Cybersecurity Awareness and Advisory Programme (CAAP) – Body of Knowledge for SME Business Owners

TABLE OF CONTENTS

Module 1: Understanding the Digital Business Landscape 3

Module 2: Understanding the Digital Transformation Journey 5

2.1 Improving Productivity 7

2.2 Expanding Business Online 8

2.3 Emerging IT technologies and their impact on cybersecurity cloud (IaaS, PaaS, SaaS) 9

2.4 Mobility & Internet of Things 10

Module 3: Understanding Risk and Threats to Business 11

3.1 Assets Identification & Risk Assessment 11

3.2 Cyber Attacks 14

3.3 Social Engineering 15

Module 4: Securing the Business 21

4.1 Handling data securely 21

4.2 Cyber hygiene (updating IT assets and implementing cybersecurity measures) 23

4.3 Protection of Customer Data 27

Module 5: Understanding the Business Obligations 31

5.1 PDPA 31

5.2 Cybersecurity Act 32

5.3 Computer Misuse Act 33

5.4 Contractual Obligation & Liabilities 33

5.5 International Regulatory Requirements 34

Module 6: Incident Handling / Reporting 35

MODULE 1: UNDERSTANDING THE DIGITAL BUSINESS LANDSCAPE

Digital businesses adopt technology to generate new value by developing new business models and supporting new customer experiences. Sometimes they modernise and upgrade internal capabilities within their core operations to fast track the journey to digital business. Businesses adopt digital-only, where all engagements and services are solely done online. In more traditional businesses, they tend to adopt bimodal or hybrid services; hence, transforming their businesses to be more digital does not introduce too much disruption.

1 Growing and adapting to this Digital Economy

Today, where the pandemic accelerated in 2020, the bulk of the people's activities revolves around digital spaces, ranging from social media to e-commerce. People carry out more transactions online, pushing businesses to shift their operation online to leverage on the shift and continue to operate in these challenging times. The growth and adoption by consumers in this digital economy have drive businesses to create more suitable digital products and services, creating differentiation to seek new competitive advantages within the crowded digital space.

However, digital businesses mainly revolve around selling online; according to Accenture, Digital businesses create competitive edges by adopting a combination of digital and physical presences and technologies. They deliver and adopt products and services that others cannot follow quickly to develop a comparative advantage.

2 Critical Elements of a Successful Digital Business

There are no exact definitions and standard agreements of a successful digital business. Gartner says that digital business focuses on creating and driving new value chains and business opportunities, which existing brick and mortar or traditional businesses do not offer. McKinsey emphasises that digital focuses on delivering an experience more than delivering a product to the consumers.

Generally, the digital businesses will align to these points;

- Creating new value in their core business breaking and testing new frontiers.
- Adopting technology to drive digitalisation to enhance growth, revenue opportunities. At the same time, it delivers approaches that were difficult to replicate through traditional business models.

It may be advisable for companies to review successful elements between an existing business model and a digital business. In an ever-changing business landscape with the digital realm, some trends will allow businesses to differentiate digital from traditional models.

- **Leverage existing technologies** to reduce cost and risks while gathering data and references to provide a better and uplift existing experience. Digital businesses invest in technologies to create competitive advantages such as, reduce operating overhead and create new value and experience for their customers.
- **Embrace digitalisation** and the cultural shifts within the organisation. Well-planned and execution of digital services is necessary for organisational restructuring, new roles will be created, and IT is given more significant responsibility to drive and undertake business transformation and participate in strategic planning decisions.
- **Develop new business models,** an outside-in approach and focus on customer experience with digital strategy as a first-class citizen. Consumers nowadays are looking to and increasingly willing to spend more for an exceptional customer experience, which is usually a crucial differentiator in the digital economy, as consumers' primary experience are online. Business models that can pivot, laser focus on customer satisfaction will become part of digital services of their consumers' daily life.

Regardless of the type of business and operating model that your organisation is in, changes in the global market trends are moving towards building a successful digital business plan that is imminent for survival. Understanding and setting up to operating a digital business is the first step to achieving success in the global digital marketplace.

MODULE 2: UNDERSTANDING THE DIGITAL TRANSFORMATION JOURNEY

Businesses are rushing to upgrade systems, reviewing and automating business processes and focus on talent management are deciding to digital transformation. Provide employees with a high-quality digital workplace to improve how they serve customers.

In 2020, to have a competitive advantage, about 30% of organisations will rely on the workforce's capability to leverage and exploit the use of technologies, according to Gartner.

A digital workplace is also part of a business strategy to boost agility and engagement among employees. It is to help individuals and teams to work more productively without compromising operations. It includes telecommunication equipment, productivity and collaboration software and tools. Nowadays, chatbots, virtual assistant technology, analytics, and immersive digital workspaces. It must be intuitive and straightforward to employees when they are performing their mission-critical work.

For a successful implementation of a digital workplace transformation, consider the following:

- **Vision**: Align to business and digital transformation goals. The “Vision” must be able to answer the need for an overhaul of the current work environment. It must also be able to measure increase employee engagement and productivity. Businesses need close collaboration between stakeholders, business, HR, and facilities managers to develop, shape and execute the changes. It must also include workplace demographics and the potential impact of the change. The organization should hold off the decisions on any investment until clear and agreed objectives of a digital workplace are defined.
- **Strategy**: Employees are empowered to have a greater voice in technology evaluation and selection. Establish a roadmap and blueprint to coordinate initiatives across lines of business.
- **Personas**: Employees are an essential component of any initiative to help the enterprises in establishing baselines for staff.
- **Metrics:** Use analytics to measure and generate metrics to create a digital scorecard. The metrics will be able to measure and provide a clearer visibility to management in workforce effectiveness, employee agility and employee satisfaction and resource retention. The collected data will also help the

management to assess the change management process and refine the current strategy.

2.1 IMPROVING PRODUCTIVITY

- **Employee experience**: Eventually, improving customer service is the goal, but let's first start with improving the employees' experience on their daily tasks. Collaborate with IT, real estate, and facilities managers to create conducive and productive workspaces. It will enhance collaborative work activities and provide individual space for working on personal work.
- **Organisational change**: Digital workplace initiatives typically require changes to internal processes, business culture, incentivising employees, personal development, and skills training. Identify new skills and competencies required for the digital workplace. Change management leaders can be appointed to anticipate obstacles. Integrate digital workplace technologies into existing process workflow.
- **Training**: Introduction to new technologies in the organisation can add stress to employees. The organisation can provide training, plan to reskill and hire external personnel to train them up.
- **Processes**: Generally, there is a need to re-engineer business processes. Firstly, observe how employees currently work and activities that they spend the most time on. Develop employee journey maps by collecting and analysing data linked to employee activities and experiences.
- **Information**: Employees want intelligent software for searching, sharing and consuming information. Employees can quickly and access information at the right moment will have proper analytics to be in place. Implement a file-sharing system that enables easy mobile access and real-time synchronisation.
- **Technology**: There is a need to tie all digital platforms together in a seamless experience to weave in contextual awareness, mobility, and real-time information to enable employees to serve customers. Lastly, allow employee BYOD to allow them to work on their preferred devices to improve productivity.

2.2 EXPANDING BUSINESS ONLINE

The objective of going online to be able to reach out to more customers. These are a few tips for developing your online strategy:

- **Setup a website for your business**: It is one of the critical steps to create your business awareness via cyberspace. There are costs involved, but there are many platforms for business owners to create a site without any programming. The website allows owners to leverage reputable search engines to pick up and let potential customers know your business while searching online.
- **Create Blogs for your products and services**: Creating a blog where you can post high-quality content and videos about your product. The blog is a long-term method, and it might not pay off overnight. However, every entrepreneur needs to comprehend the significance of grasping this internet advertising strategy.
- **Update your Social Media Profile**: Set up an organisation profile for your business on Social media, allowing your SEO to maximise your presence on the search engine. At the same time, it will enable your business to showcase to your potential clients what aptitude, product and services, and expertise the company provides.

