Cyber criminals are coming for you: are you prepared for the unexpected?

Connecting Up Webinar
June 2022

pwc

We acknowledge and pay our respects to Aboriginal and Torres Strait Islander peoples as the First Peoples of Australia, whose ancestral lands and waters we work and live on throughout Australia. We honour the wisdom of, and pay respect to, Elders past, present and future.

Presenters

Chris Davis
Director
Cybersecurity & Digital Trust
PwC Australia

Nicola O'Brien
Senior Manager
Cybersecurity & Digital Trust
PwC Australia

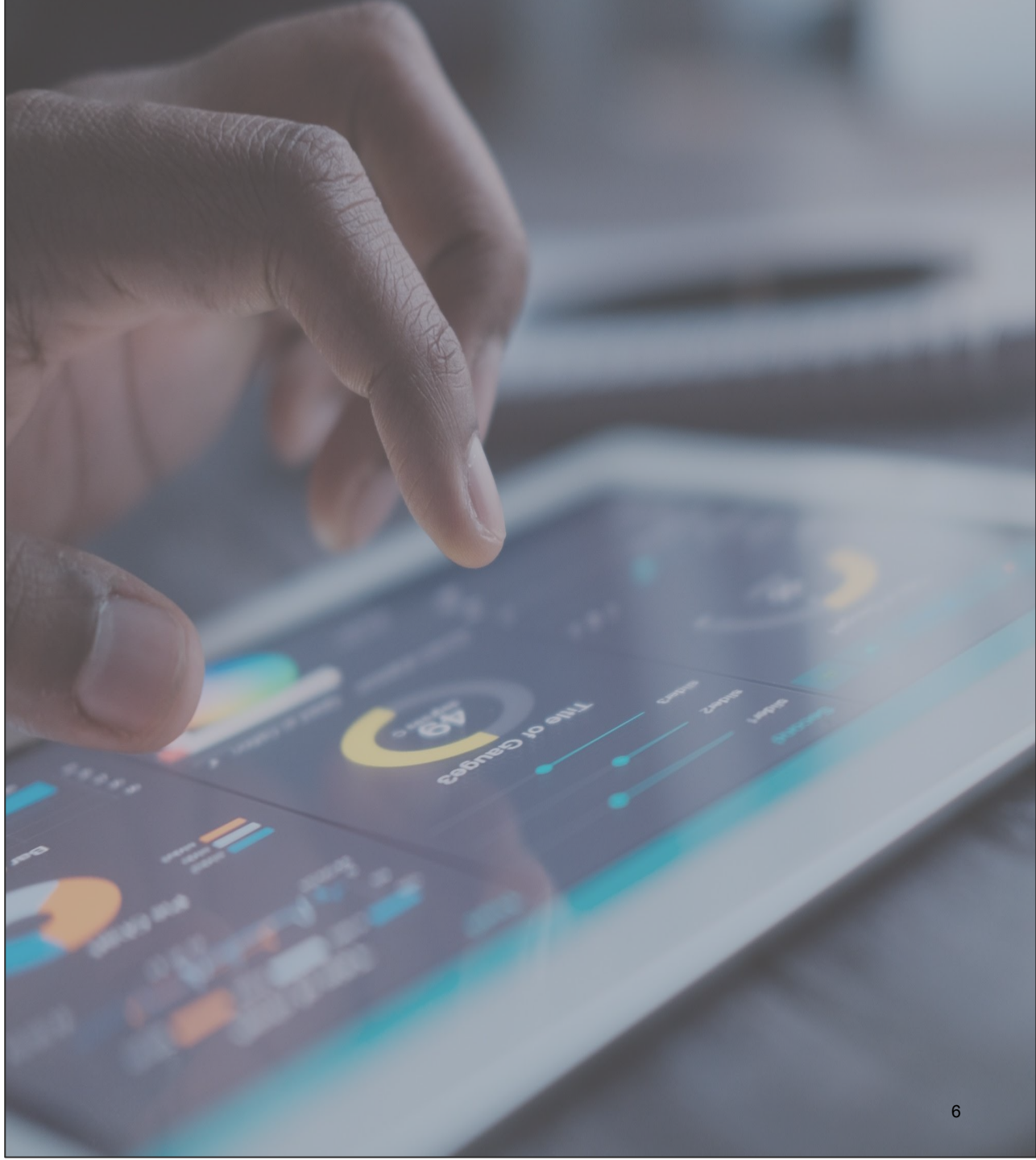
Agenda

Agenda item	Duration
Welcome	10 mins
Introduction to the cybersecurity threat landscape	10 mins
Common scams affecting individuals & businesses	10 mins
Case studies & industry examples	10 mins
Tips and tricks to protect yourself	10 mins
Q&A	10 mins

