pa.com.au

2017 Australian Cyber Security Centre Threat Report

The State of Cyber Security in Australia

LATEST CYBER SECURITY NUMBERS

Cyber security crimes are on the rise

47,000
Reported cyber crime incidents in the last year

22%
Overall increase in Online Scams and Fraud

100%
Overall increase in Online Fraud

THREAT ENVIRONMENT

Malicious adversaries are becoming more sophisticated and persistent

- Improving skills and expertise of cybercriminals in adapting their tradecraft
- Increased targeting andcompromises of trusted third parties
- Cybercriminals routinely scan the environment for vulnerabilities
- They continue to seek access to personal info to facilitate financial crimes and identity theft
- Internet of Things (IoT) devices introduce significant security risks

PRIVATE SECTOR TARGETS

Everyone is a prime target but over the last two years, these were the most affected industries

Cyber espionage activity is likely to target Australian industries where:

- Australia has particular technology or research strengths
- Foreign states have identified a specific technology gap
- A particular economic or military benefit exists
- Foreign states lack the capability to manufacture or develop the technology indigenously
- Research, development and manufacturing costs are prohibitive
- An organisation holds bulk personally identifiable information
- A foreign entity is seeking to invest or purchase within the sector

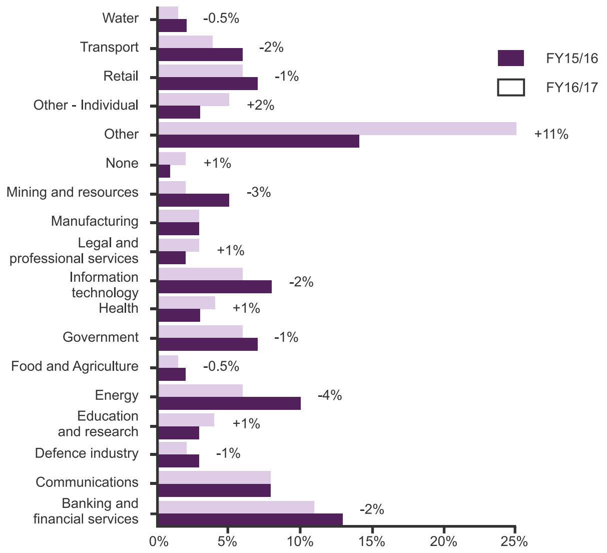


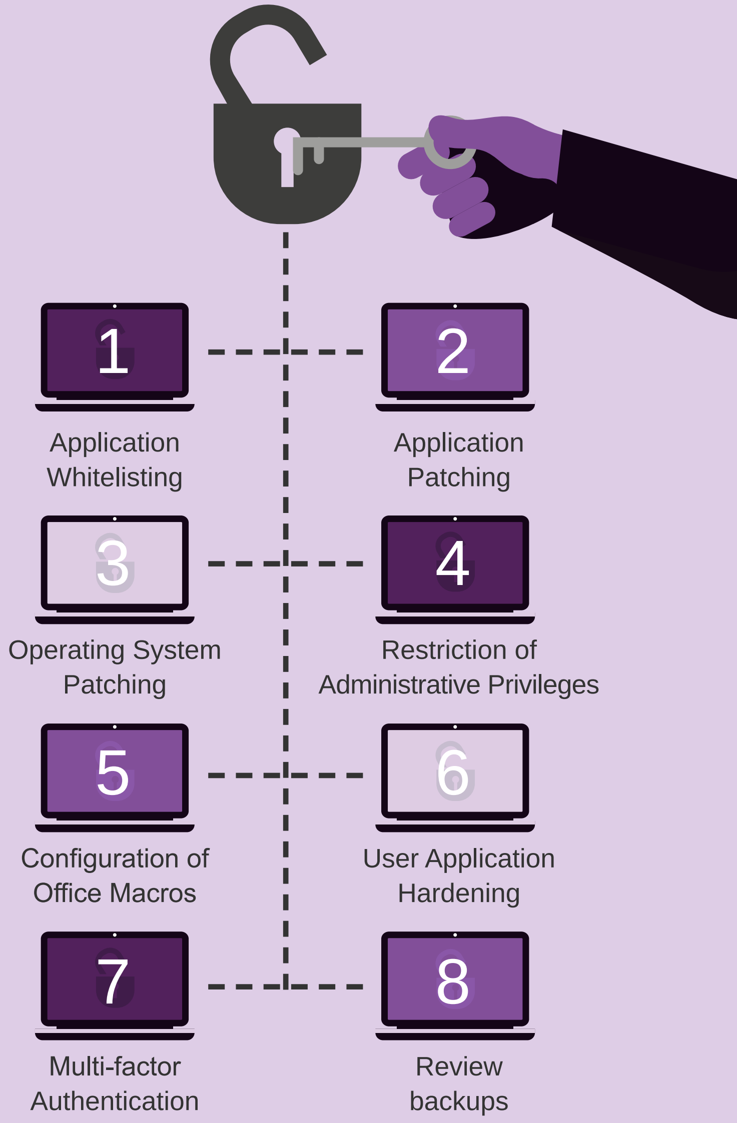
FIGURE 6:Private sector incident response by sector

* CERT Australia has had an increase in voluntary reporting from sectors that have not been traditionally targeted, such as the accomodation, automotive and hospitality sectors. This shows the expanding scope of targets for adversaries and cybercriminals.

CYBER SECURITY ESSENTIAL EIGHT

In every compromise the Australian Signals Directorate (ASD) has investigated in the past several years, correct implementation of the Essential Eight would have effectively prevented or minimised the extent of compromise. The Essential Eight helps mitigate these common risks:

- Targeted cyber intrusions
- Ransomware
- Malicious insiders
- Threats to industrial control systems
- Adversaries who have destructive intent


1
Application Whitelisting
2
Application Patching
3
Operating System Patching
4
Restriction of Administrative Privileges
5
Configuration of Office Macros
6
User Application Hardening
7
Multi-factor Authentication
8
Review backups

OUR SIMPLE TIPS TO FIGHT CYBER THREATS

Here are a few things you can immediately do now to keep your data and business safe:

- Delete suspicious emails requesting for sensitive data such as passwords or financial information.
- Be cautious about unsolicited emails.
- Use VPN if you muse use a public Wi-Fi.
- Keep your application and operating system patches and antivirus software up to date.
- Encrypt your laptops, mobile devices and portable storage with free tools that come with some of your software subscription such as Microsoft’s Data Loss Prevention and Information Rights Management.

If you want to know more about how we can help you implement your cyber security strategies, contact one of our experts for a free consultation.