It helps you get more exposure online but also creates the risk of your getting attack via various channel as:

- spoofing your website
- redirecting your customers to a fake website or profile
- attack through email with malware, ransomware and phishing for sensitive information or access to critical systems

Hence as part of getting online, in parallel, the business owners will have to look at protecting your business from advisory to uphold your customer trust and reputation within the industry.

2.3 EMERGING IT TECHNOLOGIES AND THEIR IMPACT ON CYBERSECURITY CLOUD (IAAS, PAAS, SAAS)

Cloud computing provides new opportunities for automation as well as better use of computing resources. It provides advantages, including scalability, productivity, a reduction in CAPEX and technology infrastructure as well as flexibility. As the organisations begin to expand the adoption of Infrastructure as a service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS), the organisations should evaluate the potential security risk in the company's data and resource needed while embarking on the cloud migration journey. An organisation should take into account the security trade-offs for data as well as the organisational compliance requirements when deciding to separate application and information resources from the underlying physical infrastructure.

1 IaaS security

- IaaS: A cloud platform provider that offers virtualized computing resources over the internet such as processor, storage, network resources, etc. on demand, on a pay-as-you go basis.

Compute resources; an organisation using IaaS has the same concerns as operating a data centre. The key areas of security concerns are:

- Protection against sensitive data or organisation IP
- Compliance standards align with the enterprise
- Ability to audit cloud provider to meet those compliance requirements
- What approach does the cloud vendor take in monitoring?

With IaaS environments, the organisations will have complete control of the virtualised infrastructure and resources. Any weaknesses in the vendor's security on managing the infrastructure can affect the organisation's security operation dramatically.

2 PaaS security

- PaaS: Organisation to build, run, and manage Web applications without any software and hardware infrastructure investment.

PaaS is operated in a multi-tenant setup and using shared resources, such as hardware, network, security services. In the event of successful malicious cyber attack, the high-skilled hackers is able to obtain mission-critical information and lead to data breaches. If a tenant has' root' or shell access to the servers running their instances, the hackers can access and modify the system and infrastructure configurations. Providers should define and implement sufficient security policies, guidelines, and

industry best practices on applications deployed on the PaaS platform. Consider the following when evaluating a PaaS vendor:

- Types of encryption used and where
- Data isolation
- Data and system's availability
- Support for DR and BCP

3 SaaS security

- SaaS: software is centrally hosted and licensed based on subscription

The hackers are increasingly interested in attacking the cloud environment to steal important data especially from the mission-critical systems of the company. When a SaaS provider's infrastructure is compromised, a strong data encryption mechanism provides a high level of protection for organisational data from unathorised data access. Data encryption is also able to protect against phishing and malware attacks that targets to steal user credentials which are in cleartext. Data and Network Encryption is a "must-have" technology, but it should not be the only protection.

SaaS providers take steps to mitigate risk. Organisations using SaaS services must implement internal procedures and processes to secure access to SaaS services. An organisation needs to set up internal training to teach and guide employees on how to recognise phishing campaigns. They also need to set up company policies and baselines around data security in the cloud. The organisation should be aware of the risk of storing data in the cloud. The organisations should seek security advice from a trusted, knowledgeable partner in the cloud industry to understand how company's data is sufficiently protected on-premises, hybrid and fully cloud.

2.4 MOBILITY & INTERNET OF THINGS

IoT devices have sensors, which interact and collect data based on other sensors from their environment. These devices will need to connect to the network to transmit the collcted data and be uniquely identifiable via an IP address. IoT devices use multiple methods such as WiFi and Bluetooth connections in communicating and transmitting their data. The IoT devices can also connect directly to an internet cloud-based service to exchange data.

Vulnerable IoT devices can have information stolen when connected to unsecured network. At the same time, these devices can also be manipulated to flood the data sink to cause service disruption or disseminate harmful/malicious data. Alternatively, IoT devices could also be an easy target to access and compromise a secure network or system that it connects.

MODULE 3: UNDERSTANDING RISK AND THREATS TO BUSINESS

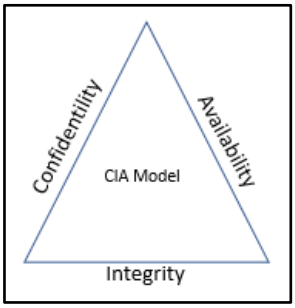
3.1 ASSETS IDENTIFICATION & RISK ASSESSMENT

1 What is Information Security?

As defined by SANS Institute,

"Information Security refers to individual or organisation undertaking the processes and methodologies designed and implemented to protect all data regardless if it is printed, stored electronically, or any other form of confidential, private and sensitive information or data storage unauthorised access, use, misuse, disclosure, destruction, modification, or disruption."

2 Information Security Objectives



Confidentiality – Only authorised access to the information

Integrity – Only authorised modifications to the information

Availability – Reliable access to the information

3 What is Risk Management

Risk is the likelihood of a loss (of an asset) and the potential impact it has on your organisation.

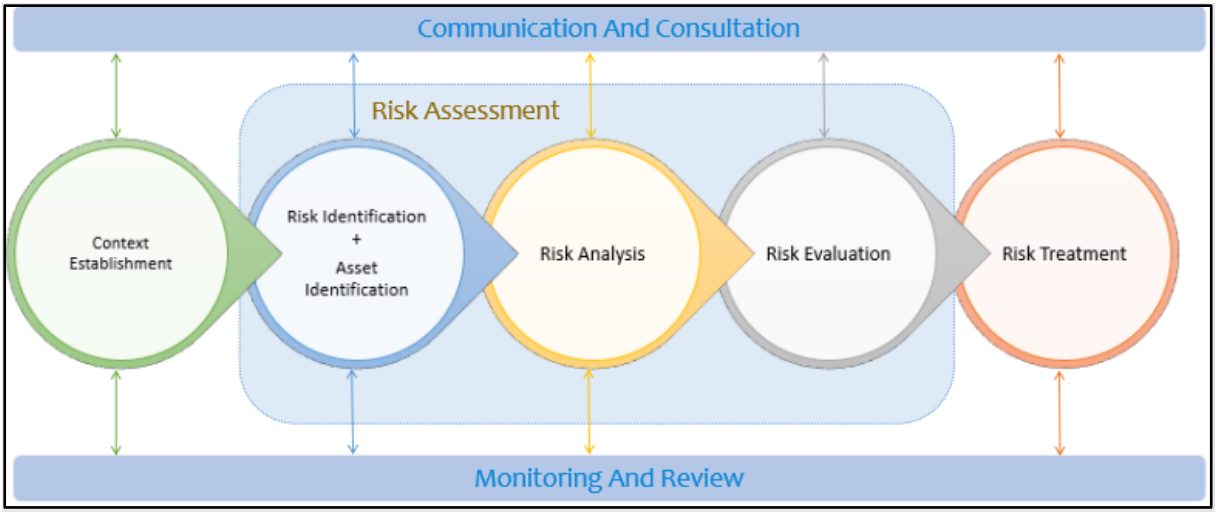
Risk Management is the process of identifying, analysing, evaluating and treating risks.

4 Benefits of an Effective Risk Management

- Effectively manage risks in a systematic approach
- Prioritise risk management based on potential consequences
- Develop a risk management culture across the organisation
- Reduce the level of risk to an acceptable level of the organisation
- Ensure that risk management resources are well utilised

Information Security Risk Management Process

5 Overview



6 Context Establishment

- Determine the purpose and scope for creating such a risk management programme.
- Identify the objectives and desired outcomes to be derived from the programme. Determine the risk appetite, which is the risk level that an organisation will accept, without further treatment of the risk.