01

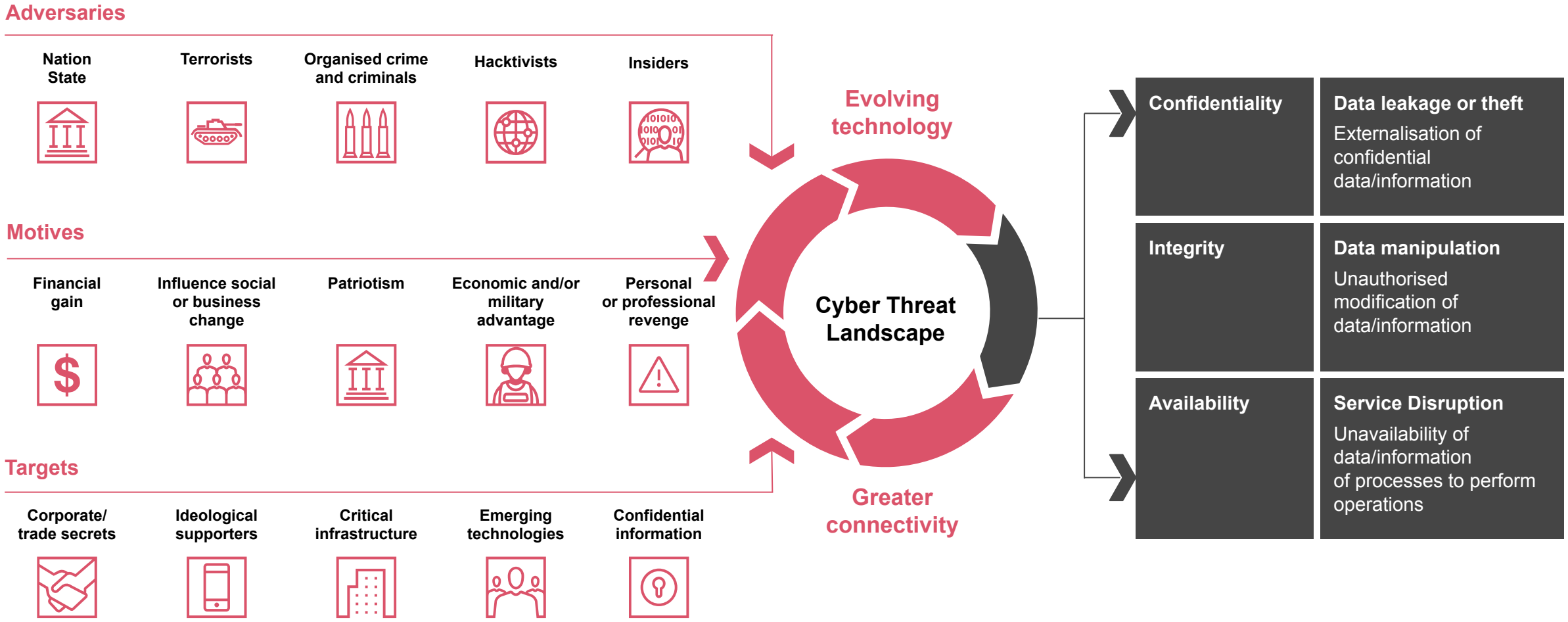
Introduction to the cybersecurity threat landscape

Poll Question 1



Cyber threat landscape

The Cybersecurity threat landscape involves adversaries from a range of threat actor groups, who have specific motives to perform attacks on target assets.



Cybersecurity threat landscape

The Cybersecurity threat landscape has continued to evolve with an increase of attacks, scams and reported losses. The Australian Cyber Security Centre (ACSC) reported the following over 2020-2021:

Online Scams - Fraud, online shopping scams and online banking scams were the top reported cybercrime types.

Reports - Over 67,500 cybercrime reports, an increase of nearly **13 per cent** from the previous financial year.

Losses - Self-reported losses from cybercrime total more than **$33 billion.**

Pandemic Attacks - More than **75 per cent** of pandemic-related cybercrime reports involved Australians losing money or personal information.

Pandemic Reports - Over **1,500** cybercrime reports of malicious cyber activity related to the coronavirus pandemic **(approximately four per day)**.

Ransomware - Nearly 500 ransomware cybercrime reports received, an increase of nearly **15 per cent** from the previous financial year.

NGO/NFP Sector - The PwC Threat Intelligence team reported 29 individual incidents in the NGO sector (top 10 of all sectors) globally throughout 2021.

Source: PwC Cyber Threats 2021: A Year in Retrospect

Source: ACSC Annual Cyber Threat Report 2020-2021

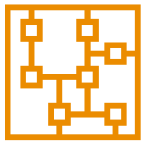
Key themes in 2021

PwC's 25th CEO Survey found that **52%** of CEOs say cyber risk is inhibiting their company's ability to innovate. The below are the key themes highlighted in the PwC Threat Intelligence team's annual Year in Retrospect report.

