SG CYBER SAFE

CYBERSECURITY TOOLKIT

FOR ENTERPRISE LEADERS

UPDATED: 7 OCTOBER 2021

About the Cyber Security Agency of Singapore (CSA)

Established in 2015, CSA seeks to keep Singapore's cyberspace safe and secure to underpin our National Security, power a Digital Economy and protect our Digital Way of Life. It maintains an oversight of national cybersecurity functions and works with sector leads to protect Singapore's Critical Information Infrastructure. CSA also engages with various stakeholders to heighten cybersecurity awareness, build a vibrant cybersecurity ecosystem supported by a robust workforce, pursue international partnerships and drive regional cybersecurity capacity building programmes.

For more news and information, please visit www.csa.gov.sg

Cybersecurity is a
business investment.
It will pay for itself over time.

Overview

Digitalisation has changed the way we work, learn, transact, and stay connected. Developments such as global pandemics have accelerated the scale, scope, and speed of digitalisation. There are tremendous opportunities as businesses embrace digitalisation. However, an increasingly digital way of life also increases cyber risks.

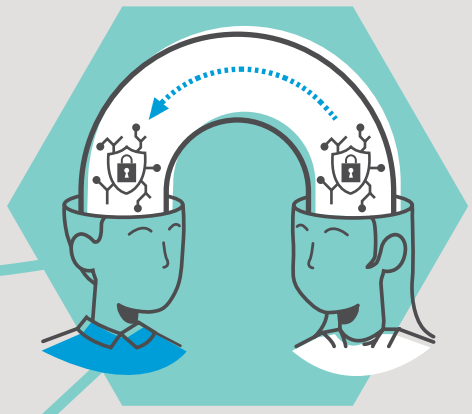
The benefits of digital transformation can be fully reaped when enterprises invest in cybersecurity. Cybersecurity is a critical enabler for businesses – business leaders should view cybersecurity as a competitive advantage, especially in industries where trust is key to business relationships.

The Cyber Security Agency of Singapore (CSA) has developed a series of cybersecurity toolkits for enterprises. These include the "**Cybersecurity Toolkit for Enterprise Leaders**", the "**Cybersecurity Toolkit for SME Owners**", the "**Cybersecurity Toolkit for Employees**", and the "**Cybersecurity Toolkit for Information Technology (IT) Teams**".

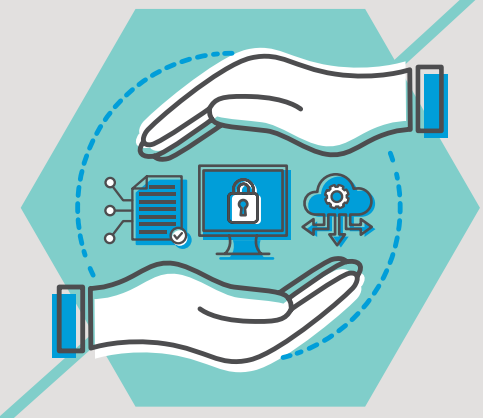
This cybersecurity toolkit is targeted at larger enterprises that adopt a two-tier corporate hierarchy with a Board of Directors and a C-suite team. This toolkit will help enterprise leaders understand the five fundamental areas that an organisation should consider to ensure cybersecurity is adequately addressed.

CYBERSECURITY GUIDANCE FOR ENTERPRISE LEADERS

Cultivate cybersecurity leadership in your organisation



Educate your employees on cybersecurity



Protect your information assets[1]

Secure your access and environment

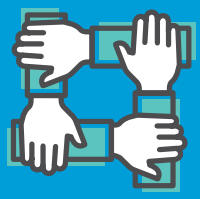
Ensure your business is cyber resilient

[1]Refers to hardware, software and data assets.

Each area within the toolkit addresses three questions:

What should you, the enterprise leader, do?

This section will provide actionable guidance for enterprise leaders.



What should your organisation do?

This section will provide actionable guidance for your organisation, with oversight from enterprise leaders required.

What do good cybersecurity practices look like?

This section provides guiding questions and statements designed to generate discussions with your relevant departments (e.g. IT/cybersecurity team and/or risk management team). This will enable enterprise leaders to assess if good cybersecurity practices are being observed in your organisation.

Cultivate Cybersecurity Leadership in Your Organisation

Why is this important?

Cybersecurity is about risk management, and not just a technical issue. It requires the Board and top management to make trade-offs between enterprise security, usability of systems, and cost. Such trade-offs require an executive decision, and will depend on the risk profile of your organisation, and the environment it operates in.This decision cannot be made by IT or security experts; it has to be made at the Board and top management level. The Board and top management should be informed about cyber risks faced by your organisation and decide how much to invest in cybersecurity.

What should you, the enterprise leader, do?