7 Risk Identification + Asset Identification

Risk identification

- Identify all risks that will have any impact on your organisation.

Asset Identification

- Identify the list of assets including Crown Jewel systems that will affect the organisation, should the assets are damaged or lost.
  Apart from assets that have a direct impact on your organisation, other assets that have an indirect impact should also be considered.

8 Risk Analysis

Can be achieved with qualitative or quantitative analysis.

- **Qualitative Analysis**: Using an assigned score of the likelihood of a threat and the impact it has from the specific threat (suitable for SMEs)
- **Quantitative Analysis**: Using the assigned monetary value of the asset and determine the loss from a specific threat

Determine the likelihood, impact and the current controls in place to reduce the risks.

9 Risk Evaluation

Risk evaluation is the process of comparing, priortizing and implement the appropriate risk-reducing controls for a list identified risk findings from the risk management process

Factors to consider:

- Compliance with regulatory controls
- Costs of mitigation
- Costs of impact

10 Risk Treatment

Risks can be treated in many ways.

- Risk Mitigation
- Risk Transference
- Risk Acceptance
- Risk Avoidance

Ensure that the residual risk falls within the acceptable risk level of the organisation.

11 Monitoring and Review

Risk Management is not a one-time process.

Ongoing monitoring and periodic review of the risk management process is to improve the quality and effectiveness of the process.

3.2 CYBER ATTACKS

A cyber attack is an attack launched from computers against another computer, multiple computers or networks.

1 Objectives

- Denial of Service
- Data Exfiltration
- Corp Espionage

Industries targeted by attackers and the corresponding objectives

Industry	Type of attackers	Objective
1. Healthcare	1. Script Kiddie	1. Money
2. Financial Institution	2. Nation State	2. Corp espionage
3. Government	3. Cyber criminal	3. Data exfiltration
4. Service Provider	4. Hacktivist	4. Denial of Service

2 Common Cyber Attacks

- **Malware**: Malicious software including spyware, ransomware, virus and worms.
- **Phishing**: Phishing is an act of sending fraudulent communications that appear to come from a reputable source, which is carried out usually through email.
- **Zero-day exploit**: A zero-day exploit hits after a network vulnerability is announced but before a patch or solution is implemented.
- **SQL Injection**: A structured query language injection occurs when an attacker inserts malicious code into a server that uses SQL and forces the server to reveal information it normally would not.
- **Denial of Service**: A denial of service attack floods systems, servers, or networks with traffic to exhaust resources and bandwidth. As a result, the system is unable to fulfil legitimate requests.
- **MitM**: Man in the middle attacks, also known as eavesdropping attacks, occurs when attackers insert themselves into a two-party transaction.

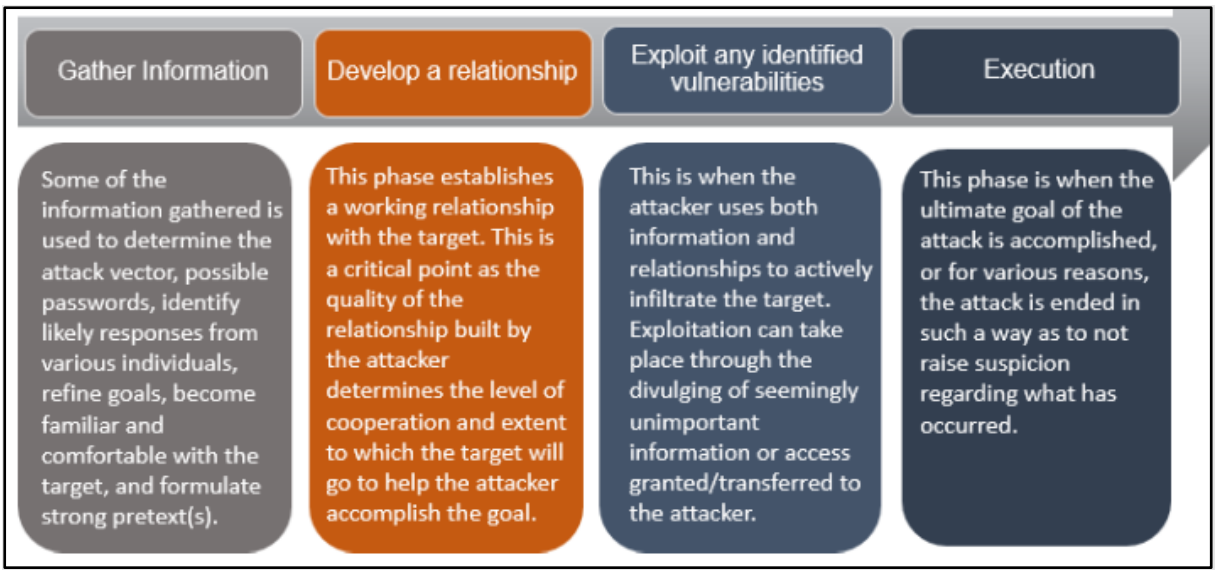
3 How do I protect myself

- Use an antivirus solution with up to date virus signature databases. There are thousands of new malware variants running every day, and having an old set of virus signature is almost equivalent to having no protection.
- Leverage a full set of protection features of your security solutions/ technology, e.g. Intrusion prevention (Network level), Antivirus (File-level) etc.

- Avoid clicking malicious or suspicious links in emails and social media websites such as Facebook, Twitter, and instant messenger chats such as WhatsApp, Skype etc.
- Make sure your software/systems are up to date, which includes the operating systems, browsers and all the plugins used by the browser

3.3 SOCIAL ENGINEERING

1 Social Engineering Overall Processes



A social engineering attack leverage human interaction (social skills) to illegally obtain or compromise information about an organisation or its computer systems. An attacker may appear unassuming and respectable, could also claim to be a new employee, handyman, or researcher and even provide credentials to gain trust and support his/her identity. The attacker can piece together enough information by asking questions to infiltrate an organisation's network. Typically an attacker will try to gather enough information from more than one source within the same organisation and rely on the data from the first source to add to his or her credibility.

2 Common Social Engineering Techniques

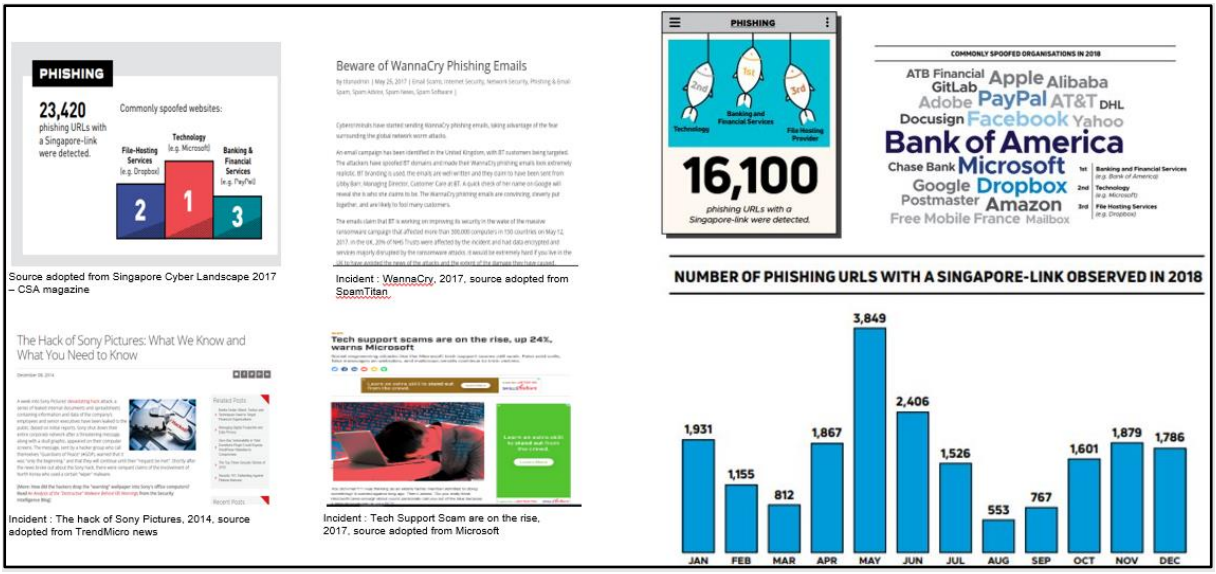
	Definition	**How it happened**	**How to prevent**
Email fraud	Phishing is one type of social engineering. The attacks are carried out using email or malicious websites to ask for personal information	An attacker will try to send an email seemingly from a reputable organisation requesting account information, often pretending that there	Do not reveal personal or financial information in emails, and do not respond to email solicitations for this information. This includes