Ransomware

Ransomware continues to be the most significant cyber security threat faced by all organisations irrespective of industry sector or location. Its impact can also be felt across organisations' supply chains and international operations, and can affect civil society. Ransomware operations are increasingly run as organised business.

Supply Chain Compromise



Supply chain compromise is here to stay, now part of the 'new normal' of the cyber landscape with cyber criminal threat actors as well as APTs adopting this tactic. After the high profile and brazen targeting across the last year, we assess that focus should likely shift to detection and response.

0-days

The leveraging and exploitation of **0-days** has increased, and is likely to continue to do so. Similar to supply chains, defence in depth could prevent the potential impacts of such a trend.

Commercial Espionage

Commercial espionage continues to be a primary driver in the cyber security market, with companies selling offensive security solutions such as spyware, 0-day exploits and related capabilities to entities who would then go on to use for malicious campaigns.

Civil society

Civil society is consistently targeted by espionage-motivated threat actors. These may include countries purchasing spyware tools from commercial brokers for the purposes of using them against their own citizens, or APTs targeting individuals, dissident communities, NGOs, activists, as well as journalists.

Top Predictions for 2023-2025 and Beyond

Gartner has unveiled the below predictions on trends for 2023 and beyond, and recommends leaders to build these strategic planning assumptions into respective cybersecurity strategies.

Privacy rights

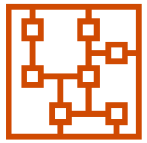
Privacy regulation to cover **5 Billion** citizens and **70%** of global GDP

Ransomware payments

30% of nation states will pass legislation that regulates ransomware payments, fines and negotiations (up from 1%)

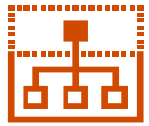
Resilience

70% of CEOs to mandate a culture of organisational resilience



Third parties

60% of organisations will use cybersecurity risk as a primary determinant for conducting business with third parties



Consolidation

80% of organisations will adopt a strategy to unify web, cloud services and private application access from a single platform

Accountability

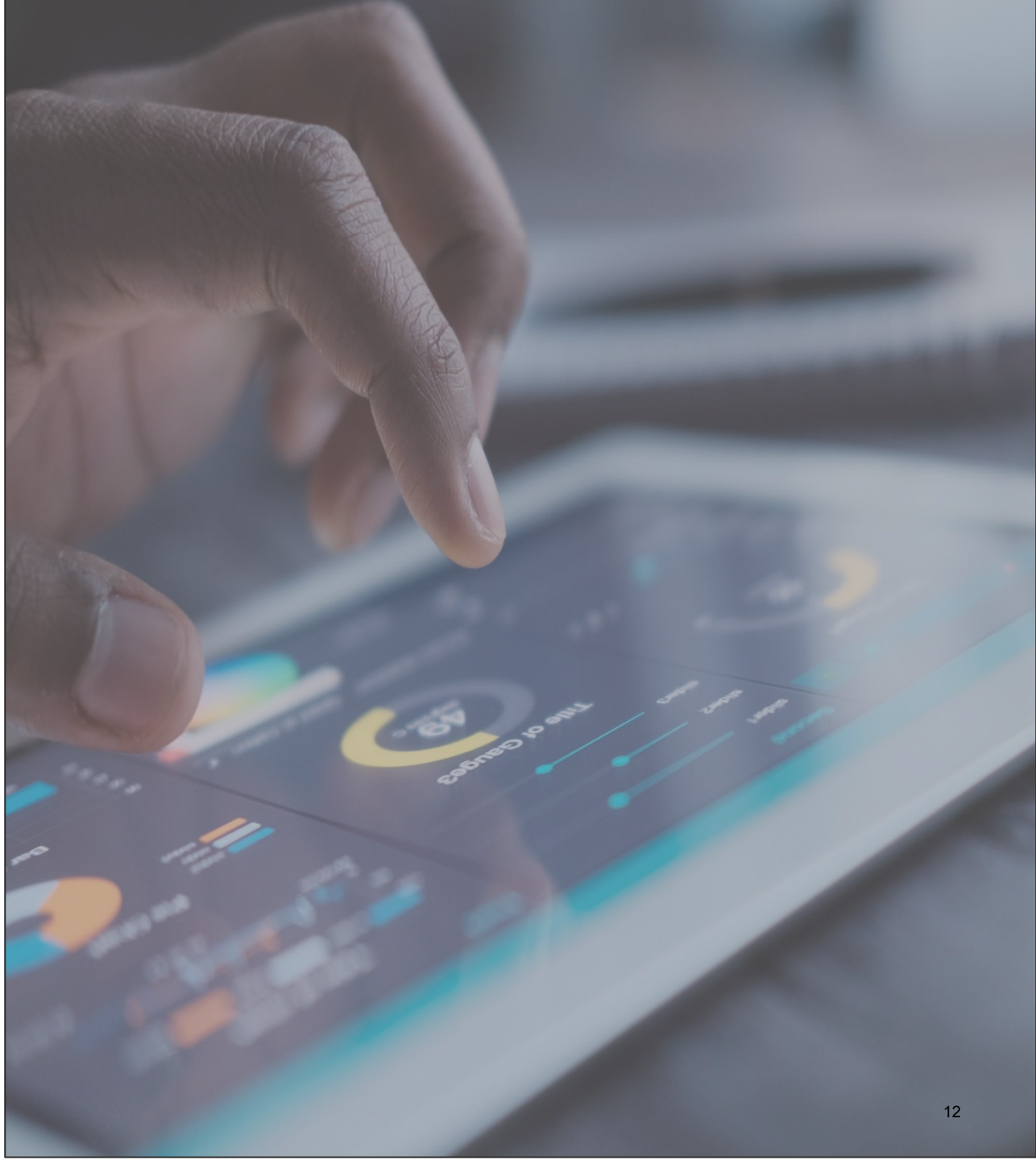
50% of C-level executives will have performance requirements related to risk in their contracts - shifting the accountability of cyber risks to senior business leaders