View cybersecurity as a business investment

- Cyber risks carry reputational and legal implications. Correspondingly, these implications translate into potential cost compensations when a company sustains reputational and legal damages. The Board and top management should therefore view cybersecurity as an investment to help their organisation prevent incurring such costs.
- Recognise cybersecurity as a competitive advantage and source of value, where organisations differentiate themselves from competitors by being more secure and trusted.
- Appoint personnel (internal or external) with sufficient authority to oversee and be responsible for your organisation's cybersecurity programme. This could be the Chief Information Security Officer (CISO) or Head of Information Security, who will be responsible for establishing and implementing the overall cybersecurity strategy and programme, including but not limited to cybersecurity policies and procedures to protect information assets, cybersecurity controls, and the management of cybersecurity in general.

Ensure governance and oversight from top management

- Maintain governance and oversight over cybersecurity-related matters. There should be sufficient expertise and knowledge within the Board and top management to provide direction on cybersecurity strategy and to be accountable for decisions made. Enterprise leaders should be bilingual in technical and strategic languages.
- Establish and/or endorse cybersecurity policies and ensure that cybersecurity practices commensurate with the risk profile of your organisation. Doing so at Board and top management level also ensures a holistic approach is taken, avoiding "silo-ed" approaches across different functional divisions.

Establish cybersecurity strategy and roadmap

- The cybersecurity strategy and roadmap reflect your organisation's investment in cybersecurity resources to pursue your organisation's goals.
- Approve the trade-offs made between security, usability of systems, and cost, whilst maintaining accountability for cybersecurity and resilience in your organisation.

What should your organisation do?

Ensure risk management practices for cybersecurity are in line with the risk profile of your organisation

- Define your organisation's cybersecurity risk management practices and determine the risk appetite and tolerance in relation to cybersecurity.
- Integrate cybersecurity risks into overall risk management in your organisation and establish a cybersecurity risk dashboard monitoring and reporting process to ensure cybersecurity risks are regularly reported to the Board and top management.
- Understand your business environment and the impact of cybersecurity threats to your business, and the corresponding cybersecurity risks. Develop cybersecurity risk metrics to monitor areas within your organisation with high risk exposure.

What do good cybersecurity practices look like?

Guiding Questions and Statements for Board Members[2]

Q1
As a Board member, do you understand how cybersecurity impacts your organisation?

- Do you understand how cybersecurity could impact your organisation? Are you equipped with the relevant expertise to understand the potential impact and risks arising from cybersecurity threats?
- How do you stay updated and refreshed on cybersecurity threats and trends in the industry? E.g. business publications on cybersecurity and risk, cybersecurity awareness workshops, consulting other Board members with cybersecurity expertise.

Q2
How does the Board get involved in governance and oversight of cybersecurity?

- Who is responsible for the governance and oversight of cybersecurity? Are C-suite leaders briefed about their roles and responsibilities on cybersecurity matters?
- Does the Board actively participate in discussions on cybersecurity matters?
- Does the Board get involved in decisions on the cybersecurity risk appetite of your organisation?
- Does the Board make trade-off decisions to ensure your organisation's cybersecurity practices commensurate with its risk profile?
- Has your organisation established a cybersecurity strategy? Is your cybersecurity strategy aligned with your business goals while taking into consideration current and future cyber risks and threats?
- What are the "crown jewels" of your organisation, and how are they protected?
- How is the Board involved when cybersecurity incidents occur? Are there channels/forums in place for the reporting of cybersecurity matters to the Board, or do they fit into another reporting process? (e.g. Board Risk Committee)

[2] The Board oversees strategy, major investments, and any important decisions in the company – they are held accountable.

Guiding Questions and Statements for C-suites[3]

Q1
Who is responsible for cybersecurity matters in your organisation?

- Is there a clear owner of cybersecurity with the appropriate knowledge, reporting capabilities, expertise, and authority to discharge their responsibilities effectively? This could be a person or a function. (e.g. IT team, CISO office)
- Are there channels/forums in place which focus on cybersecurity matters? (e.g. Cybersecurity Steering Committee, Risk Management Committee)

Q2
Does your organisation invest in sufficient resources to operationalise your organisation's cybersecurity strategy?

- This should include the following:
  - People – Developing competency and capability of employees (e.g. hiring, engaging external expertise, training)
  - Process – Implementing cybersecurity (e.g. risk management, data security)
  - Technology – Investing in technological capability (e.g. antivirus, malware protection, security monitoring tools)
- Does your organisation monitor security controls for effectiveness and performance against cybersecurity objectives?
- Are your employees briefed on their roles and responsibilities regarding cybersecurity?

Q3
How does your organisation minimise cybersecurity risks?

