceeding RM 5 million[30]. Table-4 defines further on the description of SMEs while Table-5 illustrates the number of establishments existing in Malaysia as at 2005.

In Table-4, there are 548,267 SME establishments in Malaysia. This statistics substantiates the fact that a huge number of establishment falls within the micro-service sector. Furthermore, it shows that 7.2 percent are from the manufacturing sector, 6.2 percent are from agriculture and 86.6 percent are from the services sector. The variance sector within SMEs demonstrates the complexity that exists in defining and managing information security at that level. Nevertheless, when talking about information security in general, it is all about protecting an asset.

Acknowledging the fact that, there are many different sectors of SMEs in Malaysia but noting the fact that they share a common purpose which is maximising their profits. One way of capitalising the information in question is to protect and preserve the asset and its value. Knowing the asset in the context of “information as an asset” is critical to facilitate further understanding on Information Security Knowledge Practices within SMEs in Malaysia.

[30] Malaysian SMETM Business Directory 7th Edition

BASED ON THE NUMBER OF FULL TIME EMPLOYEES			
Primary Agriculture		Manufacturing (including Agro-based and Manufacturing Related Services)	Service Sector (including ICT)
MICRO	Less than 5 employees	Less than 5 employees	Less than 5 employees
SMALL	Between 5 –19 employees	Between 5 – 50 employees	Between 5 – 19 employees
MEDIUM	Between 20 – 50 employees	Between 51 – 150 employees	Between 20 – 50 employees
BASED ON THE ANNUAL SALES TURNOVER			
Primary Agriculture		Manufacturing (including Agro-based and Manufacturing Related Services)	Service Sector (including ICT)
MICRO	Less than RM 200,000	Less than RM 250,000	Less than RM 200,000
SMALL	More than RM 200,000 but less than RM 1 million	More than RM 250,000 but less than RM 10 million	More than RM 200,000 but less than RM 1 million
MEDIUM	Between RM 1 million & RM 5 million	Between RM 10 million & RM 25 million	Between RM 1million & RM 5 million

Table-4: SME Definition (Source: Malaysian SME™)

Sector	Micro	Small	Medium	Total SMEs	Total SMEs	Large	Total Establishment
Number of Establishments					%	Number	Number
Manufacturing	21,516	15,796	2,061	39,373	7.2	1,420	40,793
Services	381,585	83,037	10,084	474,706	86.6	2,819	477,525
Agriculture	31,838	1,775	575	34,188	6.2	343	34,531
Total SMEs	434,939	100,608	12,720	548,267	100.0	4,582	552,849

Table-5: Number of Establishments by Sectors (Source: Census of Establishment and Enterprises 2005 by Department of Statistics, Malaysia)

C APPENDIX: INFORMATION AS AN ASSETS

In most organisations, asset would be considered as the company's financial resources. Asset can be acquainted with tangible or intangibles so long as it is capable of being owned or controlled to produce a positive value. Tangible assets contain various subclasses, including current assets and fixed assets. Current assets include inventory, while fixed assets include items such as buildings and equipments. Intangible assets are non-physical resources and rights that have a value to the firm because they give the firm some kind of advantage in the market place. Examples of intangible assets are goodwill, copyrights, trademarks, patents, computer programmes, and financial assets, including items such as accounts receivables, bonds and stocks[31].

Table-6 inspired by P. Pfleeger (2002) in the book Security in Computing[32], illustrates the characteristics of tangible assets and the characteristics of intangible assets being protected. In the illustration, it compares the characteristics of the tangible assets i.e. machines, equipments and money and how SMEs protect those intangible assets. Information as an asset varies on the value appreciation while tangible asset is normally associated with a certain value and depreciate over time. The value of money is always fixed to a certain amount but the worth of information often fluctuates.

Damage done to physical assets can quickly be analysed on the amount of losses suffered and can be replaced. Unfortunately, it is not the case for information loss. Data leakages can contribute a great amount of losses to an organisation if information is not properly protected. Hence, SMEs must understand and be aware of the risks in losing precious data.

Protecting information as a business asset should not be taken lightly. It should be accorded with the same importance on how SMEs protect machines and equipments within their premises. The enterprise owner should acknowledge that protecting information as an asset is important in the same way how their tangible assets are being protected.