Source: Gartner 2022 Press Release: Gartner Unveils the Top Eight Cybersecurity Predictions for 2022-23

02

Common scams affecting individuals & businesses

Poll Question 2



Consider this scenario

- It's a Friday afternoon, and you are about to go and pick up your kids or meet your friends after work
- You receive an email from your boss requesting an urgent payment be made to a priority client
- You download and open the email attachment titled "payment transfer information"
- After opening the attachment, a message pops up notifying you that a software update is required and prompting you to call the IT support desk for help
- You call the IT support team using the provided number and ask them to help you with the update
- The IT support team asks for your full name, email address, and password
- You start the update and leave your computer unlocked for the weekend
- On Monday, you go to log in to your account but can't access any of your systems or data

What red flags or potential indicators of a cyber threat you can see here?

Why scams?

54%
increase
in the total loss from Business Email Compromise (BEC) attacks in FY 2020-211
(compared with FY 2019-20)

82%
of breaches involve the human element

60%
of employees opened emails they weren't fully confident were safe.

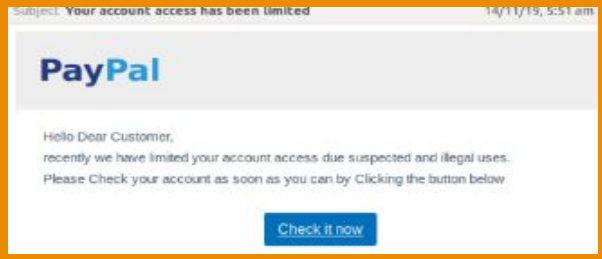
286,000
Australians reporting they were scammed last year

13 million
suspected scam calls are blocked by Telstra per month.