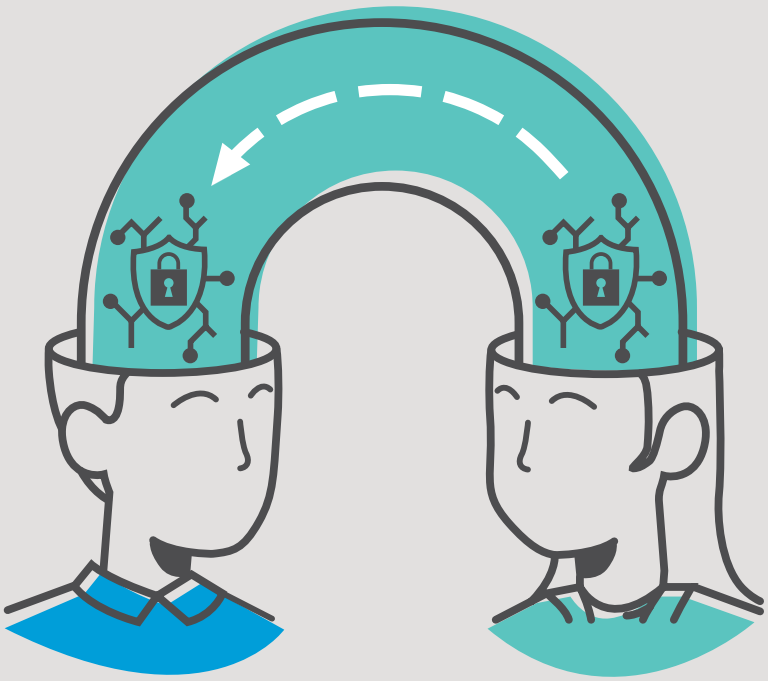
- Has your organisation established a cybersecurity risk appetite?
- Has a risk assessment been conducted to assess the current cybersecurity risk posture of your organisation?
- With the current cybersecurity risk posture, what are the possible business impacts to your organisation?
- What is the plan to address the identified cybersecurity risks?
- What are the competencies and resources your organisation needs to manage the cybersecurity risks identified?

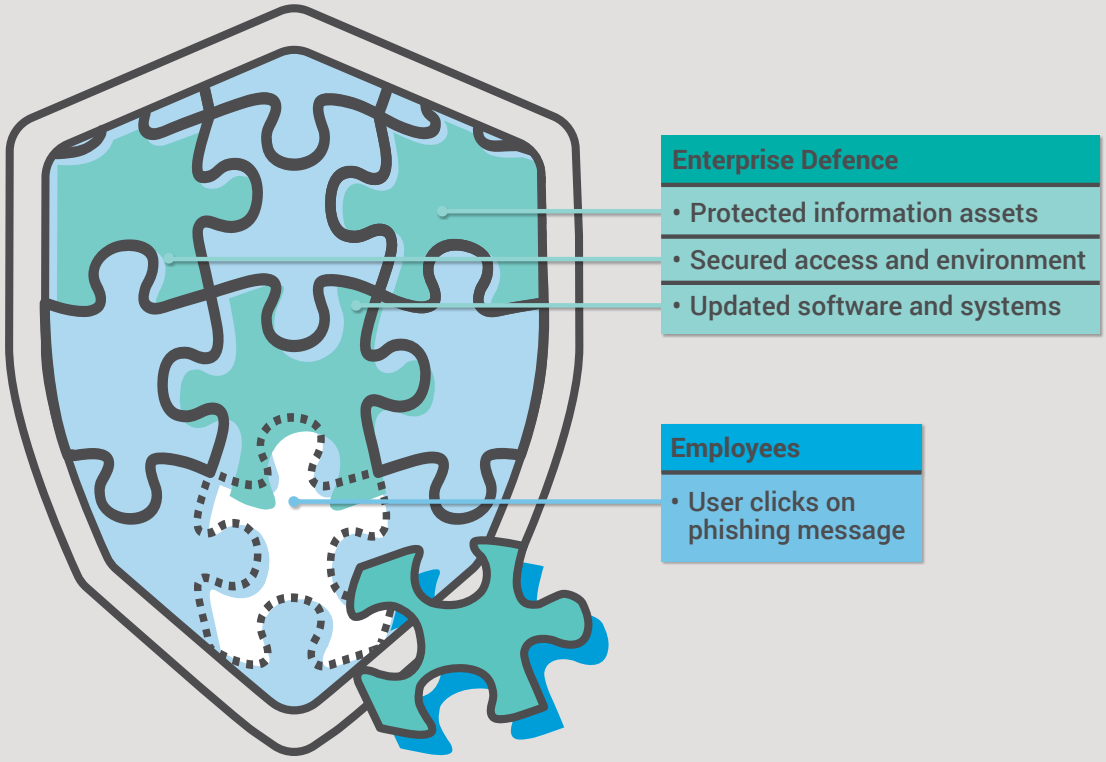
[3] The C-suite is responsible for key functional areas in the company and carries out the actual work of running the company.

Educate Your Employees on Cybersecurity

Why is this important?

One of the biggest threats to cybersecurity in any organisation comes from its employees, whose actions may inadvertently result in a cybersecurity incident in your organisation. Organisations can reduce this risk by building a culture of cybersecurity, so employees are aware of potential cybersecurity issues and can align their behaviour and working procedures to mitigate the risks. This, in turn, enables the employees to be your organisation's first line of defence.





What should you, the enterprise leader, do?

Lead by example and champion cybersecurity within your organisation

- Cybersecurity awareness needs to start from the top, and the Board and top management should set the tone to drive a cybersecurity culture within your organisation.
- Recognise that as drivers of the strategic direction of your organisation, the Board and top management may be the target of cyber attacks, because of your access to valuable assets in your organisation, or position of influence in your organisation.
- The Board and top management should keep abreast of cybersecurity threats and trends in the industry, so that you have the appropriate knowledge and skills to oversee and make cybersecurity related decisions.