[31] http://en.wikipedia.org/wiki/Asset

[32] Third Edition, Charles P. Pfleeger, Shari Lawrence Pfleeger (2002)

Characteristic	Tangible Assets	Intangible Assets
Size and portability	• Sites storing machines and equipments are large, unwieldy and not at all portable. Buildings or protected areas require guards, vaults, and many levels of physical security i.e. fence, barb wire and gates.	• Devices or items storing valuable assets are very small and portable. These physical devices can be so small that it can comfortably fit into a pocket.
Ability to avoid physical contact	• Difficult. If criminals intend to steal money, machines and equipments, they must be physically at the scene to confront security guards as well as the layered physical security in place.	• Simple. When information is handled electronically, no physical contact is necessary. Indeed, when transactions are done electronically, this is carried out without any physical contact.
Value of assets	• Very high.	• Variable, from very high to very low. Some information, such as Intellectual Property (IP), business strategies, medical histories, tax payments, investments records, staff salaries, staff background data, are confidential. Other information like sales strategies and buying patterns can be very sensitive. Some other information, such as addresses and phone numbers, may be of no consequence and easily accessible by other means. However, to a certain extent these types of information can be very sensitive as well.

Table-6: Comparison on the characteristics of tangible and intangible assets

Many believe that managing information security should not be different from one organisation to another. But, we must realise that it is the same group of hackers who are targeting assets belonging to these organisations. The Internet creates the possibility of anyone accessing any part of an SME's vault of information without boundaries. If the asset is not properly protected, certain information that was deemed valuable can be easily stolen. The size of the company is not the factor that caused it to be attacked. Whether it is a big company or a small one, it does not matter. What matters is the value of the assets residing within the company.

Hackers are no longer doing it for fun but now take pride of their success and adventures. The financial gain is the main driver for the bad guys to hack or steal information. Unfortunately, the best hackers are those that are capable of doing something bad without being detected or traced by the authorities. Hence, the bad guys are still "out there" preying on their next target.

On the other hand, small companies and particularly SMEs are operating on a tight ICT budget. Hence, treating information security would be very much different as compared to other large organisations that are capable of spending huge amounts of cash on their ICT expenditure.

D APPENDIX: SECURITY RISKS, THREATS AND VULNERABILITIES IN SMEs

SMEs are faced with security threats and vulnerabilities everyday with or without them knowing it. It does not matter whether a particular establishment falls under the micro, small or medium classification. All of these establishments are basically facing the same security risks, threats and attacks. The one that makes the difference is the one that perceives and anticipate the attacks and find a solution to mitigate it. SMEs as we acknowledged earlier, survives on making a daily profit. In basic terms, pushing an organisation to achieve a profit, means that SMEs must increase sales and control (reduce) operating costs.

In addition, preventing an organisation from making losses are part of the strategy in generating revenue. Most SMEs may not realise the fact that security threats are capable of damaging their business reputation and interrupt their operations. Hence, understanding the security threats posed is very important to all SMEs. It is imperative for SMEs to know the "how" in managing the risk and threats and the "what" to protect themselves in order to survive the ordeal.

D1 Method, Opportunity and Motive (MOM)

There are three components that must be present at the same time for an attacker to launch an attack. Those three components are "Method", "Opportunity" and "Motive" (M.O.M). Method is the skill, knowledge, tools, and other things that are used for launching attacks. Opportunity is the time and access to accomplish an attack while Motive is the reason on launching such attacks. The attacks would not take place if any one of the "M.O.M" element is absent[33]. If SME owners understand perfectly the value of their assets, they must also be willing to understand what is needed to be done in order to protect those valuables. Keeping away any of those three components may halt the attack on precious data.

Nowadays, the main motive of any attack is financial in nature. If SME owners ignore putting in place practical and reasonable measures to prevent possible attacks, they are inevitably providing more opportunities to an attacker who might already have an intention to cause destruction. Also, if SMEs are not fully alert on suspicious behaviour among employees, it could lead to disastrous results as well. SMEs must take note that their employees are already exposed with the "Method" and "Opportunity" to launch deadly attacks. They only need a "Motive" to guarantee a successful hit on the protected assets. Thus, SMEs must understand on the gravity of an insider threat as well as minimise the exposure of "Method" and "Opportunity" from external threats. If they were to let their guard down, it could present a perfect exposure for internal attacks to occur.

