



Ten critical controls 2018.



CERT NZ has summarised the ten controls that would mitigate, or better contain, the majority of information security incidents that we have analysed so far.

CERT NZ's ten critical controls are designed to give you more certainty about what to spend your time and money on. They summarise the controls that would mitigate the majority of information security incidents that CERT NZ has analysed so far.

They're based on the incidents that we've seen to date as well as other sources that CERT NZ has privileged access to, like the global CERT network and international data feeds. We will update the list annually based on the data we've received.

In the coming months, we'll publish more details on **www.cert.govt.nz** about the importance of each of the controls and how you can implement them.

This is not a complete list and we recommend you continue your usual best practice, such as maintaining an effective password policy and firewall configuration.

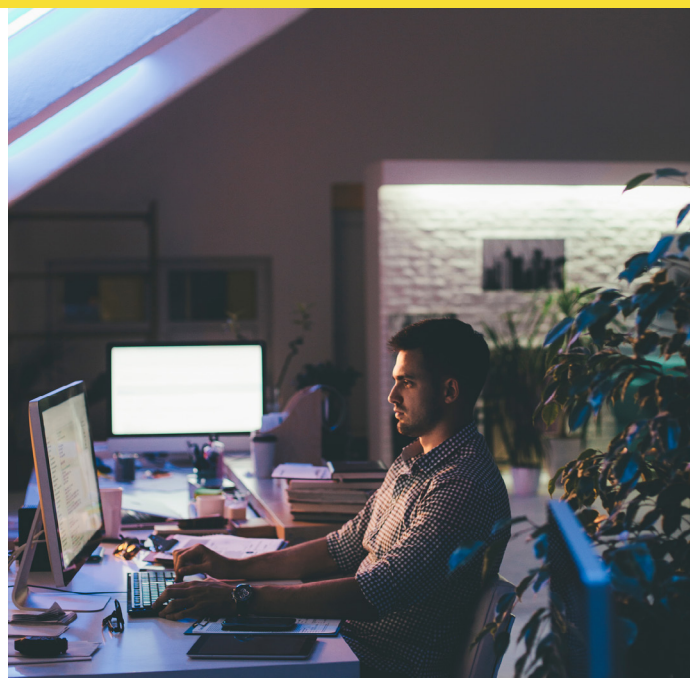
Report anything that breaches, or nearly breaches, your defences even if you don't need help. Your reports give us even richer data to assess current threats facing New Zealanders.

Ten critical controls 2018.

1. Patch your software

Keeping software, like operating systems and applications, up-to-date is one of the most simple and effective steps you can take to ensure that your environment stays secure. We recommend patching all software including:

- operating systems of all devices,
 - firmware of all devices,
 - software/ applications (particularly web browsers), and
 - any other components that connect to your network.
- Many organizations have been attacked by malware that exploits known vulnerabilities where patches have been released, but not applied.



2. Upgrade or replace legacy systems

Legacy systems frequently contain business critical data, or support important processes, which is why they're often left alone. However, business critical systems warrant the highest levels of security and maintenance.

Replace or upgrade any systems in your network that are not being maintained or receiving security updates. Several attacks this year have exploited legacy software such as Windows XP.

3. Disable unused services and protocols

Keeping your systems up-to-date isn't always enough to keep attackers away. Older devices and protocols often have their own vulnerabilities. Leaving them on your network gives attackers more opportunities to breach your network. To mitigate this, proactively scan your network for services and protocols that are not used or are known to be vulnerable. Once these are identified, carry out remediation based on your findings. This was demonstrated during the WannaCry incident, which exploited out-of-date protocols enabled in many systems.

4. Implement application whitelisting

The mail client and web browser are two of the most common ways to infect a user's workstation with malware. To prevent this, identify a list of applications that your users need. Ensure only approved applications can be executed. Most malware incidents reported to CERT NZ are thought to have originated from opening malicious email attachments, or drive by downloads. Whitelisting approved applications will help protect the system from these attacks, and is a key security control for your network.

5. Change default credentials

In the rush to get a new piece of technology into production, sometimes security is overlooked. A key step to take for any new application or device is to change or remove all default credentials. This prevents an attacker from using known usernames and passwords to gain access to your network. We continue to see organisations compromised by attackers using unchanged default credentials.

6. Enforce multi-factor authentication

Credential dumps and credential harvesting attacks are common, giving attackers large numbers of usernames and passwords. Protect your business systems and data by enabling multi-factor authentication on all privileged or remotely accessible systems. This includes VPNs, administrative consoles, webmail and published applications such as Citrix. In 2017, there have been continuous phishing campaigns focused on credential harvesting, such as the Office365 campaign. In the cases we've seen, multi-factor authentication would have prevented unauthorised access to the accounts with the leaked credentials.

