BE SAFE ONLINE

HOW TO DEFEND YOUR BUSINESS AGAINST CYBER-ATTACKS

Be Safe Online

ISBN: 978-981-11-6122-3

Cyber Security Agency of Singapore
www.csa.gov.sg

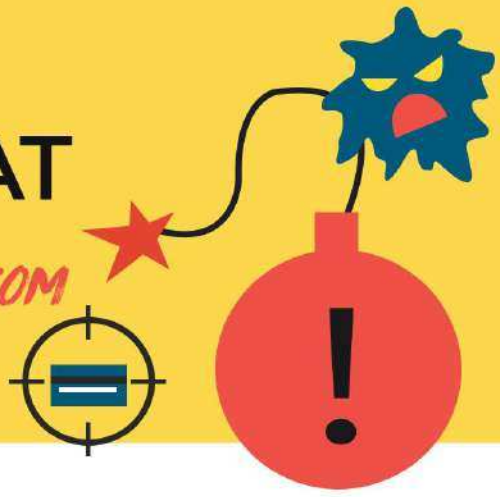
SingCERT hotline for incident reporting:
(+65) 6323 5052

SingCERT e-mail for incident reporting:
singcert@csa.gov.sg

DISCLAIMER

This publication provides a general guide to fundamental cybersecurity steps or considerations to get an organisation started on its cybersecurity journey. The contents herein have been written to aid understanding and are not an authoritative statement of the law or a substitute for legal or other professional advice. The Cyber Security Agency of Singapore shall not be held responsible for any inaccuracy, error or omission in this publication or liable for any damage or loss of any kind as a result of any use of or reliance on this publication.

THE CYBER THREAT LANDSCAPE



Be Safe Online is a handbook to help organisations enhance their cyber defence capabilities and digital risk management, so as to better protect themselves against the increasing frequency and sophistication of cyber-attacks.

A successful attack is when a threat exploits and overcomes a vulnerability presented by people, process or technology. In November 2017, ride-sharing company Uber[1] revealed that personal details of 380,000 people in Singapore, including names, e-mail addresses and mobile phone numbers, were lost to cyber-attackers. Small and medium enterprises (SMEs) have not been spared either. In March 2017, BH Global[2], a local marine lighting company, had observed that its firewall had been blocking malicious "beacon messages" or "call-back messages" successfully.

Increasingly, SMEs are being attacked and used as conduits to attack larger companies, organisations or even governments.

Cyber-attackers range from criminals who steal online identities or corporate information for financial gain, hackers who break into systems just to show off their skills, to even nation states.

Business risks arising from cyber incidents are wide ranging – from lawsuits and regulatory penalties due to theft of sensitive information, to loss of customer trust and damage to company reputations. Chief executives and senior managers can be blamed for serious cyber incidents. In late 2017, Uber's chief security officer was forced to resign[3] over his role in the company's severe 2016 data breach.

The most effective cyber defences will be those that concentrate resources on protecting their most valuable assets.

---

1. 380,000 Uber users hit in Singapore's largest data breach, December 16, 2017, The Straits Times
2. Hit by cyber attacks, some Singapore enterprises are fighting back with AI, March 14, 2017, techgoondu.com
3. Uber Chief Security Officer fired after massive data-breach cover up, December 2017, hotforsecurity.bitdefender.com

SIX CYBER DEFENCE ESSENTIALS

WHY CYBER DEFENCE?

"If you know the enemy and know yourself, you need not fear the result of a hundred battles" – Sun Tzu.

Behind every cyber threat is a person or persons, whether they are casual hackers or more sophisticated groups. As such, a purely compliance approach to cybersecurity will not be effective, as perpetrators keep up-to-date with the latest cybersecurity policies made available on the Internet to constantly find new ways to bypass security protections to gain entry into networks.

Hence, a cyber defence strategy needs to be nimble and comprehensive, which would begin with an assessment of the threats against an organisation. A simple starting point is to identify an organisation's key cyber assets, and the potential threats and risks to those assets. Thereafter, an organisation decides on the appropriate tools and controls to mitigate the risks to these assets.