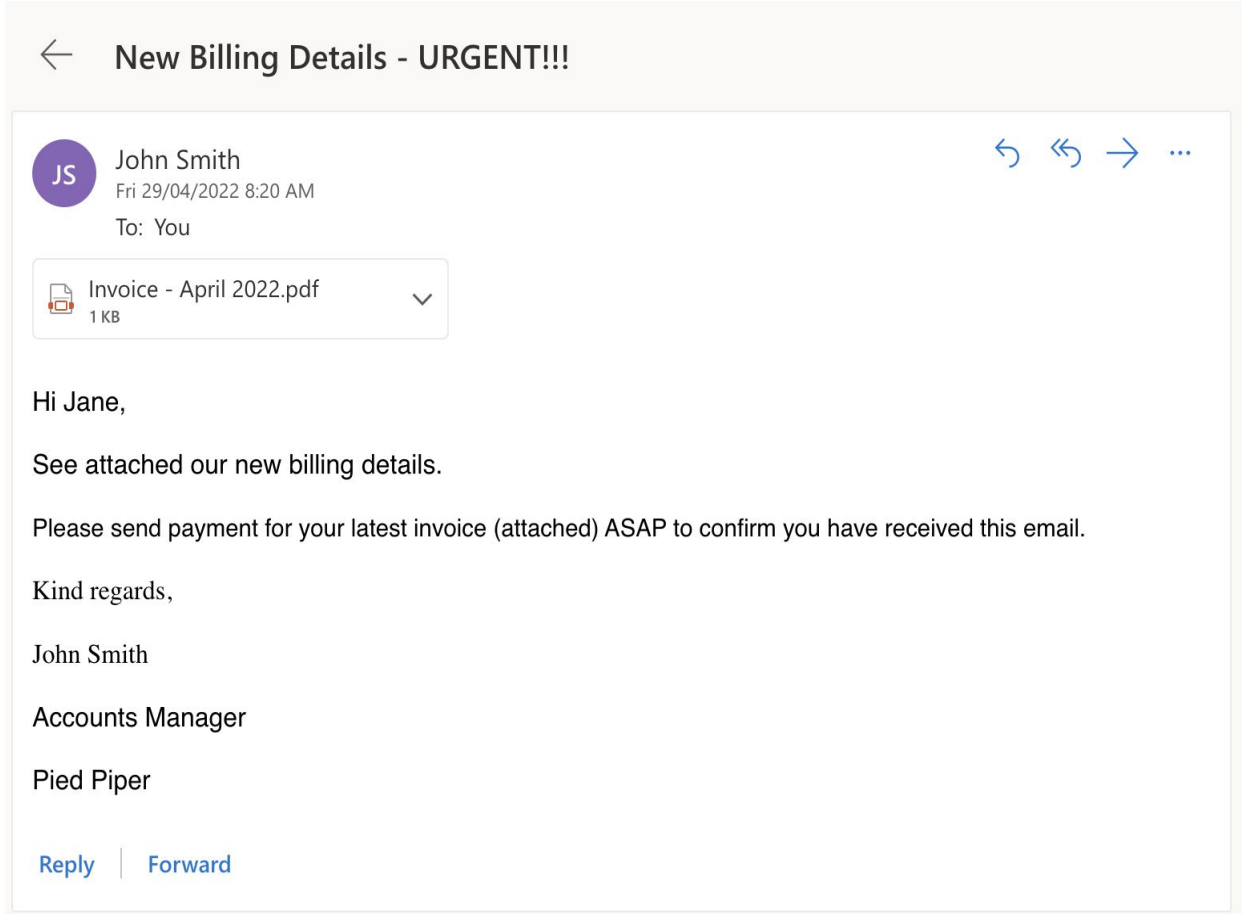
47%
of workers cited distraction as the main factor in their failure to spot phishing attempts.

41%
of employees failed to notice a phishing message because they were tired.

Common scams targeting businesses and individuals during the End of Financial Year period

SMS scams	A text message harvesting personal details or delivering malware Our guard is down when we're on our phone Watch for urgency, offers too good to be true, and dodgy links.	
Email scams (inc BEC)	Email scams are a primary tool used by attackers to steal money, account credentials, and sensitive information. Types of email scams come in many forms, including: • Phishing • Credential theft • Malware • Monetary theft • Wire Fraud • Supply-chain attacks	
Phone call scams	Phone call scams are fraudulent phone calls made to trick people into giving money or revealing sensitive information. Frequently involves a criminal pretending to represent a trusted institution, company, or government agency.	

Business email compromise



How

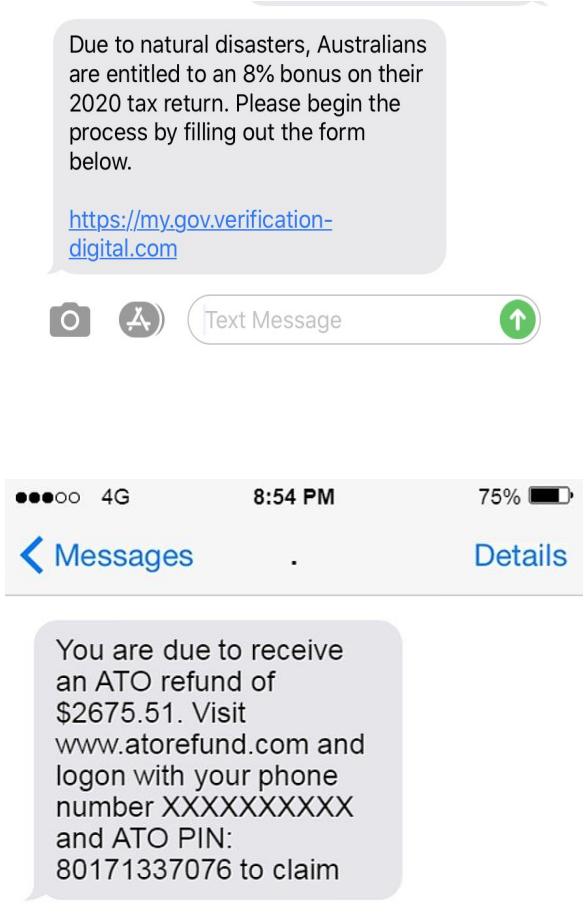
An email from a senior executive, or supplier, requesting an urgent payment, or payment to a new account.
The sender may be either have access to a legitimate email account, or be spoofing that account

Example

Homeless Charity, One Treasure Island: $625,000 BEC loss
In June 2021, we learned that San Francisco-based homelessness charity Treasure Island fell victim to a devastating, month-long **$625,000 BEC attack** after hackers infiltrated the organisation's bookkeeper's email system.