[33] Third Edition, Charles P. Pfleeger, Shari Lawrence Pfleeger (2002)

D2 Security Threats

There are many ways that threats and vulnerabilities may attack and reside in your organisation. Addressing those threats and vulnerabilities is supposed to be a unique process for each organisation. GFI Software[34], has put forward the four identified threats that are likely to have an impact on SMEs. In order to broaden our understanding on these threats, we are using four main threats namely, "Attacks on Physical System", "Authentication and Privileges Attacks", "Denial of Service" and "Malicious Internet Content". We have to take note that these threats are not only limited to the attacks that are mentioned in this section. There are a countless number of threats (attacks) and vulnerabilities existing today and are waiting to be found and exploited.

D.2.1 Attacks on Physical System

Threats	Vulnerabilities	Means (How?)
Attack on Physical Systems	Hardware Loss	Laptop Theft
		Storage Theft (USB stick/hard disk)
	Unprotected Endpoints	USB Devices
		Removal Media
	Insecure Network Points	Internal Attacks
		Network Monitoring
	Insecure Server Rooms	Unauthorised Access

Table-7: Attacks, Vulnerabilities and Means (Physical)

For the micro and the small enterprise, they may not have proper server rooms and absolute setup of Local Area Networks (LAN) in their operational environments. SMEs in the micro and the small size arena have a very limited number of computer-related machines like, PCs, servers, and printers. They usually use stand-alone PCs that are not connected via a network. Medium sized SMEs have a huge number of PCs, servers and printers. This type of SMEs might even install Enterprise Resource Planning (ERP) systems.

Ensuring secure endpoints is more critical in the medium size industry as compared to the micro and small size industry. However, installing anti-virus software is very important regardless which category and size the SMEs belong to. This is the least that SMEs must do; otherwise, their computers and network are susceptible to attacks by malicious software.

In term of occupancy of premises, space allocations at SMEs are usually occupied with equipments and machines. Those valuable equipments and machines are always protected in an area where it can be locked or guarded. Physical attacks are not restricted to the equipments, machines and premises alone. It can go beyond that. Most of the micro and small enterprises possess personal computers, notebooks, printers, and mobile devices. These types of enterprises are probably not implementing any application software or ERP systems.

[34] http://www.gfi.com/whitepapers/Security_threats_SMEs.pdf

However, they cannot run away from having the standard off-the-shelf products like Microsoft Operating Systems, Microsoft Office and Outlook. These proprietary software are globally recognised on the needs to frequently update software patches. These are necessary to address the vulnerabilities found in the systems. Hence, it is important to understand the need to deploy patches for operating systems or face the risk of being exploited by malware.

There might be bigger challenges in the medium and large enterprises since they are having more computers, servers and network points to be taken into consideration. Furthermore, networks that connected to the Internet will definitely experience an increase in the risk of being attacked and exploited by hackers. Another sore point for SMEs is the need to be careful of stolen or missing hardware. Hardware like notebooks, mobile devices, USBs, and external hard disks are easily stolen or misplaced. The problem is not limited to a particular category of SME and may even hit the big corporations as well.

On July 2009, PC World[35] announced that the largest storage media (thumb drive) capacity available in the market is up to 256 Gigabytes. This is indeed huge storage capacity and capable of storing a lot of data and ultimately information. The device size is remarkably small as compared to the storage size capacity. It can be considered as an avenue for an organisation potentially losing their confidential data. Moreover, almost everyone who experience interacting with computers basically owns a thumb drive.

It is a significant risk of data loss for the enterprise due to the highly portable nature of thumb drives or USB sticks. Approximately one in ten corporate end-users reported finding a flash drive in a public place. Additionally, when asked to pick the three most likely actions they would take if they found a flash drive in a public place, 55 percent indicated they would view the data within[36].

D.2.2 Authentication and Privileges Attacks

Threats	Vulnerabilities	Means (How?)
Authentication and Privileges Attacks	Passwords	Inappropriate password policy
		Weak passwords
	Disgruntle Employees	Low motivation, unsatisfied staff
	High Privilege Account	Internal attacks
	Privilege creep	Network monitoring

Table-7: Attacks, Vulnerabilities and Means (Auth. And Privilege)

The term Authentication may seem to be “alien” in nature for SMEs. Those in the micro and small enterprises may not be aware of its importance. Most of the applications and network usage in the micro and small enterprise arena is set to not require any kind of authentication for the sake of convenience. SMEs in this environment are normally working in the “standalone” or in a “workgroup” mode. No network authentication is required even for personal computers or notebooks. Even if it does, users are willingly sharing their IDs and passwords with each other.