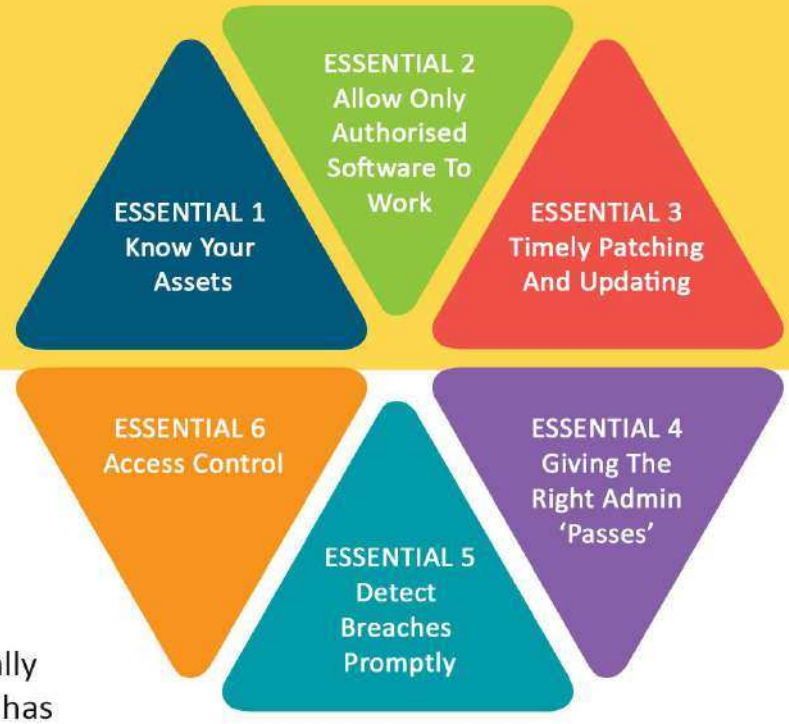
This approach aims to create a business environment that reduces soft-spots (vulnerabilities) in IT networks and infrastructure as much as possible. Through continuous vigilance and authentication safeguards, organisations can quickly detect, outwit cyber-attackers and create a safer and secure environment for businesses, employees and customers.

WHY THESE 6 ESSENTIALS?

"The whole is greater than the sum of its parts" – Aristotle.

The Cyber Security Agency of Singapore (CSA) advocates establishing cyber defence through an "integrated defence-in-depth" – which entails setting up multiple layers of defence in a well-integrated manner.

This achieves synergy and creates a multiplier-effect on organisations' cybersecurity effectiveness.



The integration of cybersecurity measures can also give rise to cost-savings whilst maintaining effective cybersecurity. In order to simplify how organisations, especially SMEs, can defend themselves, CSA has identified 13 integrated cybersecurity measures, of which the top 6 are termed 'Essentials'.

Based on CSA's view of the current cyber threat landscape, the **6 Essentials** (see synopsis below) set out in this handbook are sufficiently effective in protecting any organisation against targeted attacks. Why? They help the organisation achieve a 20/20 vision, which allows defenders to thwart attackers. CSA also recognises that there is no silver bullet solution, thus the measures are designed to ensure coexistence.

ESSENTIAL 1
Know Your Assets
To know your assets is to have identified and understood the cyber components of your organisation. An inventory should be maintained to keep this knowledge current so as to prevent and detect unauthorised access to those assets, thus enabling effective response and recovery.

ESSENTIAL 2
Allow Only Authorised Software To Work
Implementing application control integrated with antivirus programs ensures that only authorised software are at work.

ESSENTIAL 3
Timely Patching And Updating
Patch and update operating systems, firmware, and applications in a timely manner to reduce system-known vulnerabilities. This minimises exploitative attacks.

ESSENTIAL 4
Giving The Right Admin 'Passes'
Restrict administrator privileges so as not to give attackers privileged rights to compromise systems.

ESSENTIAL 5
Detect Breaches Promptly
Detect breaches as soon as possible by setting up continuous network monitoring with audit trails/security log enabled for users and application activities.

ESSENTIAL 6
Access Control
Ensure authorised access only, by implementing multifactor authentication.