The hackers found and manipulated a legitimate invoice used by one of Treasure Island's partner organisations. Staff at Treasure Island transferred a loan intended for the partner organisation straight into the cybercriminals' bank account. The nonprofit sadly lacked cybercrime insurance.

Phishing



How

These emails most commonly direct target recipients to an attacker-controlled website that delivers malware or intercepts user credentials.

Example

Australian Government department
On 7 April 2020, the ACSC received a report from an Australian Government department that a senior staff member's email was being spoofed as part of a COVID-19 themed phishing campaign. The email contained an attachment with embedded malware that was designed to steal sensitive information such as banking usernames and passwords.

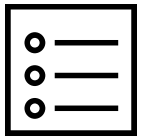
Educational institute
Users receive via email a document shared with them through Microsoft OneNote, a collaborative note-taking app. Once they clicked on a link, it directed them to a login page on the institutes Sharepoint, another collaborative platform, where credentials are stolen.

Steps to avoid scams

Pause

- Before clicking
- Before paying
- Before opening
- Before actioning request

Verify



- Verify payment requests with a phone call
- Validate requests for personal information

Use Secure Platforms

Use existing payment gateways and platforms

Education awareness

How to spot scams
How to report them
Never provide credentials

Secure your data

- Secure storage of credentials
- Secure TFN and important banking details
- Consider how much corporate information is available publicly
- Use strong passphrases and MFA

03

Case studies & industry examples

Ransomware

How

Ransomware is a type of malicious software designed to block access to a computer system until a sum of money (the ransom) is paid.

Example

Volunteer Agency (NZ)
One of New Zealand's largest volunteer agencies working in international development suffered a ransomware attack in may 2021. Attackers locked and encrypted vital information their systems and demanded a ransom. Backups were also encrypted.

The organisation refused to pay the ransom and has since recovered from the attack. They however did lose some historical information, which they were unable to recover due to the encrypted backups.

Software vulnerabilities

How

Malicious actors aim to exploit security vulnerabilities, at times within hours of public disclosure, patch release or technical write up.

Example

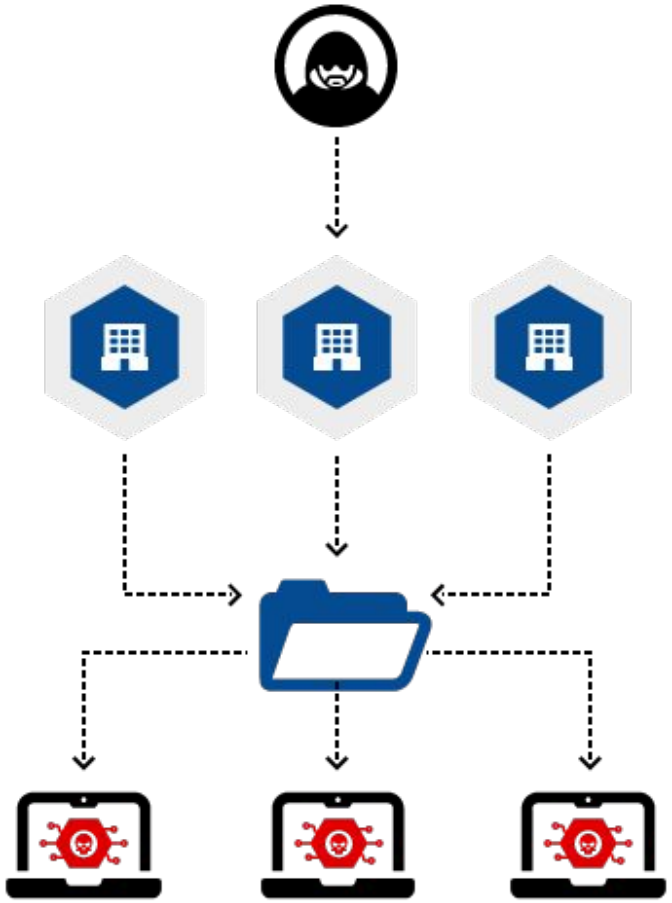
Log4j Vulnerability (CVE-2021-44228)

What is Log4j? A logging utility written in the Java programming language. It is used by administrators within broader systems and web applications versus being a standalone application or program.

How does this vulnerability work? The vulnerability within Log4j allows an attacker to remotely execute code on an impacted system. Successful exploitation of this vulnerability will give an attacker full access to a compromised system.