	by posing as trustworthy.	is an issue with an individual account or profile. The user who responds with the requested information can be used by attackers to access confidential data such as a piece of account information.	following links sent in emails.
Phone fraud/ Vishing	Cybercriminals **uses the phone to get unauthorized accessed personal confidential information of their victims**. This is known as voice phishing, criminal employed skillful social engineering tactics to trick victims, giving up private data and accessing bank accounts.	Sometimes unsolicited calls, done via robocalls or from people claiming to be officials, employees from a courier company, or call centres from banks or telcos. They usually ask you for money or validate personal information. An individual should be aware that government or institution will not seek sensitive information via phone.	1 Verify incoming calls using other sources of verification outside the current call, such as validating using OTP or secret questions 2 Do not share login information over the phone. 3 Do not share account data or personally identifiable information over the phone. 4 Be alert when being asked to change your login credentials over the phone
Tech Support Scam	A technical support scam refers to telephone fraud activities carried out by scammers claiming to offer a legitimate technical support service to gain unauthorised access	Scammers trick the victim into installing a remote desktop software with which they take control of the victim's computer and then use various Windows components and utilities, third-	Examine the message closely- look for obvious signs of fraud such as poor spelling, unprofessional images, poor grammar. You should also perform an Internet search for the

	to a sensitive system or profile.	party utilities and other tasks to gain trust from the victim in believing that the computer has issues that need to be fixed, and deceived the victim into paying for "support."	provided phone number that is listed in the pop up to verify its legitimacy.
Unsecure Third-Party Devices	Unsecured 3rd party devices, be it USBs or hard drives, potentially could allow for viruses to infect your wifi network through it.	In such attacks, people who find and plug unsecured 3rd party devices into their computers could allow for the transmission of viruses even if it came from a secure sauce.	Ensure that devices are secure with encryption and use third-party software or hardware to segregate 3rd party devices. Encourage Advice employees to utilise a separate flash drive used for personal home use from those used in the office.
Baiting	In a Universal Serial Bus, USB drop attack, attackers leave USB devices for people to find and plug into their computers.	To initiate an attack, the adversary will deliberately drop infected USB drives in public locations, such as parking lots, to entice their target victims to pick them up and opening them using their computers. These usually contain a virus, malware or ransomware. When plugin, it will infect the source machine and subsequently the entire network	Ensure that devices are secure with encryption and use third-party software or hardware to segregate 3rd party devices. Encourage Advice employees to utilise a separate flash drive used for personal home use from those used in the office.
Spear Phishing	Spear-phishing is an attempt to steal sensitive information	This attack can be achieved by getting personal information	**Monitor personal information posted on the internet:**

	such as account credentials or financial information from a specific victim, often for malicious reasons.	on their victims, such as their friend's contacts, hometown, employer, frequent locations, and what they have recently bought online. The attackers will subsequently disguise themselves as trustworthy friends or entities to acquire sensitive information.	Review your online profiles to evaluate how much personal information is publicly available for potential attackers to use? If there is information that you do not want a scammer to use, do not post it – make sure that you've configured privacy settings to limit what others can see.
Tailgating	Tailgating, sometimes referred to as piggybacking, is a physical security breach in which an unauthorised person follows an authorised individual to enter a secured premise.	An employee who opens a door and holding it open for an individual without badges, or the passive acceptance of a uniformed worker. The concern with this lax practice is that they open the office building to undocumented and unauthorised entry by individuals who could mean harm to your property and employees.	Apply physical barrier with education for the employee to be alert of any undocumented individual roaming around the buildings

3 Social Engineering Statistics



Phishing emails usually spoof or pretend to originate from reputable firms and organisations. Companies in the banking and financial services, technology, and file hosting services made up almost 90 percent of spoofed companies in 2018. In Singapore, websites of Government organisations such as the Ministry of Manpower (MOM), Singapore Police Force (SPF) and Immigration & Checkpoints Authority (ICA) were commonly spoofed to steal personal and financial data from victims. Phishing activity typically increases when major events occur. Threat actors dupe victims into opening phishing emails and their attachments.

4 Best Practices to Prevent Social Engineering

Be aware of the information you're releasing.

- Be alert of any unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information.
- In no circumstances do not provide any personal organisation information, including the company's structure or networks, unless you are confident and validate the individual credential.

Always verify the sources and recipients.

- Pay attention to the URL of a website. Malicious websites may look identical to a legitimate site and do not click on the malicious link attached in emails.
- Do not provide personal or organisation information to invalidated recipients.
- If an unknown individual claim to be from a legitimate organisation, try to verify his or her identity directly with the company.
- When you are unsure about the legitimacy of an email request, try to verify it by contacting the company directly. Do not use any contact information

provided on a website connected to the request; instead, check previous statements for contact information.

Identify which of your assets are most valuable to criminals.

- Identify, classify and protect the valuable asset of the organisation against potential cyber-attacks.

Give employees a sense of ownership when it comes to security.

- Employees should understand their obligations in security and protect the organisation from any unintentional disclosure of sensitive information.
- Install and update your antivirus software, firewalls, and email filters to reduce some of this traffic block access to suspicious websites.

MODULE 4: SECURING THE BUSINESS

4.1 HANDLING DATA SECURELY

1 Introduction

Data is one of the most important assets for any organisation. Data include customer data, personnel data, product information, financial information, business information etc. Data exists in different stages (or states), mainly data at rest, data in transit and data in use. In any organisation, most of the decisions are based on the data they process from various sources of the business components. Data related to consumers need to be handled securely to meet the compliance and regulatory controls recommended by local government bodies.

Data needs to be handled securely and safeguarded for its availability (who needs it), the integrity of data (who depends on it), and confidentiality (who authorised to process it).

Following are some of the basic controls that can help any organisation achieve data security.

2 Data Handling Policy

Normally the data handling policy states the guiding principles for information stewardship and a framework for classifying and handling data. This can be a one-page legal document providing the direction. The 'Can Dos' and 'Cannot Dos'. E.g. Internal, External, Confidential, Clean desk, no sensitive data in the cloud or email, etc.

The data handling policy should also specify how the data should be destroyed once a task has been completed.

3 Information Asset Register

An asset is defined as "anything that has value to the organisation", which means all information assets are to be considered rather than simply physical assets, but it is the information (data) that is of real interest. During the risk assessment process, we identify critical business processes and the data or IT systems that support the critical business. Each such system, in turn, comprises of various information assets, which utilise critical components like software, hardware, physical and infrastructure facilities to perform designated business functions in an efficient manner. Identification of all such information assets and critical components and maintaining an up-to-date record is essential to know what we intend to protect.

These assets can be grouped under different categories based on their criticality towards confidentiality, integrity, and availability of information. This classification is necessary to implement various protection measures.

This process results as a list of all information or data assets for an organisation called as Asset Register, which also includes the information on their owners, values, categories and classification and other additional details.

If we do not even know where your data is, then we cannot secure it. Once we know where and how it is being collected or processed (for example, shared corporate drive), it is recommended to have sufficient security controls around the data (for example, no thumb drive usage on the corporate network, unsecured personal laptops etc.).