ESSENTIAL 1

Know Your Assets

Simply put, an asset is something that is of value to the organisation. Cyber assets involve people, process or technology. They include all staff, as well as hardware, software and network links, such as Internet connections. However, data is often deemed to be the most important asset – a faulty machine can be repaired, a buggy software can be patched and fixed, but the loss of data is often irreversible. Without data, no process can take place and the organisation cannot operate normally.

To *know* is the first important step. List down all current IT equipment, software or cyber assets owned by your organisation. This is the first line of defence. With this inventory list, you will know which specific asset is connected or unconnected to your organisation, and to quickly detect unapproved hardware or software in your IT network. This is one way to keep attackers from using an unapproved device or software to break into your network. By being able to effectively detect cyber assets in such a manner, the organisation's response and/or recovery to a cyber-attack would be elevated.

What to do:

- Appoint a senior executive to undertake the inventory count.
- Physically count and list/map all cyber assets connected to the corporate IT network. This includes hardware, such as PCs, laptops, printers, modems and network routers. All purchased programs, such as Word, Excel and other professional software like accounting, video editing and programming tools, must also be listed.
- Update the list/map every quarter to ensure that new devices and software are included.

Include the device name like Dell XPS 15 laptop and the updated version ID of each software update such as macOS Sierra Version 10.12.6. This detailed asset information will aid subsequent work like patching.

If you want to do more:

- Install and run software to automatically check that only authorised organisational assets are allowed to connect into the organisation's network (otherwise, an alarm is triggered to IT and security managers for example). This software could also help manage the organisation's inventory list/map.
- Connect the dots. Draw and maintain an architecture diagram (map) to see the internal and external connections made by assets from the organisation's network.

Good rules to follow:

- For work, use only devices (including thumb drives, portable hard disks, and other removable media) issued by your organisation.
- Such devices are to be included in the organisation's inventory list/map.
- Ports, devices, and software that are no longer in use must be disconnected from the organisation's network.

ESSENTIAL 2

Allow Only Authorised Software To Work

Malicious software, more commonly called malware, infects a network in several ways. It may enter a network because a user — intentionally or unintentionally — downloaded it from a website/cloud application, or opened an email attachment that contained the malware. It may also be transferred into the network via a removable media device.

How do you prevent such unauthorised entry from doing damage? By using application control, together with antivirus software.

Application control is a security practice that restricts or blocks unauthorised (be it unwanted, untrusted or malicious) applications from running and authorised applications from doing unauthorised functions. In this way, application control helps to ensure confidentiality, integrity and availability of data used by and transmitted between applications.

Install an antivirus software that works with application control to detect, quarantine and remove the malware that can compromise computers and networks. This two-in-one defence eliminates the risks posed by sophisticated malware, which exploits known or even unknown vulnerabilities to access corporate data.

This combination prevents unwanted applications from being downloaded and accessing, removing or modifying data. It also blocks malware and removes them, stopping them from spreading in the network.

What to do:

- Install an application control solution that is integrated with antivirus software that uses both whitelisting and blacklisting to prevent unauthorised applications including malware from running. The whitelist takes reference from Essential 1's list of organisation's authorised assets.
- Once installed, the application control highlights the blocked applications. Review this blocked list and remove all unnecessary applications.
- Update antivirus definitions as soon as they are available. Antivirus software identifies new malware via its 'fingerprints'.
- Monitor and track all antivirus alerts to ensure that all malware is quarantined and removed.

Have a seamless process for employees to submit, review and approve all applications before installing them in any device or network.

ESSENTIAL 3

Timely Patching And Updating

A patch is typically something that is provided by software developers to fix a critical error or security issue. Updates tend to focus on adding functionalities and features to the software that could also be security-related. From time to time, software and sometimes hardware companies update or patch their operating systems, firmware, and applications to fix bugs or weaknesses in them.

Users must update their software because cyber-attackers can use such flaws to break into and explore corporate networks, steal data or even give themselves higher system authority.

What to do:

- Track all software and firmware updates used on all devices on the company network.
- Before using any updated or patched software, test it on computers that are not linked to the corporate network.

