SG CYBER SAFE

CYBERSECURITY TOOLKIT

FOR IT/CYBERSECURITY TEAMS

UPDATED: 29 MARCH 2022

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

As the key personnel overseeing IT in your organisation, **you play a critical role for your organisation to be cyber safe** as it goes digital.

Overview

Digitalisation has changed the way we work, learn, transact, and stay connected. Developments such as global pandemics have also 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 our exposure to cyber risks.

The benefits of digital transformation can be fully reaped when enterprises invest in cybersecurity. Cybersecurity is a critical enabler for businesses — and the personnel overseeing Information Technology (IT) functions in the organisation play a critical role to ensure cybersecurity becomes a competitive advantage, especially in industries where trust is critical 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 IT teams (or personnel overseeing IT functions) in Small and Medium Enterprises (SMEs), but can also serve as a reference for security teams in larger enterprises. It covers five fundamental areas that organisations are encouraged to consider, regardless of their size, to ensure cybersecurity is adequately addressed.

CYBERSECURITY GUIDANCE FOR IT TEAMS

Cultivate cybersecurity leadership in the organisation

Educate the employees on cybersecurity

Protect the business-critical information assets

Secure the access and environment

Ensure the business is cyber resilient

Each area in the toolkit addresses the following question:

What can you, the personnel overseeing IT/cybersecurity functions, do to enhance cybersecurity?

This section provides actionable advice for personnel overseeing IT functions in smaller enterprises to ensure appropriate measures are taken to enhance cybersecurity in the organisation.

In addition, a collection of templates is provided in the appendix for the IT team's reference.

Templates for personnel overseeing IT/cybersecurity functions

IT teams may refer to and adapt from these templates to put in place policies, processes, or guidelines to better manage cybersecurity in the organisation.

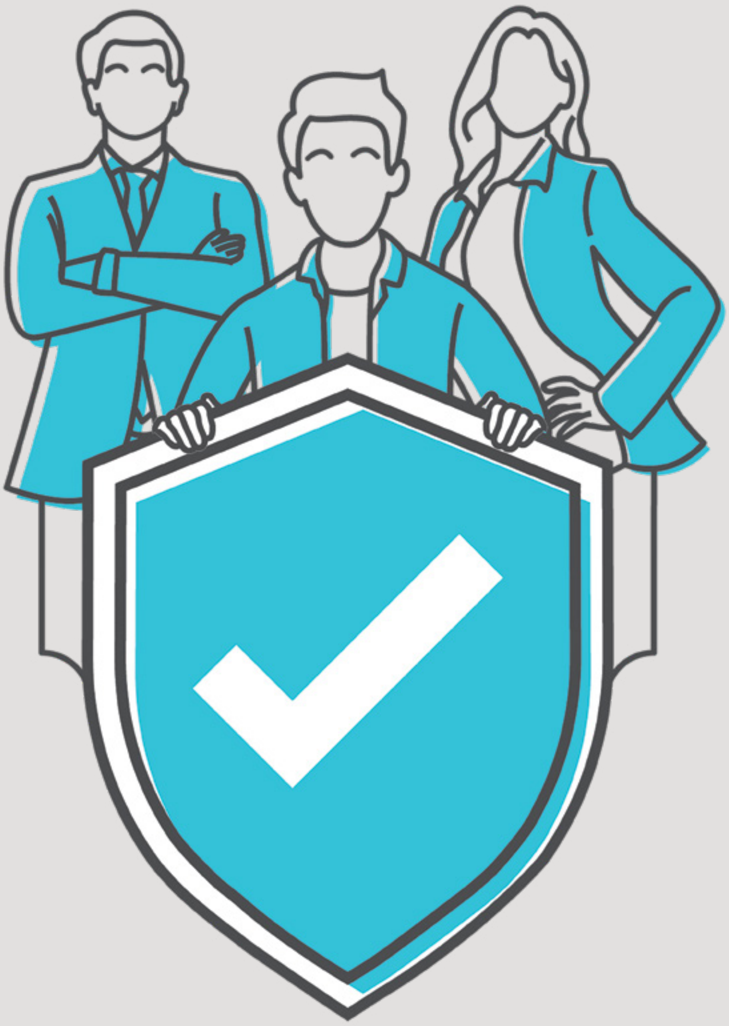
The templates in the appendix are downloadable in the form of a separate document so that IT teams may adapt them directly.

TIP: Applying for CSA's Cyber Essentials certification? Use the templates provided as a reference to prepare for certification.

Cultivate Cybersecurity Leadership in the Organisation

Why is this important?

The IT team plays a crucial role in getting the senior management informed and involved in cybersecurity. Studies show that conducting regular briefings on cyber risks is crucial to change the cybersecurity perception among senior management. This will support them in carrying out the right decisions and make sensible trade-offs between security, usability of systems, and cost to ensure that the organisation invests sufficiently in cybersecurity. By assisting to promote a proactive approach towards cybersecurity from the top down to the employees, you are also helping to create a cyber safe culture for the organisation.



What can you, the IT team, do to enhance cybersecurity?

Educate senior management on cybersecurity

- **Update your senior management on the cybersecurity threats and trends** — e.g. share articles on cybersecurity in business publications or media.
- **Inform your senior management on the cost implications of cybersecurity risks** — e.g. potential revenue loss and cost compensations when a company sustains reputational, regulatory, and/or legal damages. This helps your senior management understand that investing in cybersecurity helps to prevent incurring potential costs from cyber risks.
- **Propose how cybersecurity can be a competitive advantage and differentiator from competitors** — e.g. through reputation, or thought leadership in being secure and trusted. This helps to support the case for a budget to be allocated for cybersecurity.