4 Third-Party Security Audits

A third-party security audit is a due diligence activity to gain a level of assurance with the overall security through an independent evaluation of a business entity or professional practice conducted by experienced ethics and compliance professional.

This can be a simple one-pager questionnaire that is usually more than enough to identify risk and take positive, remedial action if the information has been put at risk.

This practice should be periodical, and the length of time between such audits should depend on the size of the organisation, state and needs of the organisation.

5 Employee Security Awareness

Well trained, security-aware staff are the backbone of the organisation in handling the data (or information assets) securely. This is part of the risk management life cycle. They act as a frontline defence against the most pervasive and successful cybersecurity issues like:

- Phishing and malware infection
- Security leaks caused by password sharing
- Accidental data disclosure

Regular security awareness campaigns and one-to-one training are essential as most of the business processes heavily rely on the employees to keep the data safe. The employees need to have an awareness of the sensitivity of data to understand why it needs to be secured. Security awareness training programmes should train staff in all aspects of security, including improving security behaviour.

6 An Incident Response Procedure

Incident Response (IR) is a well-documented and structured methodology for handling security incidents, breaches, and cyber threats to allow the employees to effectively identify, minimise the damage, and reduce the cost of a cyber-attack while finding and fixing the root cause to prevent similar future attacks. The standard procedure consists of several stages: planning/preparation, detection, initiation, recording, evaluation, containment, eradication, escalation, response, recovery, closure, reporting, post-incident review and lessons learned.

- Reduce the probability of information loss by implementing the above controls.
- A prompt, effective response will minimise the impact of any data breach.

7 Regular reviews of the above

The security programme will be successful only when it is periodically assessed to improve controls in place to address the gaps in the programme, changes in the environment and to meet new requirements.

4.2 CYBER HYGIENE (UPDATING IT ASSETS AND IMPLEMENTING CYBERSECURITY MEASURES)

1 What is Cyber Hygiene?

Cyber hygiene refers to the practices that computers and other related device administrators and users leverage to maintain system health and improve online security posture. These practices are often part of a routine to ensure identity safety and other details that could be stolen or misused. This is similar to physical hygiene. Cyber hygiene must be conducted regularly to ward off natural deterioration and commonly know threats.

2 Who is in charge of the organisation's Cyber Hygiene?

Cyber Hygiene Is Everyone's Job. Like personal hygiene, cyber hygiene should start with the basic actions that are most likely to promote good health.

3 Best Practices in Cyber Hygiene

Assign someone responsible for cybersecurity

Cyber hygiene requires ongoing discipline and attention. Someone familiar with your business needs to be responsible for cybersecurity. They need to manage the decisions related to cybersecurity and provide the management push to keep it ongoing.

In small/medium business, this person can be either the owner/operator of the business or someone who reports to them.

Patch your software

Keeping your software up to date is one of the simplest and most effective ways to protect your business. Recommend implementing patch and vulnerability management for all devices and systems.

For small businesses, the easiest option is to let the software update itself. For medium businesses, consider having your own patch management system.

Patching is not just for operating systems; make sure that applications like web browsers (Chrome, Firefox, Internet Explorer/Edge, Safari), email, office productivity and PDF document readers are kept up to date. Don't forget to include systems that aren't in the office when you consider patching. Speak to your IT provider about things like your email server, web server and mobile devices.

Backup critical data

Backups are still a cornerstone of system security. Malware and ransomware can encrypt or destroy the data stored on your systems. Once infected, it is often too late to save your data. If everything else goes wrong, reliable, well-protected backups will be the last resort to restore your business' digital infrastructure. With a little bit of attention and care, a backup system can be configured that can enable you to recover your business if the worst happens.

Cloud storage that syncs with local storage, such as OneDrive or Google Drive, should not be seen as a backup. If a ransomware attack locks local files, these changes will be synchronised to the cloud drive.

Also, if you are restoring after a ransomware attack, take a copy of your backup before attempting to restore. If you try to restore data and haven't fully fixed the ransomware infection, your backup may be destroyed or encrypted. Take another copy before plugging in a USB drive or connecting to your backup service to mitigate this possibility.

Strong Access Management

Access management is a practical and straightforward cyber hygiene best practice. You should set strong passwords and enable two-factor authentication (2FA) across all devices and accounts.

Passwords should be hard to guess, incorporating a combination of numbers and special characters. An individual should avoid reusing passwords across accounts –

especially on devices and applications, especially across accessing sensitive business information. This is to prevent because your information is leaked, credential stuffing and brute force attacks can use this leaked information to target other accounts if one of the accounts is breached.

The list below provides strategies to improve your access management:

- You are storing your passwords in a secure location, such as a password manager or vault.
- Update your passwords regularly, at least every six months.
- Using passphrases instead of passwords, which is a string of words. They are easier to remember and could be more secure than passwords.
- Configure a guest network at home using a different password for guests to use rather than giving them access to your primary network.
- Use 2FA whenever possible. This security protocol uses a secondary device to verify you are who you say you are. Verification codes are usually sent via text or email for you that have been set up during the sign-in process.

Have a secure email system

Although cybercriminals have branched out into other channels, including phone, SMS and social media, email remains one of their favourites attack methods because it is cheap and effective.

In the past, some businesses have relied on the strength of their desktop antivirus products to protect information systems. However, this is no longer sufficient, and it is important to have multiple layers of scanning on high-risk interfaces such as email.

Speak with your provider or IT staff to make sure all emails you receive are scanned with a high-quality commercial product. Also, ask them to implement attachment type filtering to prevent common malicious attachment types like executables and scripts.

Install proper endpoint protection

Very important to note that traditional AV is no longer an effective means of protection. You firstly need to move away from signature-based detection (antivirus) and start using behaviour-based monitoring - and ideally throw in some ability to detect and respond to attacks with EDR.

Have an incident response plan

All businesses, big or small, should implement an incident response and recovery plan to minimise downtime in the event of an attack. A basic incident response plan will help your business understand how to prepare and respond to an incident.

At its simplest, an incident response plan will be the contact numbers and responsibilities of people who need to be involved in a cybersecurity incident occurs. More comprehensive incident response plans can consider scenarios, business continuity strategies and more.

Educate all employees of the plan so that there are no questions about the next steps during an attack. This education program should also include having a hotline prominently displayed to know whom to contact if they suspect a breach.

Restrict access

Restricting access to information can help prevent data leaks. However, this needs to be balanced against allowing enough access to ensure all your staff can access the information they need in a timely manner. Allowing staff access but ensuring it is audited (and reviewed) can provide a reasonable compromise.

Restrict administrative privileges

Systems administrators (also known as admins, super users, and root users) all have higher levels of system access that allow them to bypass restrictions and auditing.

There are two key things to remember:

- Anyone who has administrative privilege in your business needs to have your full confidence.
- Administrative privilege is exactly the type of access that cybercriminals seek if they break your business electronically.
    - Restricting the number of administrative users helps to protect the business from insider threats and external cybercriminals.

Security Awareness and Training

Teach employees what they can do to protect both themselves and the business. Provide them with proper cybersecurity awareness training.

4.3 PROTECTION OF CUSTOMER DATA

1 Introduction

Data is one of the most important assets for any organisation. Data include customer data, personnel data, product information, financial information, business information etc. Most of the times, the decision management in an organisation depends on the data they process that is related to their business processes. All these reasons make data protection one of the top priorities for any organisation. The protection includes safeguarding the data for its availability (who needs it), the integrity of data (who depends on it) and confidentiality (who is authorised to process it).

For any process in the organisation, it is highly recommended to have clear policy, procedures to support the policy and guidelines to keep it in practice. Data Handling Policy can be a one-page legal document explaining the 'Can Dos & Can't Dos'. For example, internal, external, confidential, clean desk, no sensitive data in the cloud or email etc. This policy should also specify how the data should be destroyed once the specific task has been completed.