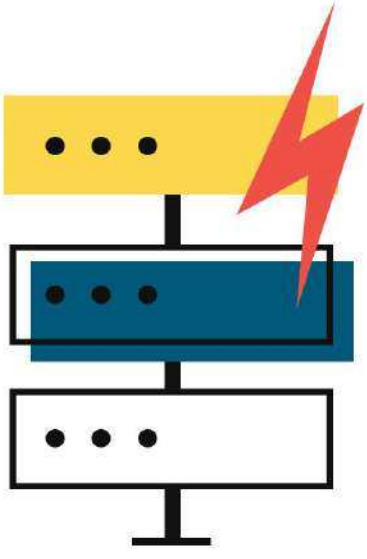
- Draw up a systematic plan for updating all software and firmware to their latest versions.
- Most reputable software vendors often inform customers when one of their software is about to or has reached the end of its lifespan. This means the vendor will not support it further with patches or updates. In this instance, prepare your organisation to use a new software from a vendor that offers support.

TIP

Do not use software that is no longer supported. For example, do not use Windows XP or earlier versions as Microsoft has stopped supporting the operating system. This means that Microsoft will not offer updates to patch any new weaknesses discovered in these older versions of Windows.

If you want to do more:

- Manage the updating process centrally so that you can easily identify all the updated software, as well as outdated applications or operating systems.
- Standardise the software used in the organisation to make updating more manageable, thereby reducing operating costs.
- Authorise someone from your organisation to proactively plan for hardware and software end-of-life.



Good rules to remember

- Ensure that updates are from established software companies or legitimate sources.
- Make sure that users who download updates use a secure process to do so.
- Provide a systematic way to monitor the updating progress of all software used.

ESSENTIAL 4

Giving The Right Admin 'Passes'

A user with administrator privileges, or Admin, has the rights to do many things on a network, such as install software, add new users or access sensitive data. If a malware infects the account or computer of an Admin account holder, it can severely compromise the network.

Data can be lost and the attacker may be able to access other systems and networks to do further damage.

This defence strategy restricts administrator privileges to authorised individuals, who need this level of access to do their work effectively and efficiently.

This prevents attackers, who illegally access a network, from installing malware that will allow them to roam the network freely and access, modify or remove information. Only the Admin of computer accounts and network shall have the necessary privileged rights. Moreover, access to an Admin's account shall only be granted via stringent multifactor authentication.

What to do

- Review the privileges required for all accounts.
- Give users, other than the Admin, the lowest user privileges necessary for work.
- Monitor the use of all accounts.

If you want to do more

- Separate Admin privileges further by different levels of authority without affecting job operations. A network administrator does not need access to corporate data and vice versa.

TIP

Delete unused computer/network accounts.

Constantly review and update all user accounts. Report suspicious use of dormant accounts.

Monitor all Admin accounts, and ensure that their actions are verified or authorised.

ESSENTIAL 5

Detect Breaches Promptly

As a business owner or IT manager, it is vital that you understand your IT networks and systems so that you can detect unauthorised or suspicious activities as quickly as possible.

This can be done through continuous monitoring and frequent reviewing of audit trails and security logs. Audit trails show who has accessed the IT network or system and what operations he or she has performed during a given period of time. Security logs contain records of login/logout activity.

This strategy helps you maintain security and recover lost transactions. It pinpoints network weaknesses and points of illegal intrusion, and also detects suspicious network activity. It also tells you whether the attacker is an employee or an outside party.

With security logging, users who log into the system can be identified. This measure also indicates if such access is unauthorised or unnecessary.

If an attacker succeeds in breaking in, comprehensive logging will identify the stolen or modified data, help the business recover from the incident and prevent similar attacks.

What to do

- Enable users' audit trail and security logging on all devices.
- Ensure that only authorised individuals have access to the security logs.
- Constantly monitor and review security logs to determine if systems have been breached.

When monitoring, focus on unusual or suspicious outgoing activity to the Internet or to external portable storage devices. This improves your chances of spotting security breaches.

If you want to do more

- Roll out a centralised audit trail so that all security logs are consolidated in a separate location for easier monitoring and security.
- Correlate all security logs and flag up suspicious behaviour.

