Nexia Australia

Cyber security and risk management

‘Essential Eight’ to reduce cyber threats

Technology has become the greatest enabler of doing business in the 21st century. Technology and cyber capabilities have become a conduit for theft, commercial espionage, hacking and defacement. Intrusions and attacks can go undetected and quickly cause great harm to an organisation. As a result, all businesses need to develop good cyber posture, even if their business is not necessarily cyber related.

Traditional discussion around cyber security has always been technically based, when in fact, it should be risk based. Cyber security is just another risk lens to view your business through. It is near impossible to understand the depth of cyber security risk without a comprehensive risk analysis review.

The Australian Cyber Security Centre (ACSC) has developed the Essential Eight Strategies to Mitigate Cyber Security Incidents. The Essential Eight are a baseline goal to aim towards in enhancing your organisation’s cyber posture.

The Essential Eight Mitigation Strategies are as follows:

1. Application whitelisting.
Restricting application use to only include programs which have been vetted and approved to operate will mitigate the risk of potential malware from being executed.

2. Patch applications.
Running the latest version of computer applications will mitigate the risk from security vulnerabilities being exploited. Ensure patches are installed in a timely manner.

3. Patch operating systems.
Security vulnerabilities in operating systems can be exploited and compromise an entire organisation’s system. Old operating systems which are no longer supported (e.g. Windows XP) do not receive security updates. Ensure all devices are running the latest version of an operating system (e.g. Windows 10) and security patches are installed in a timely manner.

4. Restrict administrative privileges.
Limiting administrative privileges to operating systems and applications can reduce the chance of higher access being compromised or falling into the wrong hands. Blocking email access and web browsing capabilities on administrative accounts can also increase their security.

5. Configure Microsoft Office macro settings.
Macros can be used to infiltrate a system. Only permitting the use of vetted macros which come from a trusted location can contribute to the overall strength of an operating system.

6. User application hardening.
Java and Flash add-ons and other program features can be used to deliver malicious code and execute malware on a system. Disabling or uninstalling add-ons can increase the security of user applications.

7. Multi-factor authentication.
Adversaries can access sensitive information and systems through user logins. Requiring multi-factor authentication (e.g. entering a password and an access pin which is system-generated and sent to a user’s phone) can reduce the chance of successful malicious access.

8. Daily backups.
Reducing the damage following a cyber incident can be achieved through maintaining backups of important data and software configuration settings. Backups should be retained for at least a three month period and tested regularly.

Implementation of the Essential Eight will vary across organisations depending on potential adversaries and risk profile. It is important to undertake a comprehensive risk analysis prior to implementation to develop a sustainable security strategy.

Ultimately, establishing a security culture throughout an organisation is fundamental to risk mitigation. Well-developed and robust security strategies can be quickly and easily undone through human interaction. Framing cyber security through a risk management lens rather than technical has a greater chance of engagement throughout an organisation.

Contact your Nexia advisor today for an internal risk management review.

Speak to a specialist
Canberra
Geoff Campbell
gcampbell@nexiacanberra.com.au
+61 2 6279 5400

www.nexia.com.au