# Internal Audit Information Series Cyber

June 2021

pwc

# Agenda

01 Introduction

02 Overview of cyber threat landscape

03 The cyber regulatory landscape in Australia

04 Steps you can take to build cyber resilience

05 Common issues & gaps to be aware of for IA professionals

06 Conversations at the Board Level

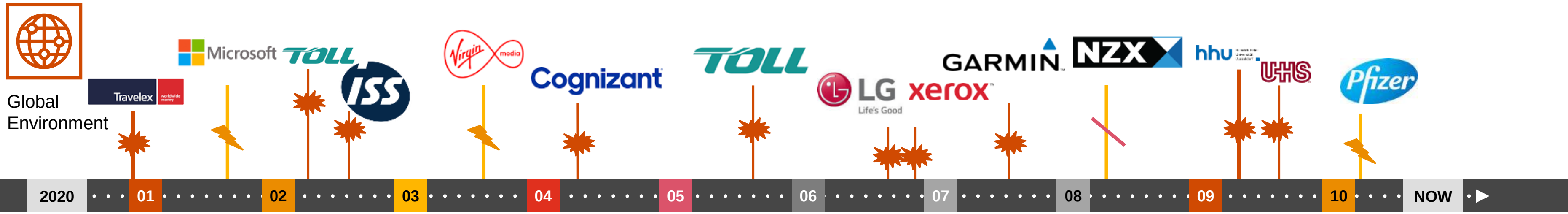
07 Wrap up and Q&A

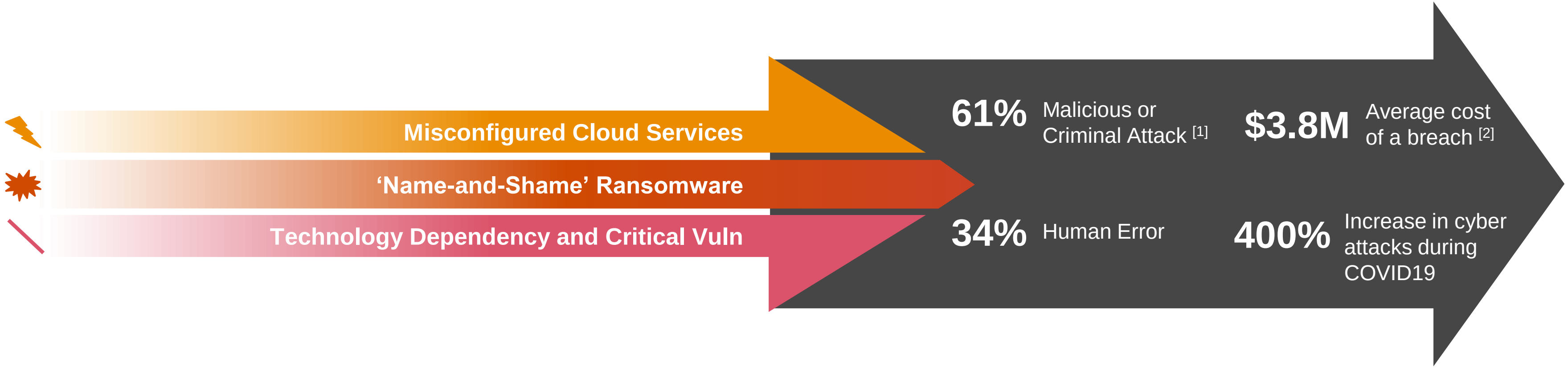
1

# Overview of Threat Landscape

# Cyber Attacks ….The year that was 2020

There has been a proliferation of Cyber threats last year…..





Misconfigured Cloud Services

'Name-and-Shame' Ransomware

Technology Dependency and Critical Vuln

**61%** Malicious or Criminal Attack [1]

**$3.8M** Average cost of a breach [2]

**34%** Human Error

**400%** Increase in cyber attacks during COVID19

# Threat Actors

### 1 Nation State

- National security
- Economic, political, and/or military advantage

### 2 Cyber Criminals

- Immediate financial gain
- Identity theft

### 3 Hacktivists

- Influence social change
- Politically motivated

### 4 Malicious Insiders

- Personal advantage
- Monetary gain
- Professional revenge

### 5 Accidental Insiders

- Not understanding or following processes
- Losing devices
- Laziness

External

Internal

# Digital Trust Insights 2021

## PwC Australia’s Cybersecurity & Digital Trust team

### Key Australian findings from the survey

**60%** reported an intent to **bake cybersecurity and privacy implications into every business decision** or plan off the back of COVID-19, compared with 50% globally