Good rules to have

- Plan for the extra storage needed to store audit trails as they take up space.
- Maintain log-in rules properly and review them periodically.
- Where there are alerts, incident management must be handled properly.

ESSENTIAL 6

Access Control

Access can be given based on what one knows, what one has, or who one is. Access to accounts or networks can be controlled with measures like passwords, token devices and fingerprints. Multifactor authentication involves granting access based on two or more of the mentioned categories.

As passwords can be broken by a skilled attacker, this single factor is no longer enough to protect your accounts. Extra authentication by digital tokens or biometrics makes it harder for unauthorised users to break into accounts.

Individuals with privileged access must use multifactor authentication, especially when accessing the IT network or system outside the workplace.

This defence also limits an attacker's access to multiple IT systems or data.

Even if the attacker gets hold of a user ID and password, these extra levels of authentication work like extra locks that he has to break to gain entry.

What to do

- Manage and audit the use of each authentication factor.
- Physically separate authentication profiles in the IT system. So even if an attacker finds out a user's password, it will not lead him to the user's biometric or physical token profile.
- Configure all accounts such that a user gets access only if he has every authentication factor right.

TIP

Users must not share physical tokens. This ensures that every one is accountable.

Biometric information must be well protected as, unlike passwords, it cannot be changed once stolen.

If you want to do more

- Create a central authentication solution that enforces and manages all multifactor authentication services for the business.

Good rules to have

- If any physical token is lost, it must be disabled immediately.
- Track all tokens and biometric profiles and ensure they are properly stored and processed.

ADDITIONAL MEASURES

The six essentials, when implemented correctly, will keep your systems and networks safe. Organisations can consider implementing seven more **Measures** outlined below, such as encryption, to meet additional business needs. More details on these measures can be found at **https://www.csa.gov.sg/gosafeonline.**

1. ENCRYPT 'CROWN JEWELS'

Once the crown jewels are identified, organisations will understand the cost of attacks. Encryption can be used to protect the crown jewels like customer data from unauthorised disclosure.

2. HARDEN DEVICE CONFIGURATIONS

Devices can be secured by reducing its surface of vulnerability. Essentially, any service, function or application not needed to support a business can be removed and disabled. Such 'hardening' efforts help organisations reduce their attack surface, making it difficult for attackers to gain entry.

3. DEFEND NETWORK PERIMETERS

To prevent network breaches and intrusions, organisations can implement network-based intrusion detection/prevention systems to detect/prevent cyber intrusions. Such systems recognise abnormal traffic patterns or spikes in network movements, which may indicate that data is being transferred out illegally.

4. SEGMENT AND SEGREGATE NETWORK

This effort to split a computer network into smaller networks and enforce rules to control communication possibilities between devices will slow attackers, thus protecting sensitive information and services, and improving performance due to less traffic congestion.

5. IMPLEMENT APPLICATION FIREWALL ON CLIENT DEVICES

Application firewalls can help control and block unknown traffic to protect client devices against malicious or unauthorised incoming network traffic. By doing this, attackers would have difficulty to know the possible points of entry.

6. IMPLEMENT INTRUSION DETECTION/PREVENTION SYSTEM ON CLIENT DEVICES

This measure uses host-based intrusion detection/prevention systems to detect/prevent malicious activities that occur or from occurring in computer memory.

7. PROTECT WEB SERVICES

Cyber-attackers can make use of web content to send malicious data to Internet surfers, thus compromising users' IT systems. By filtering web content and white-listing web domains, users can protect themselves from the 'traps' laid out in the web content and prevent accidental routing to malicious web domains.

KNOW YOUR CYBER HYGIENE

Users are the weakest link in cyber defence. Employees must be 'hygienic' to contribute to cybersecurity. Here are two hygiene rules to follow:

PASSWORDS

Passwords are essential to protect digital access.

As a guide:

a. Create as long and random a password as possible; use a 'passphrase' (5 or more words) that you can remember.
b. Set up 2FA or multifactor authentication whenever possible.

Do not use the same password for multiple accounts (especially between personal and work). Do not use publicly known information about yourself as passwords or write passwords down and leave them unprotected.