Ensure investment is in place to cyber train employees and to raise their cybersecurity awareness

- Top management should support cyber training and awareness programmes in your organisation and ensure sufficient budget and resources are available to implement the programmes in a sustainable way.

What should your organisation do?

Drive cybersecurity as a top-down approach/cultivate a cybersecurity culture

- Instill the message that every employee has a role to play in keeping your organisation safe, and the responsibility is not limited to the IT/security teams. Employees should be aware that they are your organisation's first line of defence.
- Equip employees with cybersecurity knowledge through a cybersecurity awareness training programme. As this knowledge needs to be refreshed, ensure there is a process for re-training to facilitate knowledge retention through frequent message recall.
- Empower employees to raise or report potential cybersecurity incidents or concerns so that they help to serve as the "eyes" and "ears" within your organisation.

What do good cybersecurity practices look like?

Guiding Questions and Statements for Board Members

Q1
Do the Board and top management lead by example and champion cybersecurity in your organisation?

- Do you practise good cyber hygiene such as using strong passphrases, installing the latest security patches, and using anti-virus?
- Do you speak openly and positively to inspire employees to take your organisation's cybersecurity seriously?
- Do you ensure you keep abreast of the following through cybersecurity awareness workshops or other measures:
  - Cybersecurity risks and how they might impact your organisation; and
  - Evolving cybersecurity trends and the cyber threat landscape.

Guiding Questions and Statements for C-suites

Q1
How does your organisation ensure your employees are aware of cybersecurity?

- Do you provide employees with adequate training to identify and respond to the latest cybersecurity threats?
- Is the training content kept up to date with the latest cybersecurity developments (e.g. cybersecurity trends and threats)? Does your training programme minimally include key topics — such as handling data and recognising signs of phishing[4] — for all employees, regardless of their job function or job role?
- Is there a process in place to refresh employees' knowledge and to facilitate message recall?
- How do you measure the success and value of the training programme? Some key indicators to consider include:
  - Level of attendance and participation for mandatory training; and
  - Use of metrics such as:
    - A decline in security incidents or violations
    - Percentage of employees completing training sessions
    - Number of employees with cybersecurity-related certifications

[4] Signs of phishing include use of urgent/threatening language, suspicious attachments in the message, and grammatical mistakes.

Guiding Questions and Statements for C-suites

Q2
What are the measures/processes in place to instill a cybersecurity mindset, and how does your organisation ensure joint responsibility and accountability for cybersecurity?

- Do your employees know their roles and responsibilities for cybersecurity matters? Are all employees aware that everyone has a role to play in cybersecurity, regardless of their function?
- Does your organisation recognise good cybersecurity practices and focus on the success (rather than failures) of such practices? E.g. focusing on the number of employees who successfully identified phishing emails, rather than the number of people falling prey?
- Are your employees able to recognise a security incident, and feel sufficiently empowered to report a cybersecurity incident?
- Are frequent topical messages, notifications, and advisories about cybersecurity published across your organisation? These might include messages and advisories about:
  - Good policy and practices on passphrases;
  - Phishing and cyber scams;
  - Protecting corporate devices and personal devices (used for work); and
  - Latest cybersecurity incidents.
- Is your cybersecurity training and awareness programme extended to third parties and/or in-sourced staff? Are the third parties and/or in-sourced staff aware of their roles and responsibilities in cybersecurity?
- Are there designated individuals in each business unit or department (e.g. one or more business owners or cybersecurity champions) to promote awareness messages and support behavioural change?

"Are all employees aware that everyone has a role to play in cybersecurity, regardless of their function?"

CASE STUDY #1

CASE STUDY #1:

Impact:

In 2017, a group of highly skilled hackers breached the database of a major healthcare provider and gained access to the personal information of over a million individuals.

Issue:

These hackers were able to access the database by sending phishing emails to the organisation's employees. One employee fell for the scam and inadvertently gave hackers the opportunity to exploit key vulnerabilities in the network. Further investigation showed that the victim lacked cybersecurity awareness to detect and report the incident on a timely basis. This enabled the hackers to stay in the network and exfiltrate data over a prolonged period of time.

Lesson Learnt:

Staff awareness on cybersecurity is critical to enhance the organisation's capacity and capability to prevent, detect, and respond to such cybersecurity incidents. As attackers constantly evolve their attack patterns, this needs to be a continuous process in the organisation. Enterprises need to put in place a cybersecurity awareness programme to reduce organisational risk. This would equip IT and security employees with sufficient knowledge to recognise the signs of a security incident in a real-world context and respond to and limit the effects of a security incident.

Protect Your Information Assets[5]

Why is this important?

Knowing the information assets involved in your daily business operations helps you plan for information security risk management, and to allocate resources for information protection more effectively. Additionally, putting in place protective security controls over your information assets can help to reduce the chance of data misuse, breaches and operational disruption which might adversely impact business reputation and customer trust.