Establish a cybersecurity strategy and develop a workplan with senior management to address security requirements

- **A cybersecurity strategy outlines the longer-term vision and provides directional guidance** of the organisation's intention to move from its current state to where it wants to be in future in the context of cybersecurity.
- **The cybersecurity work plan[1] provides shorter-term specifics in the form of actionable steps and timeline** in alignment with the cybersecurity strategy. It should:
  - Be approved and supported by the senior management
  - Reflect the organisation's budget for cybersecurity resources
  - Include roles and responsibilities of the employees
  - Have a realistic timeline for each actionable item

[1] See Appendix 1 — Template for Cybersecurity Work Plan

Cybersecurity Work Plan

- It should include:

Cultivating cybersecurity leadership	Update the senior management regularly on cybersecurity threats and trends, so that they are aware of the cybersecurity investments required.
Educating employees on cybersecurity	Lead by example, instil a cybersecurity mindset, and ensure the employees have sufficient knowledge and awareness on cybersecurity to perform their roles.
Protecting business-critical information assets	Manage and mitigate the risk of information assets in the organisation by putting in place cybersecurity initiatives and measures to minimise the damage and impact of cyber threats.
Securing the access and environment	Manage, control, and secure the access of every account and individual on the organisation's information assets within the environment.
Ensuring the business is cyber resilient	Establish plans incorporated with cybersecurity to respond, recover, and minimise the impact from an incident or disruptions as a result of a cyber attack.

- Discuss with your senior management the **trade-offs between security, usability of systems, and cost**, whilst maintaining accountability for cybersecurity and resilience when developing the work plan.
- Upon approval of the cybersecurity work plan, **implement, monitor the effectiveness, and review the security measures and controls** in place to meet the organisation's objectives.

Perform cybersecurity risk assessment and carry out the appropriate risk response strategy

- **A cybersecurity risk assessment[2] and management[3] helps the organisation to quantify and/or qualify the risks** it faces, and **assess the impact on the organisation**.
- Through cybersecurity risk assessment and management, the organisation:
  - Assesses if its existing cybersecurity measures are sufficient to mitigate its risks to an acceptable level
  - Identifies gaps which helps it to improve its cybersecurity against potential cyber threats and risks
- The organisation should **assign a risk owner to be accountable and responsible** for overseeing the risk treatment, to be completed within a reasonable due date.

Establish roles and responsibilities for senior management on cybersecurity

- **Senior management to promote good cybersecurity** — Encourage employees to take joint responsibility of and accountability towards cybersecurity with actionable examples, e.g. be vigilant and report any system abnormalities or suspected compromises to the IT team promptly.
- **Senior management to lead by example as cybersecurity champions** — e.g. show up-to-date knowledge on cybersecurity, and support initiatives to promote good cybersecurity practices within the organisation.
- **Senior management to support and approve cybersecurity policies, processes, and procedures** — provides clear direction for employees to follow, and their roles and responsibilities in cybersecurity in the organisation.
- **Report key cybersecurity risks or incidents to senior management** — Involve them in discussions and in making key decisions on cybersecurity in senior management meetings.

[2] See Appendix 2 — Template for Cybersecurity Risk Assessment
[3] See Appendix 3 — Template for Cybersecurity Risk Management

Educate the Employees on Cybersecurity

Why is this important?

One of the biggest threats to cybersecurity in any organisation comes from its employees, especially if they are not sufficiently trained in and aware of cybersecurity. Cyber attackers often take advantage of this and use social engineering[4] tactics to trick employees into giving up sensitive information like login credentials, or to download malicious software that could infect the rest of the organisation's systems.

In particular, business owners and senior management may potentially be targeted due to the nature of their work or roles (e.g. seniority in the organisation), where they could be making quick decisions with potentially major impact, and typically on the move. This makes them more prone to connecting to unsecured networks and opening phishing emails.

An organisation can reduce this risk by building a culture of cybersecurity and having employees who are sufficiently trained as the first line of defence. They both work hand in hand where a strong cybersecurity culture in the organisation would continuously ensure employees are aware of potential cybersecurity threats around them, so they know how to align their behaviour, and mitigate the risks.

[4] Social engineering refers to the "psychological manipulation of people into performing actions or divulging confidential information". Social engineering attacks often exploit human behaviour and are not always technological in nature. This can be done through either digital or non-digital means. Phishing is one of the most common forms of social engineering.

TIP: Applying for CSA's Cyber Essentials certification? This section addresses the measure "ASSET → People" in CSA's Cyber Essentials mark.

What can you, the IT team, do to enhance cybersecurity?

Instil a cybersecurity mindset in employees and ensure that they are aware of their roles and responsibilities in cybersecurity

- **Understand how employees could be a weak link** in the organisation and ensure that senior management understands the risks posed by employees.
- **Communicate to employees that they play an important role in the cybersecurity of the organisation** — Encourage them to act as the organisation's first line of defence against cyber attacks through their day-to-day actions.