BACKUPS

Backups are essential for protection against unexpected data loss when a system fails or during disasters. Recent growth of ransomware threats has highlighted the importance of offline data backups. Sometimes, multiple backups may be needed.

a. Perform backups regularly and frequently. If possible, automate the backup processes.
b. Keep offline backups to protect against ransomware threats.
c. Keep offsite backups to protect against natural disasters.
d. Backups should be tested periodically to ensure they are usable during an emergency.

Do not:

a. Leave backup data unprotected.
b. Keep backup data in the same drive or device as the primary data.

SPOT SIGNS OF PHISHING

Phishing is one of the top scams here in Singapore. Scammers use phishing emails to trick their way into victims' devices, steal confidential information like passwords so that they can breach accounts and possibly steal money and/or personal details. Many businesses have fallen prey to fake invoices sent by scammers posing as legitimate vendors.

To prevent phishing, ignore dodgy emails, for example, an email saying that you have won a contest which you did not participate. Additionally, be wary of misleading domain names such as 'go0v.sg' instead of the correct 'gov.sg'.

Note the following in addition to phishing:

FREE WIFI IS 'OPEN'

While free Wi-Fi is convenient for general browsing, it should never be used to perform private transactions, such as accessing one's Internet banking account. Since free Wi-Fi's access is open, it allows malicious actors to electronically 'eavesdrop' on your Internet surfing session and 'steal' password and login details to illegally access your account.

CLEAR THE CACHE

Hotel business centres and airports provide computing devices for their customers' convenience. Remember to clear the cache after using these devices, especially if you have been accessing private, confidential or sensitive information, such as corporate e-mails and Internet banking accounts. This prevents the next user from easily looking up your online transactions or visited pages.

YOU'VE BEEN HACKED.
NOW WHAT?

It is not a matter of 'if', but 'when' an organisation will be attacked.

Some signs that you have been attacked:

- When you click on an Internet link or download an online file, and you cannot access your usual files, applications or services.
- If you are locked out of your online accounts or receive messages that your password has been changed when you have not changed it.
- When your organisation's system slows to a crawl when responding to legitimate users, it may be suffering from an attack, where cyber-attackers have swamped the targeted system with so much information that it grinds to a halt.

So how?

- Find out the reason for the attack to better understand the breach. This will help with recovery.
- Take back your account. For example, if your Internet banking account has been illegally accessed, report it immediately to the bank. Immediately change the password.
- Perform a security check on all your affected systems accounts. Ensure that all **6 Essentials** (listed on pages 4 – 15) have been thoroughly implemented. Consider stepping up your security posture using the additional **Measures** (see pages 16 & 17).
- Call your organisation's incident response team immediately when you discover the cyber-attack. The team will help the organisation manage the situation. Remember to report the incident to the **Singapore Computer Emergency Response Team (SingCERT)**.

ONLINE RESOURCES ON CYBERSECURITY

You now know more about cyber defence.
Keep up with related developments by following these websites:

Cyber Security Agency of Singapore

- www.csa.gov.sg
- facebook.com/CSAsingapore
- @CSAsingapore
- contact@csa.gov.sg

The Cyber Security Agency of Singapore (CSA) is the national agency overseeing cybersecurity strategy, operations, education, outreach and ecosystem development. To find out more about Singapore's efforts in cybersecurity, please visit CSA's website.

Gosafeonline

- www.csa.gov.sg/gosafeonline
- facebook.com/gosafeonline
- @gosafeonline
- gosafeonline@csa.gov.sg

Gosafeonline is a resource portal to help build a positive culture of cybersecurity in Singapore, where cybersecurity becomes second nature for all Internet users. To find out more about essential cybersecurity practices for both individuals and organisations, please visit Gosafeonline's website.

SingCERT

- www.csa.gov.sg/singcert
- (+65) 6323 5052 for Incident Reporting
- singcert@csa.gov.sg for Incident Reporting

The Singapore Computer Emergency Response Team (SingCERT) is a portal that responds to cybersecurity incidents in Singapore. It comes under CSA and was set up to help detect, resolve and prevent cybersecurity related incidents. SingCERT provides technical advisories and alerts on a variety of vulnerabilities and malware.

ISBN 978-981-11-6122-3