**39%** of executives in Australia say they **accelerated their operations digitisation** plans due to COVID-19, on par with the global figure of 40%

**27%** of Australian respondents say they are **transforming to change core business models** and redefine their organisations, with only 22% undertaking transformation purely for efficiency

**32%** of Australian executives cite **modernisation and accessing new capabilities** as reasons for transformation

**45%** of Australian cyber executives say that they see an **increase in resilience testing** to ensure that if a disruptive cyber event occurs, critical business functions will remain up and running

**Cyber attacks** on cloud services providers are, for **66%** of Australian respondents, considered to be **‘somewhat’ or ‘very likely’ to occur** in their industry in the next 12 months

Poll of 3,249 business and technology executives around the world including Australia in late July 2020.

# Cybersecurity and Director's Duties

## Cybersecurity, a developing focus of ASIC

ASIC are focused on Cyber, and have indicated the management of Cybersecurity risks sit within scope of director's duties. Effective corporate governance should involve active engagement by the board in managing Cyber risks, and ASIC have emphasised that board participation is important to promoting a strong culture of Cyber resilience. ASIC expect a company's approach to Cyber resilience to be proportionate to the risks, nature, scale, complexity and legal/compliance requirements of the relevant business.

## Reliance on information and delegation

In addition to discharging duties, directors should have an adequate understanding of Cyber to ensure they have the benefit of safeguards in the Corporations Act around reliance and delegation. For example, directors should be able to make an independent assessment of information or advice they receive, and make assessments around the reliability and competency of a delegate

## Understanding of issues

Directors have a duty to exercise powers and discharge duties with a degree of care and diligence that a reasonable person would exercise in the circumstances. In the context of Cyber, while directors are not expected to be experts, they should be appropriately informed about the subject matter, the risks and risk profile, and the framework for managing such risks. Directors should feel equipped to oversee and challenge management where necessary.

## "Stepping stone" liability

Personal liability may arise for directors where the company contravenes a law, for example in relation to a Cybersecurity incident, and directors failed to exercise reasonable care and diligence in causing or failing to prevent the contravention where there was a reasonably foreseeable risk of harm to the company (including reputational harm). This is not a duty to ensure the company conducts all affairs in accordance with the law, but a question of liability applying the requirements of directors in discharging their duties.

# 2

# Cyber regulatory landscape in Australia

# Cyber regulation, standards and frameworks

## Relevant Enterprise Security Standards and Frameworks (examples)

- ISO 31000:2018 Risk management
- ISO 22301: 2019 Business Continuity
- AS/NZS ISO 31000:2009 Risk management (NZ)
- FINRA Rule 4370: Business Continuity Plans
- AS/NZS 5050 : Business Continuity Managing disruption-related
- NFPA 1600: Standard on Disaster/Emergency Management and Business Continuity (North America)
- ISO/IEC 27005:2018 Information Technology -- Security
- ISO/IEC 27002:2013/ Information Technology -- Code of practice for information security controls
- The Security of Critical infrastructure Act 2018
- The ASD Information Security Manual (ISM)
- Essential 8 (ACSC)
- The Protective Security Policy Framework (PSPF)
- Payment Card Industry Data Security Standards (PCI-DSS)
- Industry specific frameworks / standards, e.g. APRA, ASIC, ACNC and AESCSF
- NIST (SP) 800-53 (Rev 4)
- NIST cyber security Framework (CSF)
- ISO/IEC 27001:2018
- CERT Resilience Management Model (CERT-RMM)
- MITRE Cyber Resiliency Engineering Framework
- Government Information Privacy Principles (IPP)
- Other state-based regulation (e.g. license conditions for utilities)

## Relevant Security Regulating Bodies & Compliance Initiatives across the Globe

### United States

- Federal Continuity Directive 1 & 2 – requires agencies to establish Continuity Plans and appoint Continuity Coordinator
- NRP – National Response Plan
- National Continuity Policy NSPD 51 / HSPD 20
- National Continuity Policy Implementation Plan
- FPC 60 – Continuity of the Executive Branch of the Federal Government
- USA Patriot Act
- HIPAA (US) Health Insurance Portability and Accountability Act.
- Gramm-Leach-Bliley Act
- Sarbanes-Oxley
- Anti Money Laundering regulations