Develop and establish cybersecurity policies and/or procedures for employees

- **Develop and establish cybersecurity policies and/or procedures to establish good cyber hygiene practices** in the day-to-day operations of the organisation. The policies[5] should minimally cover the following:
  - Asset inventory and management[6]
  - Data inventory, classification and management[7]
  - Account inventory, and access control and authentication[8]
  - Configuration management[9]
  - Software patch management[10]
  - Data backup[11]
  - Incident response[12]
- **Communicate cybersecurity policies and/or procedures to employees to drive awareness** — Make them freely available within the organisation and in different forms, e.g. formal policies posted on the organisation's intranet, posters in common areas in the organisation, regular email broadcasts, and screen savers on employees' computers.
- **Obtain employees' acknowledgement of cybersecurity policies and/or procedures** — For new hires, this can be incorporated into their onboarding process when they join the organisation, or in the orientation programme.

[5] Or guidelines, in the context of smaller enterprises

[6] See Appendix 4 — Template for Asset Inventory (Hardware), Appendix 5 — Template for Asset Inventory (Software), Appendix 6 — Template for Asset Management

[7] See Appendix 7 — Template for Asset Inventory (Data), Appendix 8 — Template for Data Management, Appendix 9 — Template for Data Classification

[8] See Appendix 10 — Template for Account Inventory, Appendix 11 — Template for Access Control, Appendix 12 — Template for Passphrase, Appendix 13 — Guidance on Strong Passphrases

[9] See Appendix 14 — Template for Configuration Management

[10] See Appendix 15 — Template for Software Patch Management

[11] See Appendix 16 — Template for Data Backup

[12] See Appendix 17 — Template for Incident Response (including data breach)

Establish cybersecurity awareness and training programmes

- **Establish cybersecurity awareness and training programmes for employees** in partnership with relevant corporate divisions, e.g. Human Resource (HR).
- **Equip employees with relevant and up-to-date knowledge** to protect the organisation and themselves from cybersecurity threats and prevent breaches, e.g. through self-learning materials or external training providers.
- **Extend cybersecurity awareness initiatives to third parties** that the organisation works with, where relevant.
- **Ensure the training content is relevant to the organisation** – the training content should also be differentiated to cater to employees in various roles and with different risk profiles.

TIP: Refer to the "Cybersecurity Toolkit for Employees" published by CSA for guidance on key topics to include.

- **Facilitate employee message recall** as people may start forgetting what they have learnt after about six months[13].
  - Have regular refreshers of the cybersecurity awareness training, e.g. at least once a year. An annual refresher also allows the content to take reference from yearly threat landscape reports[14]
  - Disseminate security awareness emails or newsletters to employees regularly
  - Place physical collaterals on cybersecurity awareness in common places in the work environment
- **Develop metrics as indicators of effectiveness** — e.g. employee completion rate or assessment scores against trends observed on the number of security incidents and related breaches.
- **Conduct a phishing exercise to simulate a realistic email phishing attempt** on all employees, if resources permit — this educates those who have clicked on the link, and also encourages them to report suspicious emails to the IT team.

Establish a cybersecurity champion programme

- **Identify cybersecurity champions from different roles, teams, and departments** across the organisation to engage and encourage employees on cybersecurity, as well as share the latest security-related information.

[13] Research from industry, e.g. Advanced Computing Systems Association (Usenix)
[14] Organisations may also refer to the annual Singapore Cyber Landscape published by CSA.

Take a human-centric approach to cybersecurity

- Traditionally, technology takes a central focus in cybersecurity. However, increasingly, there has been a shift towards taking a human-centric approach to cybersecurity, which **applies knowledge of how humans behave into more effective cybersecurity implementation**.

Example 1

Long and complex passwords are stronger but difficult for people to remember. As a result, people may resort to unsafe cybersecurity practices, such as reusing passwords for multiple accounts or writing them down. IT teams can consider providing guidance to keep passwords robust whilst being easier to remember, e.g. using passphrases made up of a few random words put together which are usually long and secure but still relatively easy to remember.

Example 2

Social proof refers to how humans tend to follow the actions of their peers, or the majority. IT teams can use this to encourage cyber safe practices in the organisation. For example, to mitigate phishing, when encouraging employees not to click on email attachments from unknown sources, use messaging which highlights how the majority follows cybersecurity best practices. E.g. “90% of your colleagues do not click on email attachments sent from unknown sources”.

Example 3

Habituation refers to how humans exhibit a decrease in behavioural response after repeated stimulation. IT teams can use this to encourage cyber safe practices in the organisation. For example, when software updates are regularly delivered to end-users, habituation may set in and end-users may defer the installation of the patches. One solution could be visually changing the presentation of the “software update” alert to ensure it catches employees’ attention.

Protect the Business-Critical Information Assets

Why is this important?

Information assets consist of hardware, software, and data connected to the organisation’s infrastructure, physically and virtually, that are of value and essential to support the day-to-day business operations. It is important for organisations to first identify the assets they have in their environment before implementing controls to protect them.

Identifying information assets within the organisation allows the planning of information security management programs, and budgets to allocate resources such as having dedicated security personnel and security controls for safeguarding, monitoring, backup, and recovery of these assets. These would help to reduce the likelihood of potential cybersecurity threats and lessen the risk of data misuse and breaches in the organisation.

TIP: Applying for CSA's Cyber Essentials certification?
This section addresses the measures "ASSET → Hardware and software" and "ASSET → Data" in CSA's Cyber Essentials mark.

What can you, the IT team, do to enhance cybersecurity?