Why is this vulnerability so critical? Log4j is in widespread use across numerous systems and applications. This vulnerability is particularly concerning because exploitation is trivial, there is publicly available exploit code, and identifying Log4j in enterprise environments may be complex due to its prevalence in embedded applications. Additionally, multiple threat actors are exploiting this vulnerability.

Supply chain



How

A supply chain attack occurs when a threat actor infiltrates your system through an outside partner or service provider with access to your systems and data

Example

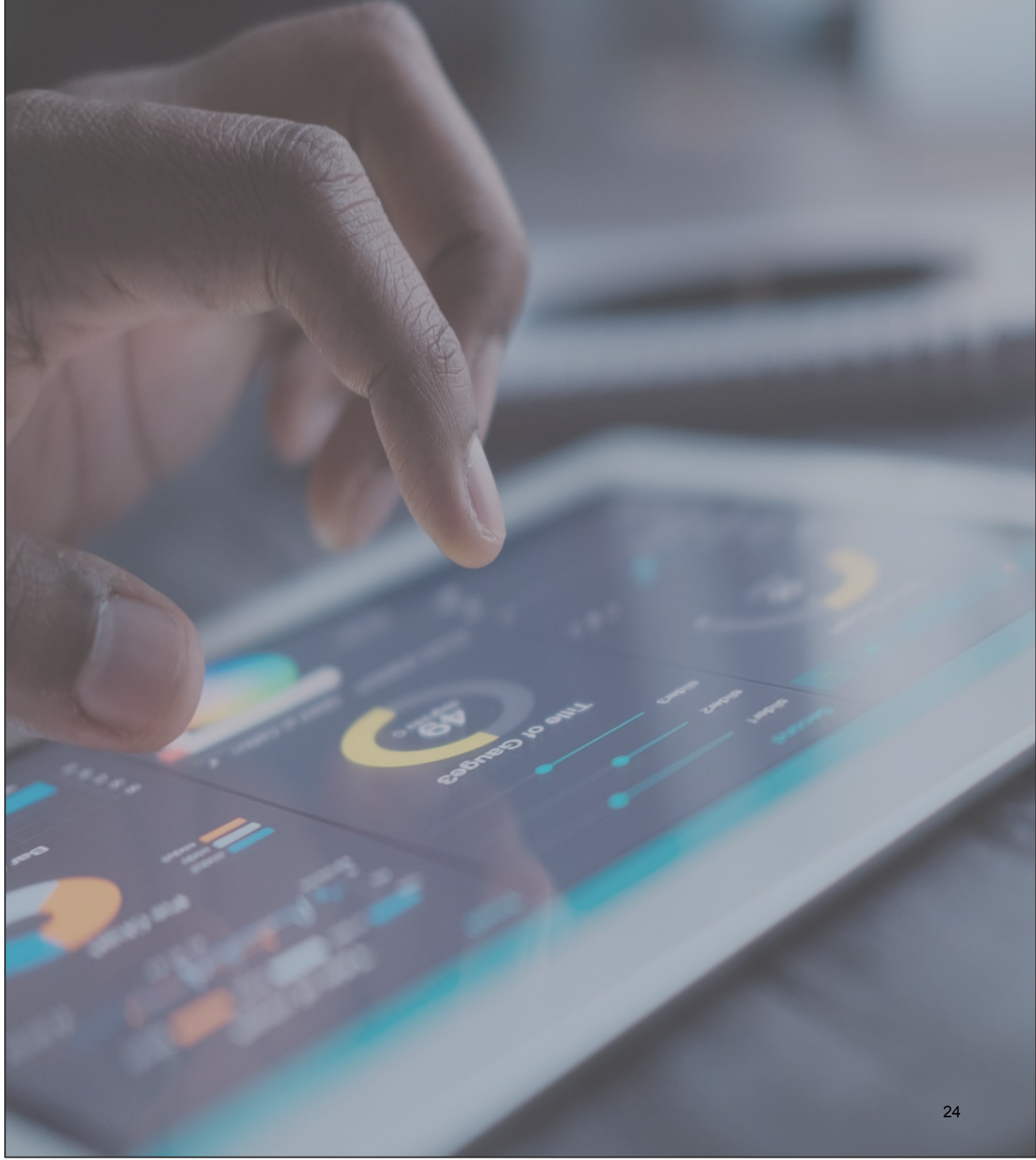
Accellion File Transfer Appliance breach 2021

Late last year, cybercriminals exploited vulnerabilities in Accellion's File Transfer Appliance, which is used to move large and sensitive files within a network, to expose private data such as social security numbers and banking information. The motive of the attack was believed to be for financial gain. Victims who were Accellion's clients were wide ranging, including Federal Reserve Banks, government departments, a leading grocery chain, universities, cybersecurity technology firms, and many more. In Australia this included ASIC and Transport for NSW.