In organisations, data security controls are used to safeguard sensitive and important data and to implement appropriate countermeasure against unauthorised use. These controls are used to detect, response, minimise, or avoid security risks for the systems & data.

2 How to achieve this?

At a high level, the process of risk assessment involves scoping, identifying & classifying information assets, identifying & assessing risks to the information assets, planning for risk management & implementing or adopting a risk mitigation strategy for all the identified risks to information assets.

3 What are the stages (or states) of data? (or How this data exists?)

The basic states of data are data at rest, data in motion & data in use. Data protection includes protection of all the states of the data irrespective of its states based on business needs. Following are few examples of data in each state that we normally come across in any organisation

Data at Rest:

- Data on disks, tapes, CDs/DVDs, USB drives & any other backup media etc

Data in Motion:

- Network traffic on the wire or the data being transferred on a network

Data in Use:

- Data that is actively in use, like the files in use, printed copies of data etc

These days, most of the times, sensitive or important information or data resides in electronic form. The main aspect of data security implies that all these forms of data (data at rest, in transit & in use) is protected, and data leak protection is implemented. Moreover, it involves other operational, administrative, and architectural controls as well.

4 Information Asset Register

During the risk assessment process, we identify critical business processes and the data or IT systems that support the critical business. Each such system, in turn, comprises of various information assets, which utilise critical components like software, hardware, physical and infrastructure facilities to perform designated business functions in an efficient manner. Identification of all such information assets and critical components and maintaining an up-to-date record is essential to know what we intend to protect. These assets can be grouped under different categories based on their criticality towards confidentiality, integrity and availability of information. This classification is necessary to implement various protection measures.

This process results in a list of all information or data assets for an organisation called as Asset Register, which also includes the information on their owners, values, categories and classification and other additional details.

5 Different ways of protecting data

Following are different ways to protect customer data and avoid data leakage in the organisation and protect customer data.

Third-Party Security Audits

The third-party security audits provide independent reports on the security status or posture as the primary mission is to provide an independent opinion. A third-party security audit involves having an independent party review a specific process or programme against established criteria. To begin with, a simple one-page questionnaire is usually more than enough to identify risk and take positive, remedial action if the information has been put at risk.

Employee Security Awareness

For any organisation, employees are the key resources. Normally, regular security awareness campaigns and one-to-one training are essential to allow organisations to mitigate risk and ensure compliance. The benefits include initiating security awareness training in any organisation. This is considered as one of the strongest control that any organisation must be considered to protect the organisation's and customer's data. It is always recommended to educate employee with the knowledge and capabilities to keep data safe.

An Incident Response Procedure

Incident Response (IR) is a well-documented structured methodology for handling security incidents, breaches, and cyber threats to allow employees to effectively identify, minimise the damage, and reduce the cost of a cyber-attack while finding the root cost and fixing the issue(s) to prevent future attacks. The IR plan's key steps may include preparation, containment, notification of appropriate personnel, reporting, eradication, and lessons learned.

Limit Access to Customer Information

Not everyone in an organisation needs to see customer's personal information irrespective of the way data is collected. The fewer people with a genuine need for access, the fewer the opportunities for hackers to strike at a weak point. If we don't restrict access to data based on who actually needs it, then we are presenting a much larger potential attack surface. This is the reason we need to identify different data categories to make sure sensitive data is protected and can be accessed only by authorised employees who have a legitimate reason to access it.

Collect only Necessary Data

Collecting unnecessary customer data means wasting energy and resources and providing a larger cache for cyber hackers to target – this also makes customers nervous about why the business needs to acquire this information. Collect only information that you need for business purposes. An additional step, offer customers the option of whether they wish to share personal information with you or not.

Consider Destroying the Data after You've used it

As part of the data collection, there should be a guideline and purpose for collecting the data. When the purpose of the document or data is no longer required, there should be a plan in place to destroy it. It should be included as a process that is carried out on an ongoing basis to ensure you are not hoarding excessive data that makes the companies vulnerable to data breaches and attacks. You may want to look at the following data destruction approach:

What Are The Different Forms of Data Destruction?

- Delete/Reformat.
- Wipe.
- Overwriting data.
- Erasure.
- Degaussing.
- Physical destruction (drill/band/crush/hammer)
- Electronic shredding.
- Solid-state shredding.

Make Customer Privacy Everyone's Business

Customer Privacy is critical to the success of any business especially around reputation and branding. Hence it is critical that their information is securely protected. At the same time, there must be an education and awareness plan in place to educate everyone in the your organisation about the comprehensive security program and policy that is in place.

A common data protection approach currently being used by businesses is to limit access to the data after it's been acquired. This approach insufficient to provide data. Firstly, as soon as a company shares data internally or externally, its ability to control access deteriorates rapidly.

Synthetic Data as Protection

Add random noises. For instance, observations are grouped into segments based on a collection of sales and a random number added to the sales in each segment.

- Rounding. For example, sales are rounded to the nearest hundred
- Top Coding. For example, observations are divided into groups
- Aggregating. For example, weekly sales are summed, and prices and promotions are averaged across stores within a market.

MODULE 5: UNDERSTANDING THE BUSINESS OBLIGATIONS

5.1 PDPA

1 What is Personal Data?

Personal data refers to data used to identify an individual with a single piece of information or a set of data put together. Personal data can be information gathered from a single organisation or coming from a combination of services available.

2 What is the PDPA?

It provides a baseline standard of protection for personal data in Singapore. It complements sector-specific legislative and regulatory frameworks such as the Banking Act and Insurance Act.

It comprises various requirements governing the collection, use, disclosure and care of personal data in Singapore.

PDPA is also part of the national effort for the Do Not Call (DNC) Registry. Individuals may register their Singapore telephone numbers with the DNC Registry to opt-out of receiving unwanted telemarketing messages from organisations.

3 Objectives of the PDPA

It defines the baseline for and how organisations collect, use, or disclose while conducting their business operations.

Data protection is a process that necessary to ensure the safeguard data from being misused for revenue and other unethical activities. It helps to maintain individuals' trust in organisations that manage their data.

The purpose is to regulate the use and sharing of personal data among organisations.

PDPA endeavours to strengthen Singapore's position as a trusted hub for businesses.

4 Scope of the PDPA

It includes all personal data stored both digitally and manually on paper.

The areas that PDPA does not covers are:

- Using data for individual or personal capacity.
- An employee of an organisation but acting in an individual capacity.
- public agency with the collection.

- Business contact. (e.g., individual's name, business title, telephone number, business address, business email, business fax number and similar information)

5.2 CYBERSECURITY ACT

The Bill was passed on 5 Feb 2018. It also received the President's assent on 2 Mar 2018 to become the Cybersecurity Act. The purpose of the Act establishes a legal framework to create oversight and maintenance of Cybersecurity practices and implementation within Singapore.

There are four key focuses:

Strengthen the protection of Critical Information Infrastructure (CII) against cyber-attacks.

- Systems directly providing key services
- Cyber-attacks on CII create a huge impact on the economy and society.
- Provides a framework for CII owner on their obligations to protect the systems from cyberattacks
- Helps to build resilience into CII, protecting Singapore's economy and our way of life
- Business includes: Energy, Water, Banking and Finance, Healthcare, Land, Maritime, and Aviation transport, Infocomm, Media, Security and Emergency Services, & Government

Authorise CSA to prevent and respond to cybersecurity threats and incidents.

- empowering the Commissioner of Cybersecurity to investigate cybersecurity threats and incidents
- determine incidents impact and prevent further harm or cybersecurity incidents from arising
- will be calibrated based on the severity of the cybersecurity threat or incident

Establish a framework for sharing cybersecurity information.