[35] http://www.pcworld.com/article/168802/worlds_biggest_flash_drive_comes_at_a_price.html

[36] http://www.pcworld.com/businesscenter/article/144495/flash_drives_threaten_security.html

By right, any application systems are normally equipped with authentication methods. Users are required to key in their passwords whenever needed to use the system. Many times, users will choose to have the simplest password that can be easily remembered. For some medium enterprises and most large ones, a proper policy might be in place. Passwords generated or created by the user will follow certain policy requirements like combinations of small and capital letters, numerics and special characters.

Unfortunately, most SMEs do not have the luxury of manpower. Putting someone in-charge of ICT in an SME is normally done without job segregation. Most micro and medium enterprises has no specific person in-charge of ICT. The person chosen to work in the ICT department will be doing "everything" as long as it relates to computers, networks, and machines. That person will be having all the privileges and that can be very dangerous especially in the event that the person turns into a disgruntled employee. If a person with too much privilege is not well equipped with the proper knowledge and skills, it can lead to unnecessary human mistakes. After all, the weakest link will always be the human.

D.2.3 Denial of Service

Threats	Vulnerabilities	Means (How?)
Denial of Service	Natural Disaster	Connection Downtime
		Power Cuts
	Targeted DOS	Bandwidth Exhaustion
		Vulnerable Servers
	Single Point of Failure	Relying too much on one person
		Unprepared for security incidents
		Lack of documentation

Table-8: Attacks, Vulnerabilities and Means (DOS)

SMEs providing e-Commerce services are the most affected with these kinds of attacks. The attacks may have been deliberately or undeliberately inflicted onto their services, servers and network infrastructure. DOS and DDOS attacks are less likely to happen to micro and small enterprises if they are not providing e-Commerce solutions. However, this is something that warrants concern. This is due to the fact that most micro and small enterprises are having their own websites with less complicated features as compared to the large and medium enterprises. Their websites are either internally hosted or outsourced to a third party service provider and used for promoting products and services. Even though their websites are not providing features like on-line sales or an online store, it can still impact the company's image if potential customers are not able to browse the websites due to service disruptions.

For the large and medium enterprise with online features, DOS or DDOS attacks will heavily impact their businesses. According to Malaysia Computer Emergency Response Team (MyCERT) from CyberSecurity Malaysia, as of 2010, there were about 2,886 attacks and 2,082 attacks during the entire period of 2009 on registered domains. SMEs could have been effected as they would have subscribed to any of the said domains that were being attacked for the past two years.

Domain	Year	
	2009	2010
.BIZ	25	24
.COM	1019	1558
.COM.MY	692	829
.NET	163	172
.NET.MY	94	177
.ORG	33	81
.ORG.MY	56	45
TOTAL	2082	2886

Table-9: Attacks on Domains 2009 – 2010 (Source: MYCERT)

D.2.4 Malicious Internet Content

Threats	Vulnerabilities	Means (How?)
Malicious Internet Content	Web Application Attack	Cross-site scripting (XSS), buffer overflow, SQL injection, DOS, DDOS, etc.
	Drive by Download	Forced to download malware
	Social Engineering	Phishing
	Malware	Viruses
		Trojans
		Worms

Table-10: Attacks, Vulnerabilities and Means (Internet)

Malicious Internet Content can be very difficult to contain if an organisation did not properly secure its endpoints. Nowadays, it is very convenient to “hook up” to the Internet with the emergence of broadband services. All that you need is a PC or a notebook and broadband subscription services. Employees who are careless may cause malware and viruses to wreck havoc on a network. Worms and Trojan Horse attacks disturb a company’s operations by creeping into its networks. Users may not be careful enough and thus prone to download malicious programmes into their PCs and subsequently spread it throughout the network. Awareness is pretty much important to ensure SMEs know the “dos” and the “don’ts” while surfing the Internet. Furthermore, SMEs must find a way to assess and rectify the vulnerabilities that may currently exist in their environment.

The usage of the Web (Internet) definitely contributes to the risk factor in protecting assets and resources. In the old days, when people were dealing with a business counterpart, they need to be physically in contact with each other. That is, between the supplier and the buyer. But now, people can complete a business transaction without having to be physically in contact with each other. Furthermore, there are no restrictions in terms of geographical considerations. People can do business or transact with anyone beyond borders. SMEs should participate in the global market and take advantage of the Internet where they can overcome global barriers between themselves and potential customers. The only thing that SMEs must be aware of is that the Internet is not a secure place by default. Hence, some protective measures and actions must take place prior to implementation.