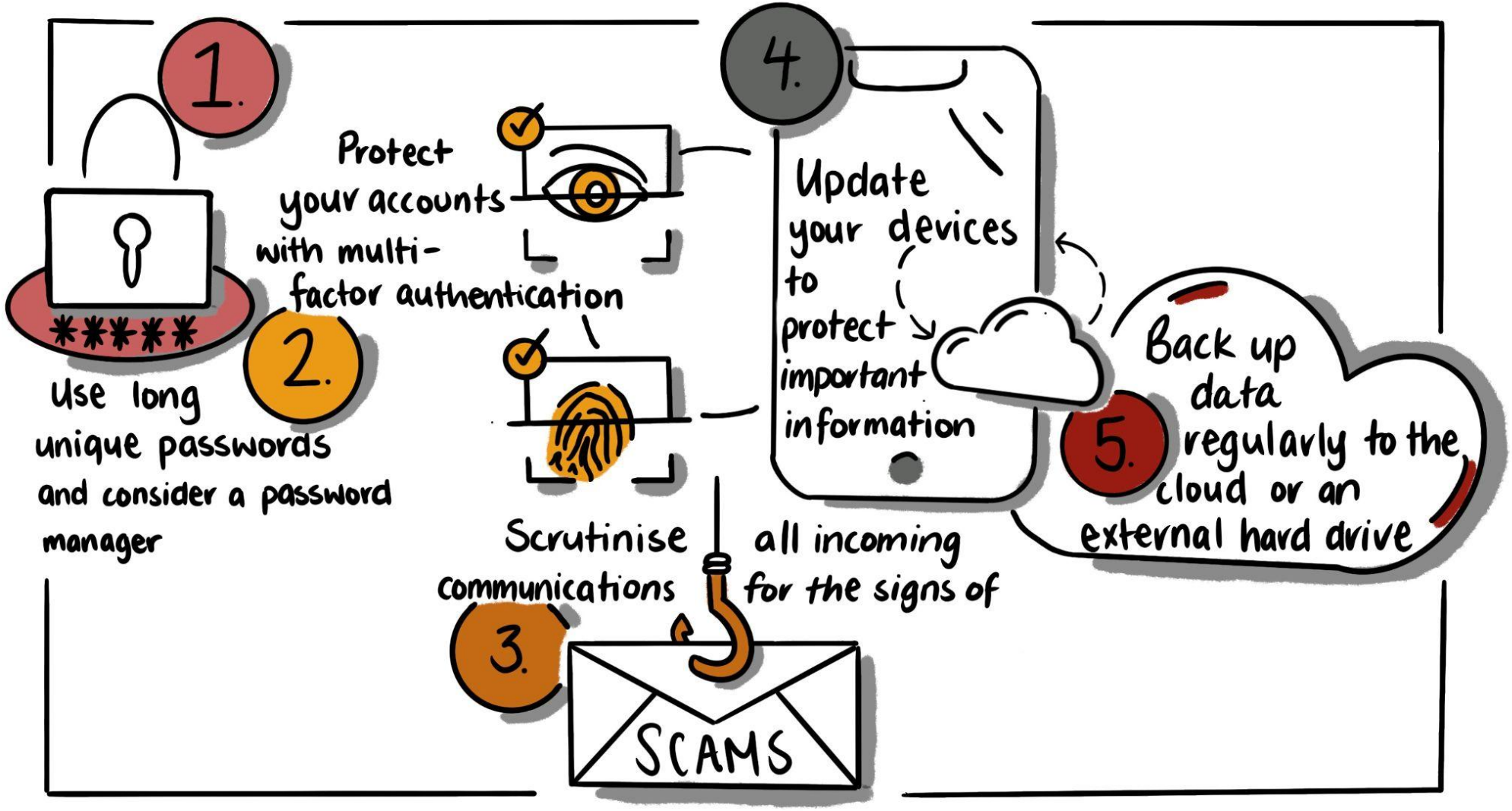
04

Tips and tricks to protect yourself

Poll Question 3



Tips and tricks to protect you, your family and your organisation



Where to find help

Digital Transformation Hub

digitaltransformation.org.au/

ACSC Australian Cyber Security Centre

cyber.gov.au/

Australian Charities and Not-for-profits Commission

acnc.gov.au

Resources for Not For Profits:

https://www.pwc.com.au/about-us/social-impact/privacy-guidelines-for-not-for-profits-nfp.html

Downloadable resources

- Download our Privacy Guidelines for Not-For-Profits (NFPs)
- Download our End User Security Policy Template
- Download our Privacy Policy Template
- Webinar 101 for Not-for-profits
- Information Security Policy template
- IT security register template

05

Q&A

Thank you

pwc.com.au/cybersecurity