Develop, establish, and maintain an asset inventory of hardware and software

- **Identify the essential and critical hardware and software assets** in the organisation[15] needed to keep the day-to-day operations running.
- The assets should also include:
  - Company-issued mobile devices and IoT devices used within the organisation
  - Cloud infrastructure and services
- **Develop, establish, and maintain an up-to-date information asset inventory** to keep track of the hardware and software in the organisation[16].
- The asset inventory list should include the key fields to capture the appropriate attributes for hardware[17] and software[18].

[15] This can be done manually, or through asset discovery tools.
[16] This can be done using spreadsheets or asset management software.
[17] See Appendix 4 — Template for Asset Inventory (Hardware)
[18] See Appendix 5 — Template for Asset Inventory (Software)

Develop, establish, and maintain an asset inventory of data

- **Identify sensitive and business-critical data**[19] within the organisation – consider the impact of the loss and unauthorised disclosure of such data, including personal data, e.g. customers' phone number, home address, etc.
- **Classify all identified data assets**[20] based on their sensitivity level and impact of loss to the organisation – typical categories include "Restricted", "Confidential", "Public", and "Internal".
- **Develop, establish, and maintain an up-to-date information data asset inventory** to keep track of the business-critical data in the organisation.
- The asset inventory list should include the key fields to capture the appropriate attributes for data assets[21].

[19] This includes confidential and/or sensitive data, including personal data. Examples include data within the enterprise such as product, staff and/or financial data that is vital to the operation of the enterprise, and where exposing them could lead to potential financial losses and/or legal issues.

[20] See Appendix 9 — Template for Data Classification

[21] See Appendix 7 — Template for Asset Inventory (Data)

Develop, establish, and implement policies on management of hardware and software assets

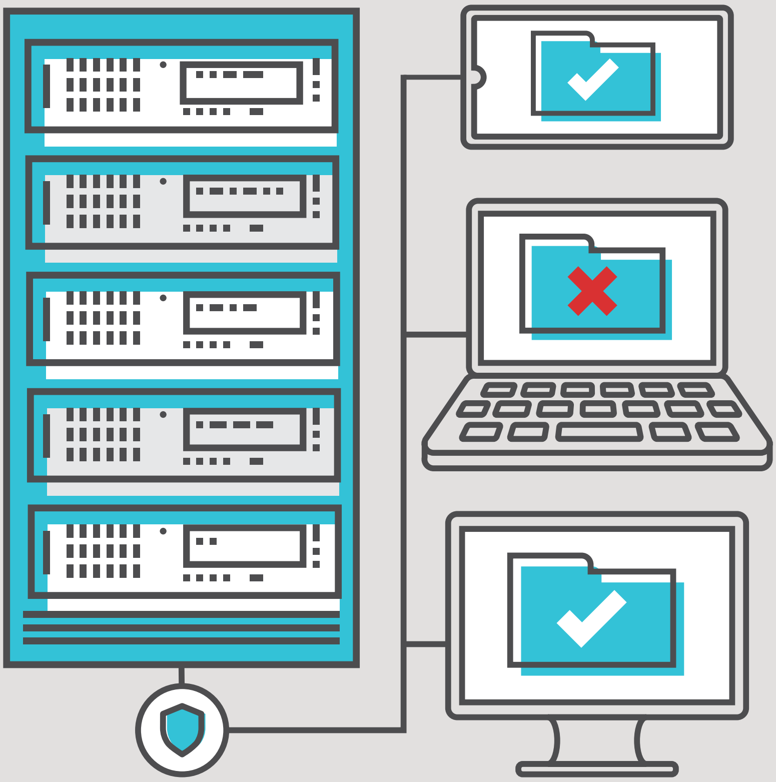
- **Establish and implement a policy on asset management**[22] including:
  - Authorising, onboarding and tracking new assets
  - Reviewing and updating asset inventory
  - Managing and monitoring assets that have reached End-of-Service or Support (EOS)
  - Carrying out secure disposal of assets
- **Review the hardware and software asset inventory list regularly**[23] so that assets movement and total assets count are captured accurately and are up to date.
- **Replace hardware and software assets that are unauthorised or have reached their End-of-Support (EOS) or End-of-Life (EOL)[24] date**. If the organisation continues to use unsupported assets, do assess the associated risks, seek approval from senior management, and monitor the assets until they can be replaced.
- **Validate new hardware and software during onboarding** to ensure that they come from official or trusted sources. Anti-malware scans should also be conducted to ensure that they are safe to be used.
- **Establish and implement a policy on the acceptable usage of hardware and software**[25] for employees to protect against possible cyber threats such as eavesdropping on and interception of business-critical data.
- **Detect the use of shadow IT**[26] — They should be assessed immediately to ensure that they do not raise any cybersecurity risks or compatibility issues to the organisation. The identified assets should also go through the formal onboarding and approval process before further use.
- **Dispose of the EOS/faulty hardware assets securely** — Ensure that the stored data is unrecoverable[27].