E APPENDIX: INCIDENT HANDLING TEMPLATE

Adopted from SANS Reading Room – Incident Handling for SMEs by Terry Morreale

E.1 Initial Response

Incident Handler Information:
Name: Contact Information: Date and Time:
Incident Information:
System Name: Type of Incident Suspected: Other systems that may also be affected: Actions that were already taken:
System Information:
Describe the risk of this incident (i.e. is sensitive data at risk? How much damage is already known to have occurred?)
Analysis Information:
What analysis were done? What are the recommended next steps?

E.2 Response Strategy

Communication Plan:
Record who has been involved in communications:
Approval:
Recommended Subsequent Steps: Remove the system from the network (or isolate it)? Analyse system without removing it from the network? Approver Name: Approver Signature:
System Backup:
Has the system been backed up? Forensic copy of the system created?
Analysis:
What was determined to be the cause of the incident? What data support this conclusion?
Eradication:
How would the system be recovered? Will the system be restored from a backup? Will the system be rebuilt from scratch? Approver Name: Approver Signature: If the system will be restored from a backup, what steps were / will be taken to ensure all artefacts left by hackers are removed (i.e. root kits, viruses, backdoors)?
Recovery:
Validate System Security: Scans with Nessus tool and/or Microsoft Baseline Security Analyzer produce a clean report? Applied all current OS patches? Applied all current application patches? Continuation of this practise? Disabled all unnecessary services? Are all system passwords complex in nature? Installed antivirus/anti malware software? Regularly updated? Validate system functions: Are all required system functions intact? Is the system ready to be put back in production? Approver Name: Approver Signature:

E.3 Lessons Learnt Report

Incident Description:
Affected Systems:
Incident Cause:
Actions Taken to Eradicate Compromises:
Actions Taken to Prevent Future Compromises:
Recommended Additional Actions:

APPENDIX:
SOURCE OF REFERENCES

[1] KS Tan, SC Chong, B Lin, UC Eze, “Internet-Based ICT Adoption: Evidence from Malaysian SMEs”, 2009

[2] Chen Xin, “The Problems of SMEs in E-Commerce”, 2009

[3] Siti Shafrah and Rosnah Idrus, “Pre-Considered Factors Affecting ERP System Adoption in Malaysian SMEs”, 2010

[4] Sherah Kurnia, Basil Alzougool, Mazen Ali and Saadat, “Adoption of Electronic Commerce Technologies by SMEs in Malaysia”, 2009

[5] M.A Burhanuddin, Fahmi Arif, V. Azizah and Anton Satria, “Barriers and Challenges for Technology Transfer in Malaysian Small and Medium Industries”, 2009

[6] ISACA, “An Introduction to the Business Model for Information Security”, 2009

[7] GFI Software, “Security Threats: A Guide for Small and Medium Businesses”, 2009

[8] KS Tan and UC Eze, “An Empirical Study of Internet-Based ICT Adoption among Malaysian SMEs”, 2008

[9] Basie and Rossouw Solms, “The 10 Deadly Sins of Information Security Management”, 2004

[10] SL. Pfleeger and SJ Stolfo, “Addressing the Insider Threat”, 2009

[11] http://www.smecorp.com.my

Notes

Information Security Guidelines for Small and Medium Enterprises (SMEs)

This guideline is produced in order to assist Malaysian Small and Medium Enterprises (SMEs) that are perceived as lacking in information security awareness which result in the haphazard management of their information and digital assets. With this guideline, it outlines the basic principles of implementing information security through the exercise of the six Knowledge Practices. The Knowledge Practices are further explained on the relevant action and awareness that needs to be taken to protect business (relevant assets) within SMEs environment. With the S-ME phrase that stands for S.E.C.U.R.E M.E, it give a good insight on how SMEs should inculcate and practice the information security and digital asset protection. Furthermore, the "1PAGE ASSESSMENT – FOR SMALL & MEDIUM ENTERPRISES" checklist designed to enable SMEs in measuring the information security readiness and the assessment of managers and/or owners basic information security awareness. This guideline will also provide guidance for SMEs to practice "due care" and "due diligence" in protecting their digital assets and assurance for business profit.

CyberSecurity Malaysia,
Level 8, Block A, Mines Waterfront Business Park,
No 3 Jalan Tasik, The Mines Resort City,
43300 Seri Kembangan, Selangor Darul Ehsan,
Malaysia.

Tel: +603 - 8946 0999 Fax: +603 - 8946 0888
Email: info@cybersecurity.my
www.cybersecurity.my