7. Enforce the principle of least privilege

Grant users the minimum level of access and control in your network required to do their job, and remove accounts once they are no longer needed. This will limit the damage that intrusions into your network can cause. CERT NZ is aware of incidents where users held administrative privileges unnecessarily, which attackers were able to exploit in order to make unauthorised changes to the environment. We also recommend enforcing separation of privilege – use a separate account when a user requires administrative privileges.

8. Implement and test backups

Regularly back up your business data and systems. These should be stored offline, and regularly tested.

In response to threats such as ransomware, businesses' often need to restore data from their latest backup. We have seen organisations lose data and incur significant operational costs due to a lack of up-to-date, well-maintained backups.

9. Configure centralised logging

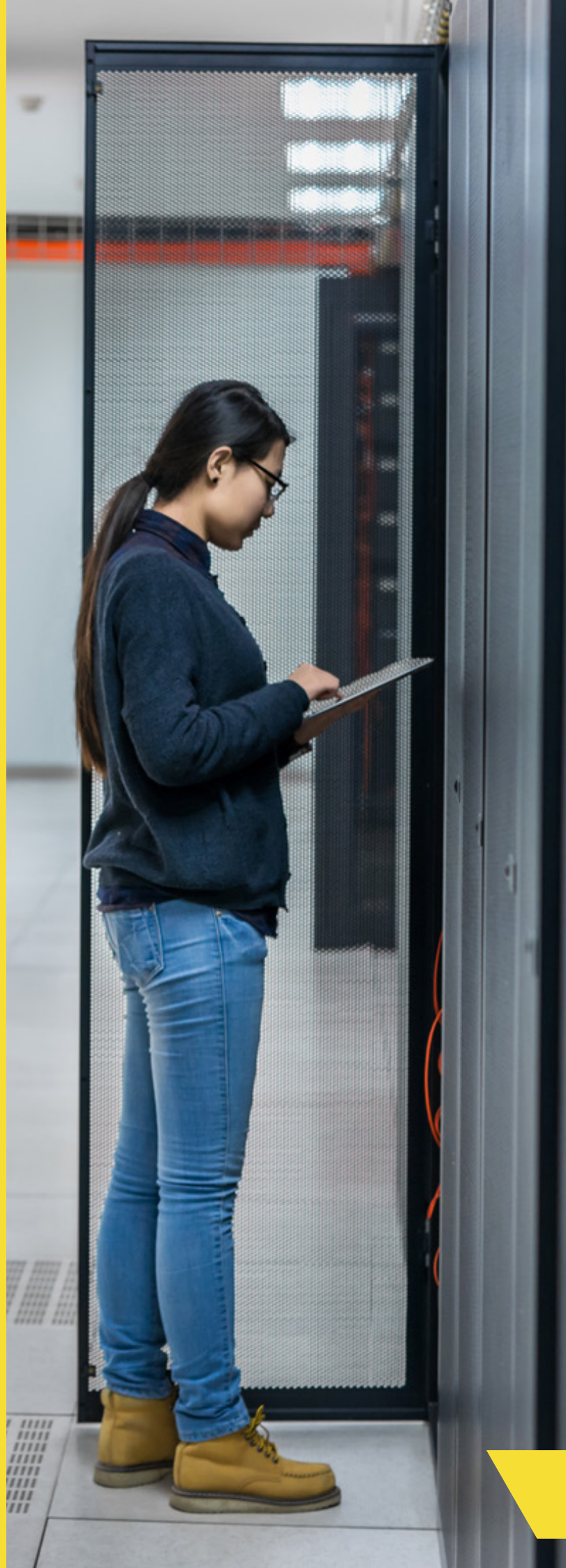
Implement and maintain centralised logging of your network and systems. This enables you to detect abnormal behaviours and investigate them. Without good logging, it's very difficult to discover the nature and extent of a compromise. This makes your efforts to contain and recover from an incident much harder. In many incidents reported to CERT NZ, a complete post-incident investigation has not been possible, due to lack of logs.



10. Manage your mobile devices

It has become common to access or hold business information on mobile devices. Mobile devices are easier to steal or lose, which may allow attackers to access or destroy business data.

Make sure you have the same level of control and maintenance on those mobile devices as you do on your workstations. Without mobile device management, you will be unable to verify the implementation of critical security controls.



Ten critical controls 2018.

1. Patch your software
2. Upgrade or replace legacy systems
3. Disable unused services and protocols
4. Implement application whitelisting
5. Change default credentials
6. Enforce multi-factor authentication
7. Enforce the principle of least privilege
8. Implement and test backups
9. Configure centralised logging
10. Manage your mobile devices

About CERT NZ

We work to support businesses, organisations and individuals who are affected (or may be affected) by cyber security incidents. We provide trusted and authoritative information and advice, while also collating a profile of the threat landscape in New Zealand.

To report an information security incident, visit
www.cert.govt.nz