[22] See Appendix 6 — Template for Asset Management
[23] Typically on a bi-annual basis
[24] EOS or EOL refers to the date when the product vendor or manufacturer announces that it will stop providing updates or maintenance for the product.
[25] See Appendix 20 — Template for IT Acceptable Use Policy
[26] Shadow IT refers to IT systems such as applications and devices that are being used and managed in the organisation without the IT team's knowledge and approval.
[27] E.g. destroy the hard disk physically or engage a disk-shredding service

Develop, establish, and implement policies on management of data assets

- **Develop and implement a policy on data classification and handling**[28] for employees to understand the security requirements and guidelines to handle data assets.
- **Review the data asset inventory list regularly**[29] or whenever there are any changes in the list to ensure that the data flow is captured accurately and up to date.
- **Establish and implement a process to protect the confidentiality of business-critical data** to ensure they are not easily accessible and visible in plain text to unauthorised parties[30]. It should also be communicated to the employees so that they are aware of the organisation's practices.
- **Establish and implement security measures to prevent business-critical data leakage**[31]. They act as a safety net against insider threats in the event of human error or when the employees do not follow the established process in place.
- **Retain confidential and/or sensitive data based on a need-to basis and set a retention date** for them. Reviews should be carried out at least annually to delete data that has exceeded its retention date and is no longer required in the organisation. If the data is still required, the retention date should be extended accordingly.
- **Delete all the confidential and/or sensitive data in hardware assets before disposal**[32].
- **Set up a data breach reporting channel or hotline**. Communicate to the employees to report any suspicious emails or attachments that could result in a data breach or compromise so that investigations can be carried out immediately.

[28] See Appendix 8 — Template for Data Management
[29] Typically on a bi-annual basis
[30] E.g. use of password protection, encryption of data at rest and/or in transit
[31] E.g. disable USB ports, enable data loss prevention features in the mail server
[32] E.g. encrypting the hard disk before reformatting and overwriting it, and shredding paper-based media containing confidential and/or sensitive data



Secure the Access and Environment

Why is this important?

Taking steps to secure the organisation's access and environment helps to prevent unauthorised parties from accessing information assets that could result in the loss and disclosure of confidential and/or sensitive data, such as customers' data. Failure to secure the access and environment has also contributed to insider threat being the leading cause of cyber attacks when employees or third parties are given a higher level of permission or privilege than they actually require. This has resulted in either accidental or intentional data breaches and cyber attacks.

Thus, it is important for organisations to adopt security measures such as setting a strong passphrase, establishing multi-factor authentication, and having physical access control to secure their access and environment to protect against the risks of information asset breaches.

TIP: Applying for CSA's Cyber Essentials certification?
This section addresses the measures “SECURE/PROTECT → Virus and Malware Protection” in CSA’s Cyber Essentials mark.

What can you, the IT team, do to enhance cybersecurity?

Install, run, and configure anti-malware solutions to protect the hardware and software assets from viruses and malware in the environment

- **Install and run anti-malware solutions** on endpoint devices[33], mobile[34] and where feasible, IoT devices[35] to prevent viruses and malware from accessing and infecting the environment.
- **Malware protection in the cloud environment** — As enterprises shift their workloads to cloud services, potentially large volumes of business-critical data could be stored in the cloud. Under the cloud shared responsibility model, it is the cloud customers’ responsibility to protect their own data.
- **Virus and malware scans should be automatically run** on all accessed files[36] and external sources such as USB drives.
- **Enable auto-update of signature files** to ensure they are receiving the latest virus and malware signature files.
- **Protect against malware via a web browser/email client** with:
  - **Anti-phishing tools to detect and alert employees** of suspected phishing websites and/or phishing email attempts before they fall for the social engineering attack
  - **Spam filtering tools** to detect and block unwanted, unsolicited and virus-infected emails and web popups
  - **Website filtering**[37] to blacklist and prevent browsers from loading known malicious websites
  - **Running only fully supported web browsers and email clients** with up-to-date security controls and features
  - **Disabling or removing web browser and email plug-ins/extensions/add-ons** that are not in use to reduce the threat attack surface and avenues for exploitation

[33] E.g. laptops, desktops, servers, and virtual environments
[34] Risks are higher when the security software has not been updated, or if the devices have been rooted/jailbroken.
[35] Compromised IoT devices have been known to launch botnet and DDoS attacks.
[36] Including files downloaded from the Internet through web browsers
[37] Website whitelisting can be the alternative, where employees can only visit the whitelisted sites.

Deploy, enable, and configure a firewall to protect hardware and software assets from malicious and/or unauthorised network traffic accessing the environment

- **Deploy, enable, and configure a firewall** on the network[38] and on endpoint devices, including mobile[39] and where feasible, IoT devices to prevent access of malicious and/or unauthorised network traffic.
- **Review and verify firewall configurations and access rules regularly**[40] and whenever there are any changes to the network diagram, network device or access rules so that they are up to date and effective in protecting the organisation's internet-facing assets against malicious threats.

[38] Monitor incoming and outgoing network traffic and filter malicious or unauthorised network traffic between the private network and public internet.
[39] Host-based firewalls protect endpoints from being used as the source of entry into the rest of the organisation network.
[40] Typically on an annual basis

TIP: Applying for CSA's Cyber Essentials certification? This section addresses the measures "SECURE/PROTECT → Access Control" in CSA's Cyber Essentials mark.

Develop, establish, and maintain an account inventory list to ensure employees are assigned with the right permission and access

- **Develop and establish an account management program** with policies[41] in place to maintain and manage the account inventory list[42] which captures the key fields for user, administrator, third-party, and service accounts.
- **Review the account inventory list[43] regularly** and whenever there are any changes to the account list, e.g. during employee onboarding and offboarding process or organisation restructuring.
- Develop an access control policy incorporating the following:
  - **Principle of least privilege** — Ensure users are given the right role with minimum access to carry out their work
  - **Separation of duties** — Ensure critical business functions are being divided among different employees to limit the power held, and to ensure that no individual has the authority to commit fraud or engage in unethical acts
- **Perform user access account management**, including:
  - Disabling dormant or inactive accounts — The accounts could have been forgotten, or be no longer in use
  - Disabling accounts that are no longer required, e.g. employees offboarding, or accounts that have exceeded the requested date
- Establish and implement a **process for granting or revoking access**.