- facilitates information sharing - helping government and system owners to identify vulnerabilities and prevent cyber incidents
- defines a framework where CSA can request information from system owners

Establish a light-touch licensing framework for cybersecurity service providers.

- license only two types of service currently - penetration testing & managing security operations centre (SOC) monitoring

- considering the services to have access to sensitive client information
- considered mainstream in our market and have a significant impact on the overall security landscape
- striking the need to maintain a balance between security and the creating of a vibrant ecosystem
- You can access the Cybersecurity Act on Singapore Statutes Online.

5.3 Computer Misuse Act

The Computer Misuse Act is to make provisioning for securing computer material against unauthorised access or modification and for matters related to it. It covers

- Any unauthorised access to computer material who knowingly use a system to perform any function to get access to any data, a program without authority, including any damage resulted due to the offence
- Unauthorised modification of computer material, including any damage, is caused
- Enhanced punishment for crimes involving protected computers by personnel who have been granted and abuse their access

5.4 Contractual Obligation & Liabilities

The contract protects your business. It is critical to include clauses that will limit your liability. The contract also provides security liability when doing online transactions. The contract will help your business limit the compensation claimed when a breach of contract happens. It happens when a service or good isn't delivered, for instance, if an SLA is breached.

A contract includes clauses that limit your liability. On occasion, the contracts contain provisions that exclude all liability on their part. It might be considered an ideal solution to protect your business, but it is not straightforward to define and evaluate the reasonable amount.

When using this kind of clause, it must be made clear to any party and agreed upon, as the court will only uphold provisions that all parties were made aware of. The Unfair Contract Terms Act 1977 was created precisely to limit how easy it is to use limitations and exclusions of liability in any commercial contract.

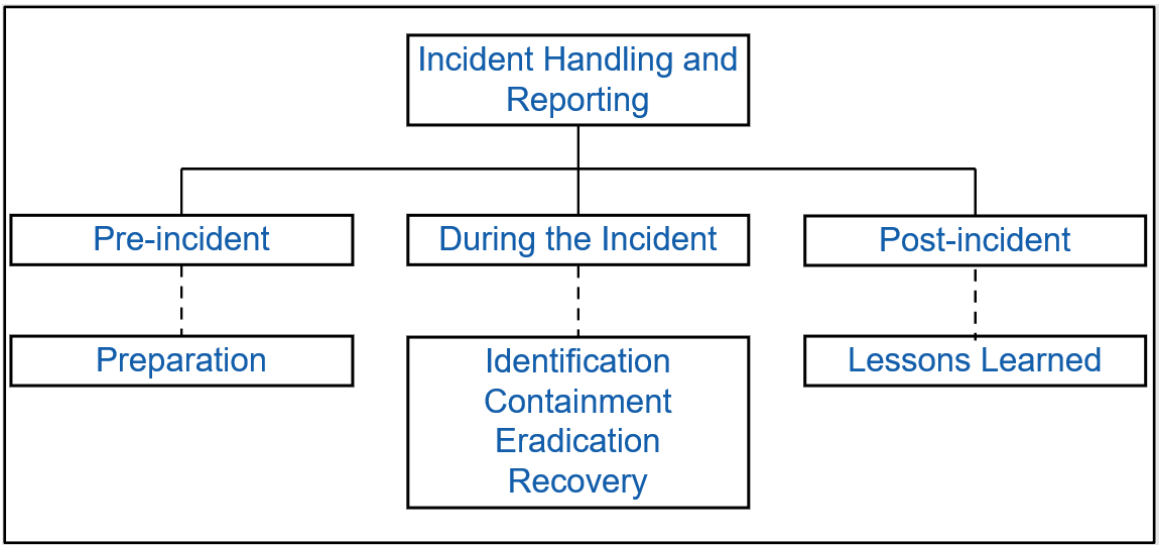
The key is to limit your liabilities as effectively as possible with an agreed sum. Putting a cap on penalties is beneficial, must be clearly defined per contract or aggregated amount.

5.5 INTERNATIONAL REGULATORY REQUIREMENTS

It is an international effort towards standardising requirements for marketing applications. When regulatory authorities are involved in reviewing the data submitted to support a proposed clinical trial, in most cases, they operate a harmful vetting procedure. In most other countries, the regulatory authorities review the safety and quality data presented to them in summary form and, if appropriate, indicate that they have no objections to the proposed trial. Some regulatory authorities require complete safety reports to be included in applications to undertake clinical trials.

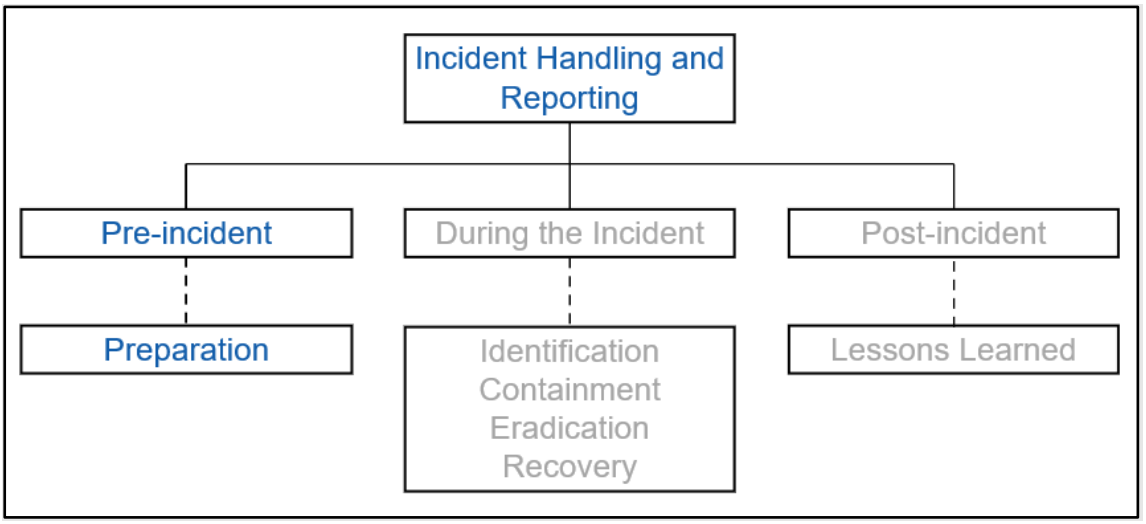
MODULE 6: INCIDENT HANDLING / REPORTING

1 Overview

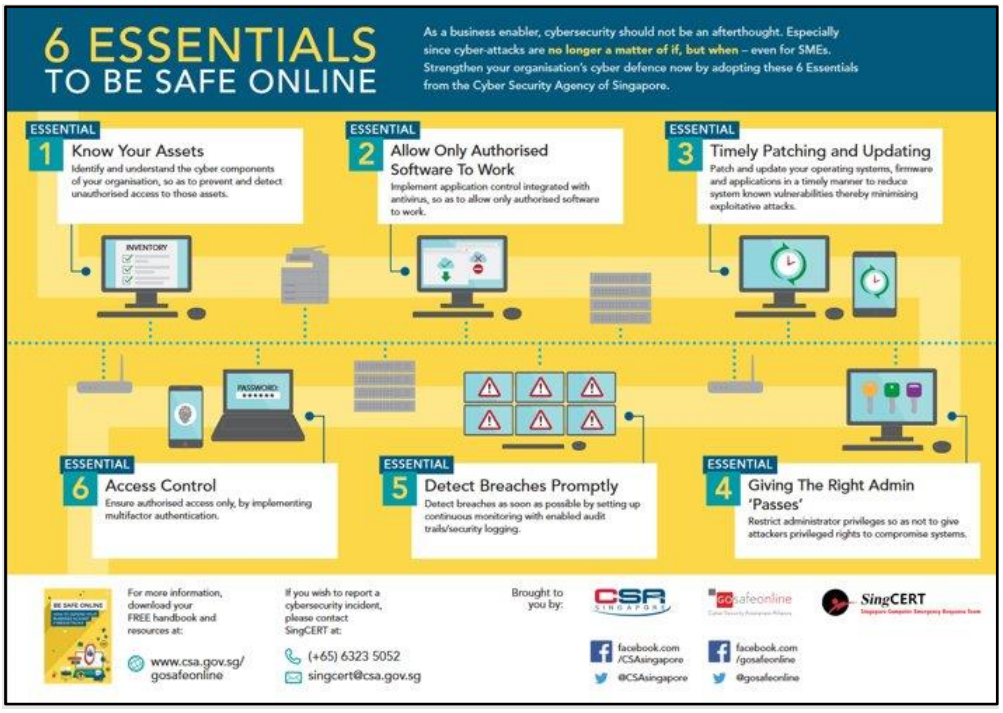


As illustrated, a lot of work is required during an active incident. SMEs usually would not be able to cope when an incident occurs. Thus, the pre-incident phase is key to any SME's survival. In addition, the post-incident phase is an important facet too. Failure to learn from history only means adversaries can exploit weaknesses in the same manner.