### UK, EU & Africa

- UK Turnbull Report – requires that anyone listed on the London Stock Exchange has a BCP
- UK Civil Contingencies Bill – Requires persons or bodies listed in the document to assess the risk of an emergency and maintain plans
- FSA – Financial Services Authority (Advanced, Risk – Responsive Operating framework (ARROW)
- Basel I – IV
- MiFID – Markets in Financial Instruments Directive
- Disaster Management Act of South Africa

### Asia

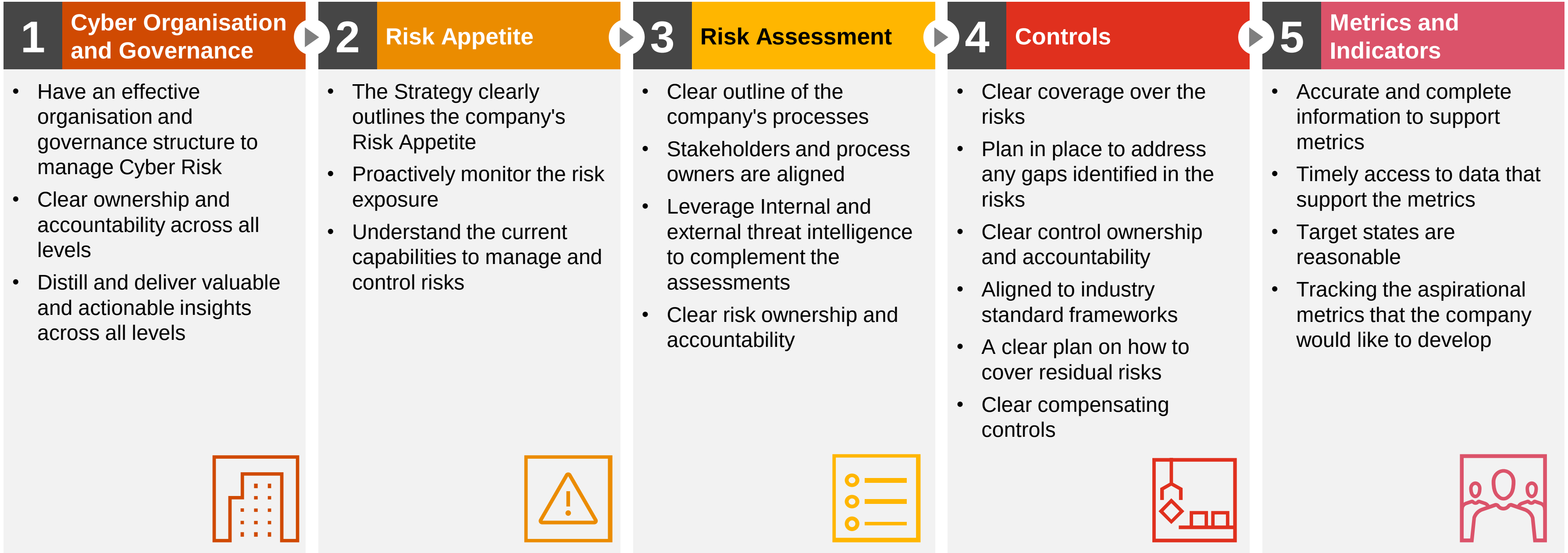
- CBRC – China Banking Regulatory Commission
- CSRC – China Securities Regulatory Commission
- The Hong Kong Monetary Authority
- Monetary Authority of Singapore
- Thailand – Bank of Thailand (BOT) and Stock Exchange of Thailand (SET) mandatory BCM requirements for financial services industry
- India – Requirement for BCPs tested annually across:
  - Reserve Bank
  - Securities & Exchange Board
  - Stock Exchange
- Japan Financial Services Agency

3

# Steps you can take to build cyber resilience

# To mitigate Cyber threats, organisations must have an end to end process for managing Cyber risk

The end to end process helps organisations determine their ability to operate, sustain and continuously improve on managing Cyber risks



## 1 Cyber Organisation and Governance

- Have an effective organisation and governance structure to manage Cyber Risk
- Clear ownership and accountability across all levels
- Distill and deliver valuable and actionable insights across all levels

## 2 Risk Appetite

- The Strategy clearly outlines the company's Risk Appetite
- Proactively monitor the risk exposure
- Understand the current capabilities to manage and control risks

## 3 Risk Assessment

- Clear outline of the company's processes
- Stakeholders and process owners are aligned
- Leverage Internal and external threat intelligence to complement the assessments
- Clear risk ownership and accountability

## 4 Controls

- Clear coverage over the risks
- Plan in place to address any gaps identified in the risks
- Clear control ownership and accountability
- Aligned to industry standard frameworks
- A clear plan on how to cover residual risks
- Clear compensating controls

## 5 Metrics and Indicators

- Accurate and complete information to support metrics
- Timely access to data that support the metrics
- Target states are reasonable
- Tracking the aspirational metrics that the company would like to develop

# Foundational cyber capabilities

## 1 Risk Management and Governance

- Evaluating threat scenarios, identifying potential risks and assessing the impact. Considering whether investment is allocated to the most effective controls.