[41] See Appendix 11 — Template for Access Control
[42] See Appendix 10 — Template for Account Inventory
[43] Typically on a quarterly basis

Manage third-party access control when engaging external vendors, products, or services

- **Maintain an inventory of outsourced service providers** and assess the risk of third parties including vendors, products, and services as part of the organisation's risk assessment:
  - Consider how data will be accessed, stored, and transmitted by third parties
  - Monitor whether service providers are processing data in a secure environment
  - Develop a Service Level Agreement (SLA)[44] and Key Risk Indicator (KRI)[45] with the service providers to address the services committed, remedies, penalties, and risk metrics
- **Manage the access of third parties and external vendors** to ensure they only have restricted access to perform their work. Conduct reviews more frequently to ensure timely revocation of their access to the organisation's environment.
- Require the third parties or external vendors who are working with sensitive information in the organisation to **sign a non-disclosure agreement form**[46].

[44] See Appendix 21 — Template for Service Level Agreement (SLA)
[45] See Appendix 22 — Template for Key Risk Indicator (KRI)
[46] See Appendix 14 — Template for Non-Disclosure Agreement

Develop and implement security measures to carry out access control

- **Enforce physical access control**[47] **on the employees and/or third parties** to ensure only authorised parties can access the organisation's IT assets and/or environment.
- Educate employees and/or third parties to **change their account password immediately in the event of any suspected compromise**, so that their accounts would not be used by any unauthorised parties.
- **Establish the use of a trusted password or passphrase manager** to suggest, store, and manage employees' passphrases.
  - This relieves employees from having to remember all the different passwords to the different accounts
  - Employees will need to ensure they use a secure master passphrase[48] to protect access to the software
- **Implement two-factor authentication (2FA)**[49,50] **for administrative access to critical systems**, such as an Internet-facing system containing business-critical data.
- **Monitor account access to detect and identify any abnormalities**[51] such as multiple failed logins within a short period of time, as well as logins during odd timings.
- **Disable and/or lock out accounts after multiple**[52] **failed login attempts** to deter unauthorised logins to the accounts.

[47] E.g. use of card access door lock to authenticate and authorise entry
[48] See Appendix 13 — Guidance on Strong Passphrases
[49] E.g. authenticator mobile application or one-time password (OTP) token
[50] The 3 main types of authentication include: (i) things you know (e.g. password or PIN), (ii) things you have (e.g. token), and (iii) things you are (e.g. biometrics).
[51] E.g. use of user behaviour analytics
[52] E.g. 10 failed logins

TIP: Applying for CSA's Cyber Essentials certification?
This section addresses the measures "SECURE/PROTECT → Secure Configuration" in CSA's Cyber Essentials mark.

Configure to use secure settings on the hardware and software assets in the environment

- **Implement secure configuration** on endpoint devices, mobile devices and IoT devices to minimise the attack surface of threats accessing the environment[53].
- On endpoint devices, **industry recommendations and standards on secure configuration** can be obtained from the Centre for Internet Security (CIS), or vendors.
- On mobile devices, **ensure mobile devices are not jail-broken or rooted** as this would disable some of the in-built security features; also download mobile applications only from official or trusted sources.
- On IoT devices, **segment the network** hosting the IoT devices from the rest of the enterprise network and enable security features.
- Cloud – Turn on **security logging and monitoring** for cloud visibility, e.g. history of API calls, change-tracking, and compliance.

[53] See Appendix 19 – Template for Change Management

- As part of the **secure configuration good practices**[54]:
  - **Enable logging[55] for software and hardware assets** to provide visibility on how the assets are running and identify issues such as system faults and failures
  - **Enable automatic session lock/log out** after a prolonged period of inactivity[56] for enterprise assets to ensure that it is not being hijacked by unauthorised parties. This includes user sessions on the laptop, server, non-mobile device, database, and administrator portal
  - **Update weak or default configurations before use**, e.g. changing of default password and configuring the anti-malware solution to perform a deep scan instead of a standard scan to ensure scans are being carried out thoroughly
  - **Upgrade insecure configurations and weak protocols[57]** to address the associated vulnerabilities
  - **Turn off features, services, or applications that are not in use**, as any additional services or features act as an attack vector and increase the surface areas for attackers to carry out their exploits
  - **Disable automatic connection to open networks and auto-run feature of non-essential programs** other than backup or anti-malware solutions. This would allow proper due diligence to be carried out in assessing the risk involved before connecting to the network or running the program

[54] See Appendix 15 — Template for Configuration Management
[55] E.g. system, events, security and debugging logs
[56] E.g. Five minutes
[57] E.g. using HTTPS over normal HTTP to encrypt data communication, and upgrading WEP to WPA2 to enhance the Wi-Fi security standards

TIP: Applying for CSA's Cyber Essentials certification?
This section addresses the measures "UPDATE → Software Updates" in CSA's Cyber Essentials mark.

Carry out regular application and system patching and/or updates on the hardware and software assets in the environment

- Plan to **patch and/or update the applications and systems**[58] in the organisation as soon as they are released to reduce possible exposure to cybersecurity threats and risks:
    - Prioritise critical or important patches and/or updates for operating systems and applications (e.g. security patches) and apply them as soon as possible to protect your systems from newly discovered zero-days
    - Enable automatic patches and/or updates where possible so that the latest patches and/or updates can be applied upon release
- **Remove or replace any outdated systems, applications and IoT devices** not receiving any software patches and/or updates for a prolonged period of time[59].