[5] An information asset refers to anything that has value to an organisation, including hardware, software and data that support business operations.

What should you, the enterprise leader, do?

Establish and endorse an information asset management programme

- Identify the key roles involved in the asset management programme – these include roles for management and the relevant department or teams.
- Endorse and ensure the implementation of a data/asset classification policy to organise the information assets according to their **confidentiality**[6], **integrity**[7], and **availability**[8] as well as the criticality to the business operation.

[6] Preserving of authorised restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
[7] Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
[8] Ensuring timely and reliable access to and use of information.

What should your organisation do?

Identify what are your information assets

- Assess how critical information assets are, based on confidentiality, integrity, and availability. This is to identify the "crown jewels" which are crucial to the running of day-to-day business operations. Information assets containing customer information, personal identifiable data, or sensitive business information should be treated as critical information assets by default.

Implement security controls for protection of information assets

- Ensure security controls are in place to protect the information assets. The level of protection should be aligned to their classification.
- Ensure IT assets are properly managed throughout the stages of the entire lifecycle i.e. purchase, configuration, deployment, decommissioning, and disposal. Ensure all assets are properly tracked and monitored e.g. using an asset inventory.

Establish data backup strategy

- Ensure data backup has been performed according to the criticality of the data so that business operations can be resumed in the event of a business disruption.

Drive the importance of regular system/application updates and manage the risks of using outdated systems and applications

- Ensure system updates have been conducted in a timely manner to reduce exposure to cybersecurity risks. Regular patching of your systems with the latest security updates can protect your systems from vulnerabilities which could lead to potential cyber attacks.
- Avoid using outdated systems and applications, as these systems are usually at their "End-Of-Life" or "End-Of-Support", which makes them vulnerable to new cyber attacks.

What do good cybersecurity practices look like?

Guiding Questions and Statements for Board Members

Q1
Do you know what are the "crown jewels" in your organisation?

- Do you know what are the critical information assets in your organisation, and what are the cybersecurity threats and risks associated with them?
- Have you considered the impact to your organisation in the event of a cyber attack? Do you know the steps to be taken in the event of a cyber attack (e.g. Distributed Denial of Service (DDoS) attack[9], phishing, ransomware[10])? Have you been briefed on your roles and responsibilities during a cyber attack?

Guiding Questions and Statements for C-suites

Q1
Do you know what are the "crown jewels" in your organisation?

- Do you have an asset management programme with an established asset classification criteria to identify the "crown jewels" in your organisation?
  - Do your asset classification criteria for identifying critical information assets take into consideration the confidentiality, integrity, and availability impact of the assets?
  - Do you know what are the risks and impact to your organisation if the information assets are compromised?
- Do you have delegated resources (internal or external) to manage the assets in your organisation?
  - Is there an asset classification plan in place to guide the resources in identifying and classifying assets that correspond to their criticality? Are the assets classified according to the risks and impact, should the assets ever be compromised?
  - Are these resources aware about the required security controls (such as implementing passphrase protection on files, limiting access, etc.) to be implemented and followed, to protect and handle classified assets?

[9] A Distributed Denial of Service (DDoS) attack is a malicious attempt to make a machine (i.e. server) or network resource unavailable to its intended users by flooding it with unnecessary traffic or to cause the application or service to become unavailable by sending it specially-crafted requests.
[10] Ransomware is a form of malware designed to encrypt files on a device; it targets victims by holding their data hostage and demanding ransoms from victims.

Guiding Questions and Statements for C-suites

Q2
Do you have a data backup strategy to resume your business operations in the event that the primary system is unavailable?

- Do you have a backup strategy and programme established? The backup strategy should clearly define the backup requirements (e.g. backup frequency) according to the criticality of the system and data.
- Do you have dedicated resources (internal or external) to perform the backup job to ensure critical information is backed up regularly?

Q3
Have you discussed with the IT team on the importance of regular system/application updates and to avoid the usage of outdated systems/applications?

- Are there any outdated systems/applications that are crucial to your business operations? Are there plans to upgrade and replace the outdated systems/applications to ensure business continuity?
- Do you have policy requirements to enforce timely software patching to be conducted on systems/applications to ensure that they are protected from the latest security vulnerabilities?

CASE STUDY #2:

Impact:

In 2020, a major bank was forced to close all its branches due to a ransomware attack which encrypted most of the bank's internal servers and employee workstations.

Issue:

It is believed that hackers were able to gain access to the bank's network through a malicious file opened by an employee. This created a backdoor for hackers to install the ransomware. Even though the ransomware encrypted internal servers and workstations, the bank had ensured that its internal networks were segregated. This significantly limited the spread of the ransomware, and ensured that the bank's website, online banking portal, mobile app, and ATMs were unaffected, and kept customer funds secure.

Lesson Learnt:

Organisations with important data are often key targets for ransomware attacks. Prevention is key to avoid falling victim to an attack. Organisations should take appropriate measures to secure their infrastructure and systems, and to ensure that their networks are properly segmented (e.g. between external and internal networks, guest and wireless networks) to minimise the impact of an attack. In addition, they should perform regular backups and keep these backups offline.