2 Pre – incident



- Do you know what your IT assets are?
- Do you know who to contact and who should take charge during an incident?
- Do you have any potential evidence sources but have not identified them yet?
- Do you have all the necessary documentation?
- Do you store/process any Personally Identifiable Information (PII)?



Do you know what your IT assets are?

- Where are they located?
- What type of hardware?
- What is the IP address range? (Static or dynamic IP?)
- How many?
- Who is using that particular IT asset?

Do you know who to contact and who should take charge during an incident?

- Planning for an incident could be your best business decision in times of crisis.
- Have important contact numbers ready, such as your IT vendor or SingCERT (Singapore Computer Emergency Response Team).

Do you have any potential evidence sources but have not identified them yet?

- Discuss with your IT team or IT vendor (Have a conversation with your IT team or vendor. Having that conversation before a critical incident may increase the chances of your precious business being resilient in the face of cyber-attacks as it speeds up the investigation process later. Should your IT vendor or IT team be unable to advise you, perhaps consider professional consultancy services?)
- Some incident simulations may help you identify the evidence sources (This is usually done as part of professional consultancy services but can prove valuable.)
- Consider purchasing solutions that could help automate these processes (endpoint agent solutions, but these could cost lots)

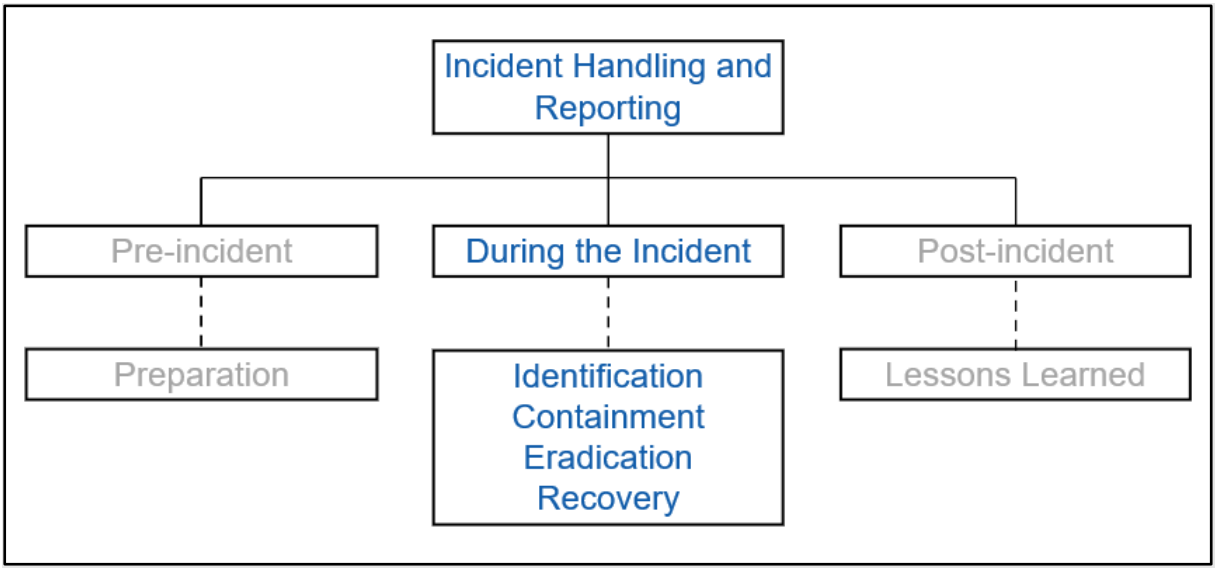
Do you have all the necessary documentation? (Paperwork is tedious, but could be accepted as key evidence and helps in recovery)

- Contact list
- Incident forms
- Communication Log
- Chain of Custody forms

Do you store/process any Personally Identifiable Information (PII)?

- Keep in mind about the Personal Data Protection Act (PDPA)
- Business owners may have to report any PII loss within 72 hours

3 During the incident



Things to note:

- Are you confident of handling the incident internally?
- If not, engage professional services
- Do not tamper with any assets that are suspected to be the cause of the incident

Contact SingCERT

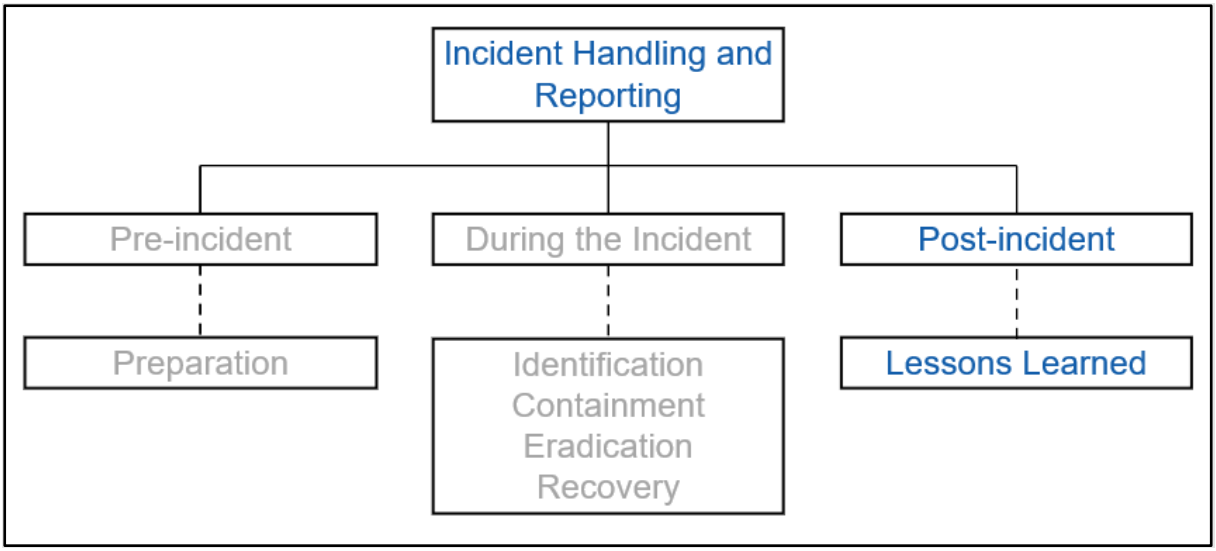
Generally, during the incident:

- Identify the cause
- Contain the incident
- Eradicate the cause of the incident
- Once all is safe, gradually recover services

Usually, what is highlighted above may require technical expertise and preparation.

Watch out for common mistakes! (include accidental tampering of evidence)

4 Post-incident



- Assess what led to the incident
- Document it down. History often provides valuable lessons
- Assess if money needs to be spent to fix the weaknesses