[58] See Appendix 15 — Template for Software Patch Management

[59] If they are EOL or EOS and are no longer receiving patches and/or updates from the product vendor or manufacturer, they are highly vulnerable to cyber attacks.

- **Carry out testing such as compatibility checks on software patches and/or updates on the testing environment**, verify that there are no adverse implications or failures before installing them to the production environment. This prevents any disruptions to other systems or applications that are tightly coupled which may be affected by the newly installed updates and/or patches.
- Ensure that **patches and/or updates for mobile devices are only downloaded from trusted sources**[60] to prevent downloading any rogue updates and/or patches that may be infected with malware.
- For cloud deployments, be aware of the **cloud customer's responsibility** to update and/or patch the guest operating systems and applications in the cloud. The Cloud Service Provider is responsible for patching and/or updating the infrastructure of the cloud.

[60] E.g. official app store from the manufacturer

TIP: Applying for CSA's Cyber Essentials certification?
This section addresses the measures "BACKUP → Back up essential data" in CSA's Cyber Essentials mark.

Establish a policy and develop a plan to back up essential data on the hardware and software assets in the environment

- Identify business-critical systems and those containing essential business information to determine what to back up.
- **Back up essential data in the environment** to ensure high recoverability in the event of any data loss or corruption.
- **Establish a data backup policy**[61] and develop a plan to define the backup requirements[62] according to the criticality of the system and data.
- **Automate the backup process** where possible to ensure that they are being performed at a desired frequency without the need for human intervention and to reduce any possible human errors.
- Backups should be carried out for:
  - **Business-critical systems and data on a regular basis**[63]
  - **Non-business-critical systems and data** with a lower backup frequency as compared to business-critical systems and data, to ensure that data can still be recovered when required
  - **Business-critical data in mobile and IoT devices** and transferred into an external storage location to protect against malware infection and the risk of being stolen
  - **Data stored in the cloud.** This is the responsibility of the organisation under the Shared Responsibility Model — back up cloud-based data in a hard disk drive, purchase the backup services by the cloud provider, or adopt a multi-cloud strategy

[61] See Appendix 17 — Template for Data Backup
[62] E.g. systems to perform backup, frequency, type, storage, and recovery testing
[63] Align the frequency to the business requirement, in terms of the amount of data (in days) the organisation can afford to lose in the event of a system disruption.

- Backups should be stored:
  - **Securely with physical security**[64] in place and protected from unauthorised access to prevent the backups from being stolen and damaged. The data should also be encrypted so that in the event of a loss of backup media, the data would be incomprehensible
  - **Offline and isolated from the operating environment and network**, if the malware transverses and spreads across the entire organisation's network
  - **Offsite and in a different location** where feasible to create geographical redundancy so that in the event of a natural disaster, the backup is retrievable and could still be recovered from the alternate site
  - **Offline and offsite for long-term backups**[65] that would not be carried out frequently in an external storage location and on a separate site
  - **Online for short-term backups**[66] that would be carried out more frequently
- **Test data backup and restoration regularly** to assess the backup plan and procedures in place to ensure business-critical systems data can be restored in a timely manner in an incident.

[64] E.g. physical locks, CCTV, security guards
[65] E.g. monthly or quarterly backups
[66] E.g. daily or weekly backups

Ensure the Business is Cyber Resilient

Why is this important?

In today's increasingly volatile business environment and expanding threat landscape, having just cybersecurity in place is not adequate. Organisations also need cyber resiliency in order to respond to cyber incidents and attacks which they are unable to detect or prevent, and recover their systems and data. This would greatly reduce the impact of business disruptions, regulatory conflict, and reputational loss.

In order to ensure that the business is cyber resilient, organisations should come up with an effective Business Continuity Plan and Disaster Recovery Plan to help them identify, protect, detect, respond to, and recover their critical assets.

TIP: Applying for CSA's Cyber Essentials certification?
This section addresses the measures "RESPOND → Incident Response" in CSA's Cyber Essentials mark.

What can you, the IT team, do to enhance cybersecurity?

Develop and implement a cybersecurity and data breach Incident Response Plan (IRP)

- **Develop and implement a cybersecurity and data breach Incident Response Plan (IRP)**[67].
- Conduct **post-incident reviews and incorporate learning points** and areas of improvement to strengthen and improve the IRP.
- **Communicate the IRP to employees** in the organisation so that they can be aware of their roles and responsibilities in carrying out the IRP.
- **Review and test out the IRP** at least annually to ensure the personnel involved are clear of their roles and familiar with what steps to perform.