In the event of a ransomware attack, it is not recommended to pay the ransom as the payment does not guarantee the decryption and confidentiality of your data. It also encourages the hackers to continue their criminal activities and target more victims. The hackers may also see your organisation as a soft target and may strike again in the future.

Organisations may also refer to SingCERT's advisory on ransomware for more information.

Secure Your Access and Environment

Why is this important?

Implementing good cybersecurity measures can help secure your organisation and reduce the likelihood of a significant cybersecurity incident. You can secure your organisation by managing and controlling the access of every account and individual within your environment, including third parties. Additional cybersecurity measures such as usage of strong passphrases[11] and Multi-Factor Authentication (MFA)[12] can further secure your organisation's environment.

[11] Passphrases are similar to passwords, but they use a sequence of random words, rather than characters, e.g. putting five random words together. Strong passphrases should be at least twelve characters long, include upper case, lower case, numbers and/or special characters.

[12] MFA is the use of multiple keys to strengthen security. One key is typically your passphrase, and the other key could be an authorisation from an application on your mobile device or through biometrics (like fingerprints and face recognition).

What should you, the enterprise leader, do?

Establish and endorse a user access management programme for systems and data

- Having a user access management programme would ensure that only users with the assigned privileges and rights have access to the data or assets appropriate for their roles. The principles of "least privilege[13]" and "segregation of duties[14]" should be minimally applied when granting access to information assets.
- An established access management programme would ensure:
  - Consistent access rights and assigning of roles to users;
  - Provisioning of access; and
  - De-provisioning of access.

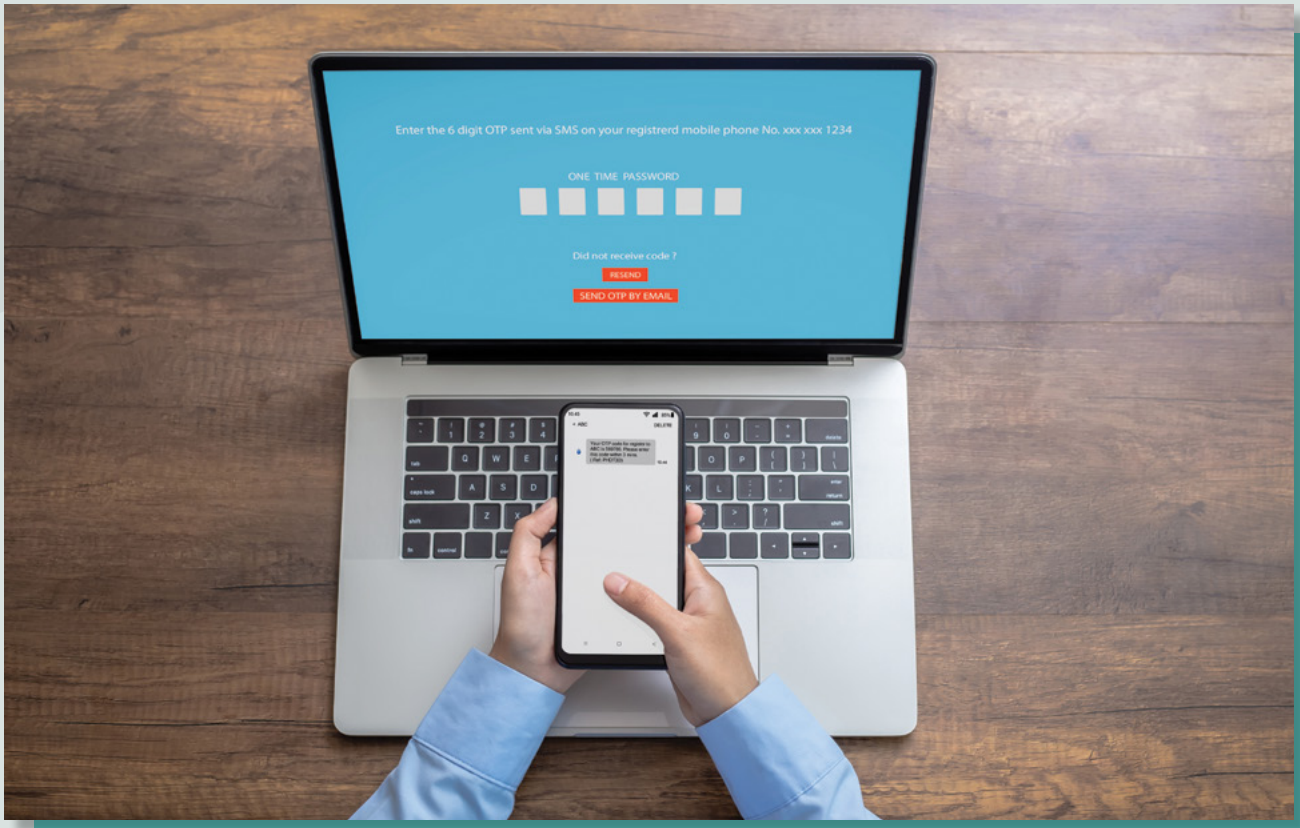
Establish and endorse a cyber third-party risk management programme

- Having a third-party risk management programme allows your organisation to assess and manage the risks posed by third parties, including vendors, products, and services. Regardless of the size of your organisation, a process should be established to review and assign a risk rating to each and every third-party arrangement.
- With such a risk management programme in place, your organisation can determine the following:
  - How the third party will be accessing, storing, or transmitting your organisation's data;
  - Whether it has a secure control environment that meets your organisation's expectations; and
  - Whether any specific security requirements should be negotiated into the contract's terms and conditions.