## 2 Authorised Access Management

- Applying strong authentication mechanisms and monitoring changes to sensitive data.

## 3 User Awareness and Training

- Updating security training and awareness materials in accordance with new developments of the threat environment.

## 4 Incident Detection & Response

- Enhancing the ability to detect and manage cyber incidents and coordinating appropriate response.

## 5 Third Parties (Including Cloud Services)

- Understanding data flows and associated risks with third parties (including cloud services).

## 6 System and Data Protection

- Protecting sensitive information while managing and implementing security controls to current and new systems.

# 4

# Common issues & gaps

# Understanding the Human Factor

2021 – 85% of Data Breaches involved human interaction*

The weakest link in any chain of security is not the technology itself, but the person operating it; iron gates have no compassion to appeal to, nor fears to exploit, nor insecurities to use to one's advantage. They are, however, operated by us – by beings of unlimited vulnerability and limited energy. Why waste time brute-forcing what can be easily circumvented by a clever façade and a crimson tongue?

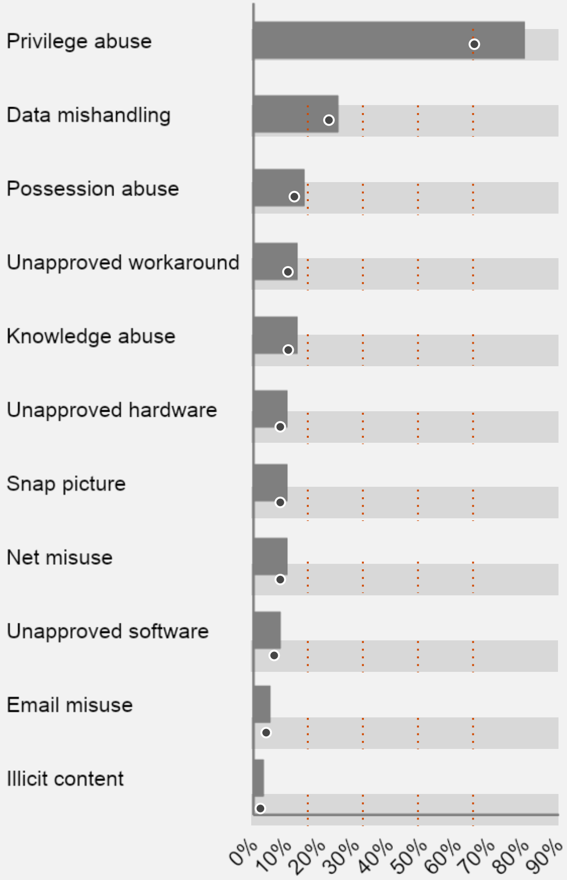
– **A J Darkholme (Canadian Poet and Programmer)**

**The Peltzman Effect**

"The more effort and expense invested in controls to minimise risk, the more likely people are to undertake risky behaviour."

**– Sam Peltzman (Professor Emeritus University of Chicago)**

Source: Verizon Data Breach Investigations report 2021.



# Common and recurring gaps

## 1 Failure to develop appropriate Risk Management:

- ICT/Cyber Risk assessments and management plans
- System Risk Management Plans (SRMP)
- System Security Plans (SSPs)
- Linking activities and strategies to highest risks

## 2 Failure to develop a strategic plan for ICT:

- Including what the organisations ICT looks like 5 years in to the future
- Financial implications and budgets to support the strategy
- Planning for lifecycle management of software and hardware
- Skill sets and skills gaps

## 3 Failing to convey the important and urgency of ICT gaps to the executive:

- Use of plain language in reporting issues (avoid technobabble)
- Link ICT risks to organisational objectives
- Legislative obligations and personal liabilities of executives

## 4 Failing to plan responses to a Cyber event:

- Enabling activation of Business Continuity Plans
- Rapid closing of attack vectors
- Planned communications to stakeholders
- Meeting reporting requirements (eg OAIC for information breaches)
- Retaining evidence for investigations

# Assurance over third party providers

- Increasingly key services for organisations are being outsourced to external third party providers.
- It is reasonable to assume that your provider has Assurance in place.
- Consider at a minimum IT General Controls (ITGCs) as part of all system based internal audits.