[67] See Appendix 18 — Template for Incident Response (including data breach)

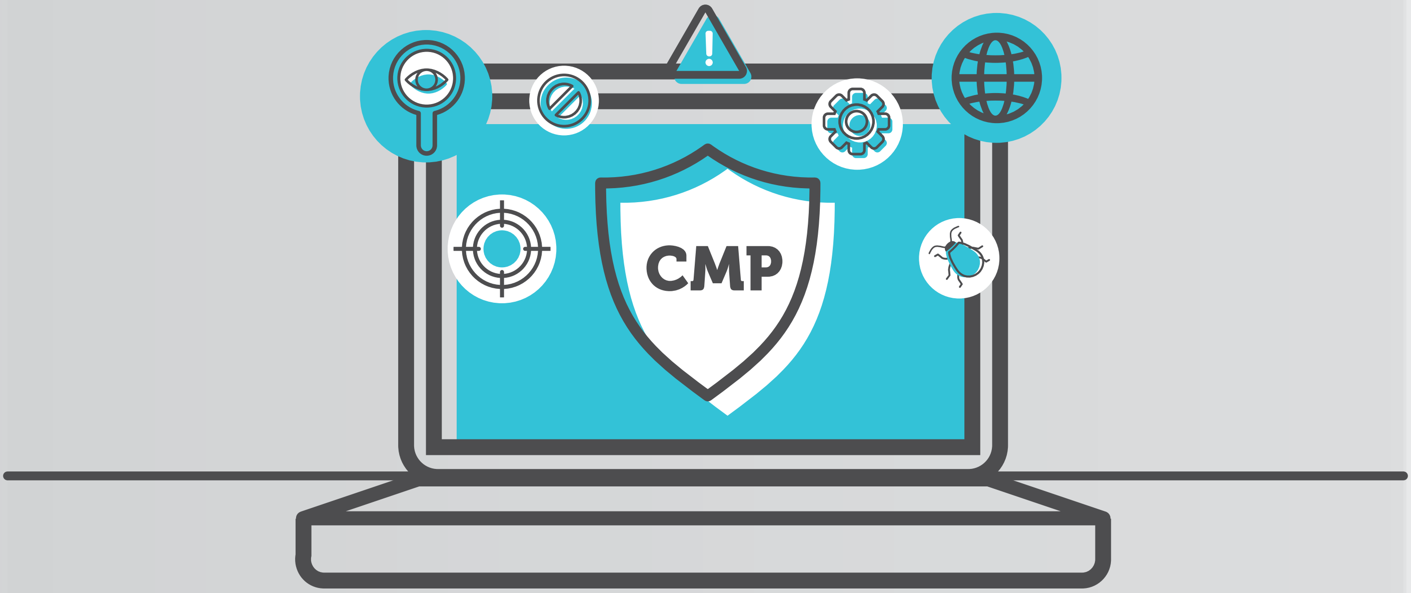
Keep up to date with and report cybersecurity incidents

- Visit the CSA SingCERT website to receive alerts and timely information on the latest security issues, vulnerabilities, and exploits to keep up to date with the cyber threat landscape and developments.
- Obtain advisories from the CSA SingCERT website for detailed information on high-impact cybersecurity threats in Singapore, as well as how to protect against them.
- Report any cybersecurity incidents based in Singapore to SingCERT.

Ensure the inclusion of cybersecurity in developing the organisation’s Business Continuity Plan (BCP)

- **Include cybersecurity into the organisation Business Impact Analysis (BIA)[68]** to identify the critical business functions, systems, data, and any other key dependencies on the potential impact of loss and damage should any cyber-related disruptions occur.
- Develop the maximum Recovery Time Objective (RTO)[69] of critical systems.
- **Include cybersecurity when developing and implementing a Business Continuity Plan (BCP)[70]** to reflect the organisation’s ability to protect, respond and recover the business operations during a cyber-related disruption. Cybersecurity should be integrated into the plan with the inclusion of plausible scenarios that could result in business disruptions, e.g. cyber attacks, data loss, and breaches.
- **Test and review the BCP regularly[71]** and whenever there are any significant changes to the plan. If a failover site is involved, the organisation should operate in the alternative site for an extended period of time[72] for a more realistic simulation.
- Monitor and evaluate the key events and actions taken to come up with areas of improvement.
- **Report to the senior management on the result of the BCP** so that they are kept aware of the impact and loss incurred to the organisation.

[68] See Appendix 23 — Template for Business Impact Analysis (BIA)
[69] The maximum duration that the critical systems should be recovered by in order to ensure minimal business impact
[70] See Appendix 24 — Template for Business Continuity Plan (BCP)
[71] Typically on an annual basis
[72] E.g. Three days



Ensure the inclusion of cybersecurity in developing the organisation's Disaster Recovery Plan (DRP)

- **Include cybersecurity when developing and implementing a Disaster Recovery Plan (DRP)**[73] to reflect the organisation's ability to recover from catastrophic cyber or technology failures to minimise downtime as a result of a cyber-related incident.
- **Test and review the DRP regularly**[74] and whenever there are any significant changes to the plan.

Ensure the inclusion of cybersecurity in developing the organisation's Crisis Management Plan (CMP)

- Escalate incidents to crisis[75] level whenever there is a high level of uncertainty, or potential that the core business of the organisation will be disrupted, and when it requires urgent or crucial decisions to be made.
- **Include cybersecurity when developing and implementing a Crisis Management Plan** (CMP)[76] to reflect the organisation's ability to manage escalation, communication, and coordination during a crisis. The plan also provides a structure to guide stakeholders in understanding their crisis management roles and responsibilities in the event of a crisis caused by cyber incidents.
- **Test and review the CMP regularly**[77] and whenever there are any significant changes to the plan.

[73] See Appendix 25 — Template for Disaster Recovery Plan (DRP)
[74] Typically on an annual basis
[75] The key difference between an incident and a crisis is that a crisis is typically more strategic and involves the senior management, focuses on communication, and has a huge impact on the organisation's reputation.
[76] See Appendix 26 — Template for Crisis Management Plan (CMP)
[77] Typically on an annual basis

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