[13] The principle that users and programs should only have the necessary privileges to complete their tasks.
[14] The principle that no user should be given enough privileges to misuse the system on their own. For example, the person authorising a paycheck should not also be the one who can prepare them.

What should your organisation do?

Drive the importance of using strong passphrases and Multi-Factor Authentication (MFA)



- Cyber attacks occur frequently due to the use of weak and easy-to-guess passwords. Organisations should focus on strengthening their defences by using strong passphrases and MFA.
  - Passphrases are longer, more complex passcodes which makes them harder for hackers to crack. At the same time, passphrases can be easy to remember for users.
  - MFA helps to protect your organisation by adding an additional security layer which uses two or more factors to verify the user's claimed identity.

What do good cybersecurity practices look like?

Guiding Questions and Statements for Board Members

Q1
What are the threats and risks arising from third parties and the cybersecurity supply chain?

- Are you aware of how these threats and risks could affect your organisation?

Guiding Questions and Statements for C-suites

Q1
As an organisation, how are you managing privileged and user access?

- Have you established a User Access Management Policy and Framework to manage the user access to your systems? The Policy and Framework should clearly define the requirements, process, roles, and responsibilities regarding provisioning and de-provisioning of access for business users and privileged users.
- How are you tracking who has access to which network and information assets in your organisation?
- Do you maintain a list of privileged users in your organisation to ensure access is only granted to users who need it?
- What are the controls established for managing and monitoring access?

Q2
As an organisation, how are you managing your third-party/supplier risks?

- How are you monitoring your third parties/suppliers?
  - Do you maintain an inventory/list of all your third parties to ensure oversight over these arrangements?
  - Do you have ongoing monitoring of your third-party contracts?
  - How are you tracking the performance of your third parties against service level agreements (SLAs)?
  - How are you tracking the risks of your third parties against key risk indicators (KRIs)?
  - Are there any controls or defined notification requirements (e.g. stated in the contract) in place for third parties to inform your organisation in the event of any incidents on their end?

Guiding Questions and Statements for C-suites

Q3
As an organisation, what authentication methods are used to control access to systems and data?

- Has your organisation implemented any MFAs to ensure multiple authentication mechanisms? This should be strongly encouraged for access to high-value systems[15].
- Is your organisation using strong passphrases instead of passwords to make them harder to guess? Is your organisation teaching employees how to formulate strong yet easy-to-remember passphrases?

CASE STUDY #3

CASE STUDY #3:

Impact:

In 2020, a social media company was breached causing the hijacking of 130 accounts, some belonging to high-profile and influential people. These accounts were then used for a major financial scam.

Issue:

It is believed that the attack started from a culmination of a strikingly elaborate spear-phishing campaign that targeted the company employees. Using social engineering, the attacker managed to create a number of fake login pages which allowed him to successfully obtain login credentials to the company's secure systems, and from there to hijack the accounts.

Lesson Learnt:

Ensuring that access to your critical data is restricted to only the necessary individuals is basic and critical security control. Organisations need to make sure that this list stays current by performing regular access reviews and monitoring of the employee accounts. To protect against sophisticated social engineering attacks like spear-phishing, it's critical that strong authentication protocols are in place, like Multi-Factor Authentication (MFA).

[15] High-value systems are critical to your organisation in the way that any loss or disruption to the information they store, or any disruption to the systems, would have an adverse impact on your organisation's ability to conduct your business operations.

Ensure Your Business is Cyber Resilient

Why is this important?

In an increasingly volatile business environment, organisations have to prepare for cybersecurity incidents on the assumption that they will happen. For your organisation to be cyber resilient, it must have the ability to respond to and recover from a cyber attack with as little business disruption, regulatory conflict, and reputational impact as possible.

What should you, the enterprise leader, do?

Ensure you have a cybersecurity Incident Response Plan

- Having a robust Incident Response Plan ready before an incident can help organisations quickly and more effectively contain threats and recover.
- An Incident Response Plan that has been thought through and rehearsed beforehand is key to containing the incident and limiting the damage and disruption to business operations.

Ensure cybersecurity is integrated into your Business Continuity Plan (BCP)

- Having a BCP reflects your organisation's ability to protect and continue with critical business operations during a disruption, including but not limited to disruptions caused by cyber incidents.
- An effective BCP should ensure your organisation is equipped with the ability to prevent, respond to, and recover from various operational disruptions including but not limited to disruptions caused by cyber incidents.
- Business Impact Analysis (BIA) should be performed to identify critical business functions and the dependent people, process, and technology.