ICT enablement

Records and information mgmt

Payment systems

Financial management

Payroll

Procurement

Recruitment

Grants management

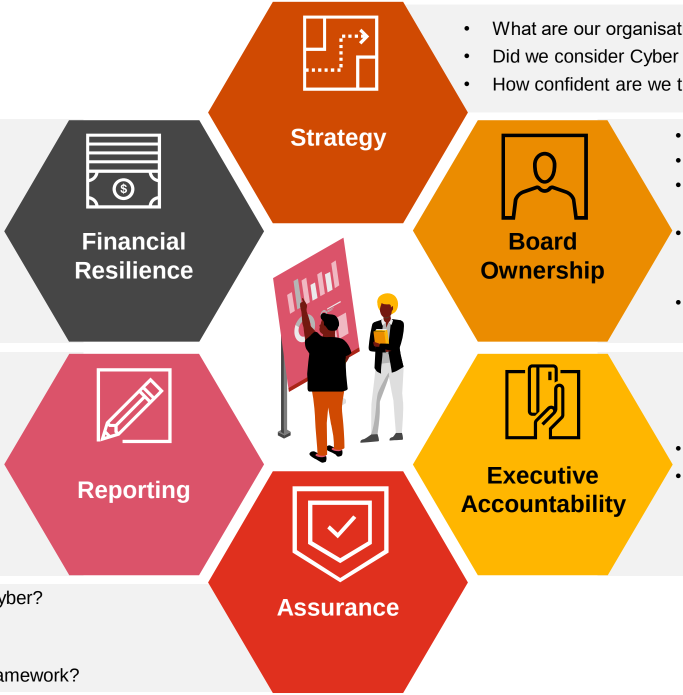
Content management

Customer relationship management

5

# Board level conversation

# Board engagement in Cyber Conversation



### Strategy

- What are our organisation’s current top three Cyber risks?
- Did we consider Cyber risk last time we talked about our digital strategy?
- How confident are we that we understand all the ways we are exposed to Cyber risk?

### Financial Resilience

- What would a $100 million Cyber event be for our organisation?
- How much ($) capital do we reserve for Cyber events?

### Board Ownership

- What is our largest Cybersecurity control gap today?
- Do we know who our most risky 3rd parties are and why?
- To what extent do we consider the impact on our Cyber risk profile in decisions and discussions at board level?
- To what extent are we seeking simplification to reduce operational complexity and make the organisation more secure?
- Do we have the right capabilities to be able to discharge our duties for technology and cyber?

### Reporting

- How is our Cyber risk position and progress reported to the Board? What actions have we taken as a result of your position?
- How aware are we of the actors that are currently attacking our organisation, their interests and how successful they are in breaching our defences?

### Executive Accountability

- What are our responsibilities for Cyber Risk management?
- What would our personal role be in a Cyber incident?

### Assurance

- When was the last independent assurance report done for Cyber? What was the outcome?
- What compliance framework do we use for Cyber?
- How does Cyber fit in with our Enterprise Assurance/Risk Framework?

# Possible focus areas for internal audit – Addressing cyber risk

- Compliance with relevant authority (ACSC, APRA, OAIC, ACNC etc)
- Essential 8 compliance
- Identity and access reviews of framework and User Access Reviews
- Adequacy of Assurance provided by third party providers
- Inclusion of IT General controls, in system specific reviews of (finance, payments, payroll, procurement processes, contract management, grants management) - seeking assurance on ITGCs where these services are outsourced
- Security and safety over data management.
- ICT Disaster Recovery including, preparedness to respond to attacks, such as Ransomware, viruses.
- Information Security and records management – (remote working implications)
- Use of emerging tech (eg AI and machine learning, safety and ethics)
- Approach to management of legacy systems and software
- Project Assurance over change preparedness (eg ICT Projects to migrate to cloud, use smart contact etc)
- Consideration of Operational Technology / Industrial Control Systems where relevant

6

# Wrap up and Q&A

# Thank you

www.pwc.com

PwC refers to the Australia member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.

Liability limited by a scheme approved under Professional Standards Legislation.

At PwC Australia our purpose is to build trust in society and solve important problems. We're a network of firms in 158 countries with more than 250,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at .

WL 127083020