Ensure cybersecurity is integrated into your Disaster Recovery Strategy and Plan (DRP)

- Having a DRP reflects your organisation's ability to recover from catastrophic cyber or technology failures. This would help identify the preventative measures that can be put in to minimise system downtime.

Ensure cybersecurity is integrated into your Crisis Management Plan (CMP)

- Having a crisis management plan reflects your organisation's ability to manage escalation, communication, and coordination during a crisis, including but not limited to a crisis caused by cyber incidents.
- The CMP will provide a structure to guide stakeholders (e.g. Incident Response team, IT team, Communications team, Legal team) in understanding their crisis management roles and responsibilities in the event of a crisis caused by a cyber incident.

What should your organisation do?

Establish and endorse a cybersecurity Incident Response Plan

- Cybersecurity incidents can have a huge impact on an organisation in terms of cost and reputation. Having a cybersecurity Incident Response Plan allows your organisation to detect, respond to, and recover from cyber incidents in a timely manner.
- Due to the nature of these incidents happening at inopportune moments, it is crucial that everyone is clear of their roles and responsibilities during a cybersecurity incident.

Maintain oversight on regular BCP, DRP and CMP exercises

- Having a BCP, DRP and CMP in place is a good start. However, these plans should be tested regularly in exercises to ensure their efficiency, and to identify gaps in the plans. The plans can be further fine-tuned and improved on after addressing the gaps identified.
- Regular testing exercises also allow employees to understand the importance of the plan and employees' roles and responsibilities during a cyber incident.

What do good cybersecurity practices look like?

Guiding Questions and Statements for Board Members

Q1
As a Board member, are you aware of your roles and responsibilities during a cybersecurity crisis/incident?

- Are you equipped with the resources and training to perform your role during a cybersecurity crisis/incident?

Q2
As a Board member, do you know who will lead in the event of a cybersecurity crisis/incident, and who has the authority to make the necessary decisions?

- Is there a crisis management team established in your organisation, where roles and responsibilities are clearly designated?
- Has the crisis management team gone through any crisis management exercises to ensure your organisation is familiar with the crisis management plan?

Guiding Questions and Statements for C-suites

Q1
As an organisation, do you have a cybersecurity Incident Response Plan and how do you ensure it is effective for cyber incidents?

- A basic cybersecurity Incident Response Plan should minimally include the following:
  - Clear roles and responsibilities;
  - Escalation plan;
  - Communication protocols; and
  - Playbooks and scenarios.

Q2
As an organisation, do you have a Business Continuity Plan (BCP) which factors in cybersecurity, and how do you ensure it is effective in the event of a business disruption?

- A basic BCP should minimally include the following:
  - Clear roles and responsibilities;
  - Triggers for activation;
  - Stakeholders and contact details;
  - Recovery strategy; and
  - Various business disruption scenarios.

Q3
As an organisation, do you have a Disaster Recovery Plan (DRP) which factors in cybersecurity, and how do you ensure it is effective in the event of a disaster?

- A basic DRP should minimally include the following:
  - Alternative backup methods;
  - Testing of backup and restoration processes; and
  - Various system breakdown scenarios.

Q4
As an organisation, do you have a Crisis Management Plan (CMP) which factors in cybersecurity, and how do you ensure it is effective in the event of a crisis?

- A basic CMP should minimally include the following:
  - Criteria to determine a crisis;
  - Crisis management team;
  - Communication protocols; and
  - Spokesperson.

CASE STUDY #4

CASE STUDY #4:

Impact:

In July 2021, a cyber attack disrupted a port and rail company's operations. The attacker took down a critical system that tracks containers' movements in the terminal. This led to massive delays and unreliability to the movement of goods.

Issue:

The attackers left a ransom note to the organisation, claiming they encrypted the organisation's files, including a terabyte of personal data, financial reports and other documents. There was a subsequent note instructing the organisation to visit a chat portal on the dark web for negotiations.

Lesson Learnt:

A common saying in the cybersecurity world is that it's not if, but when a cyber incident will occur. That said, all organisations should have plans such as a BCP, DRP, CMP and cybersecurity Incident Response Plan in place to quickly and efficiently get operations up and running again in case of a cyber incident. This may not only reduce the impact but also maintain the trust of their stakeholders and customers.

Contact Details

If you wish to find out more about Singapore's efforts in cybersecurity, please visit the following website or contact us:

Cyber Security Agency of Singapore

www.csa.gov.sg

contact@csa.gov.sg
for general enquiries/feedback

If you have any feedback on this publication, or wish to find out more about the SG Cyber Safe Programme, please visit the following programme page or contact us:

SG Cyber Safe Programme

www.csa.gov.sg/sgcybersafe

sgcybersafe@csa.gov.sg
for general enquiries/feedback

If you wish to report a cybersecurity incident, please contact:

SingCERT

www.csa.gov.sg/singcert


CSA
SINGAPORE


SG
CYBER
SAFE