



You know cyber security is more important than ever, but how do you practically identify and plug the gaps

CAANZ May 2024

Today's Presentation – in 60 Seconds

- Key technology risk issues for your firm
- Cyber and incident response procedures
- Our work on recent matters
- Next steps and how we can help you



Cyber is Contextual – Accounting Firms

- Cyber security is one of the major business risks worldwide, with leaders citing cyber attacks and data breaches as the top two risks businesses face.
- Many small and medium businesses (SMEs) face an existential threat from a critical cyber security incident and with the accounting profession growing increasingly reliant on online systems, a cyber security threat is not a question of if, but when.

Cyber Snapshot according to the Accounting Industry

- Cyber threats are increasing, and pose serious and continuous risks to organisations and individuals everywhere.
- Everyone must take responsibility for the data, software and devices we use. One person can bring down a network with a careless error.
- Strengthening your cyber security posture and maturity is a continual iterative process.
- Invest in best-practice security. Cyber threats are a major risk whatever the size of your business or organisation.
- Too few organisations plan both to prevent cyber incidents as well as respond to and recover from them. It's when, not if, they occur.
- Focus on people and process, not just technology. You need people to be aware of threats and with knowledge and skills to respond effectively.

Technology Risk Management



Theft of Information

Hackers and dissatisfied employees try to obtain personally identifiable information (PII), or steal credit card information, customer lists, intellectual property, and other sensitive information.



Password Theft

Attackers steal passwords to access company systems.



Phishing Attacks

Email designed to look like legitimate correspondence that tricks recipients into clicking on a link that installs malware on the system.



Ransomware

Malicious software blocks access to a computer so that criminals can hold your data for ransom.



Natural Disasters

Data loss occurs due to natural events and accidents like fires and floods.



Defacement and Downtime

Attackers force your website or other technology to no longer look or function properly. This could be as a joke, for political reasons, or to damage your reputation

Thinking Ahead. Being Prepared

In October 2018, the New Zealand National Cyber Security Centre (NCSC) published the results of its survey of 250 nationally significant organisations.

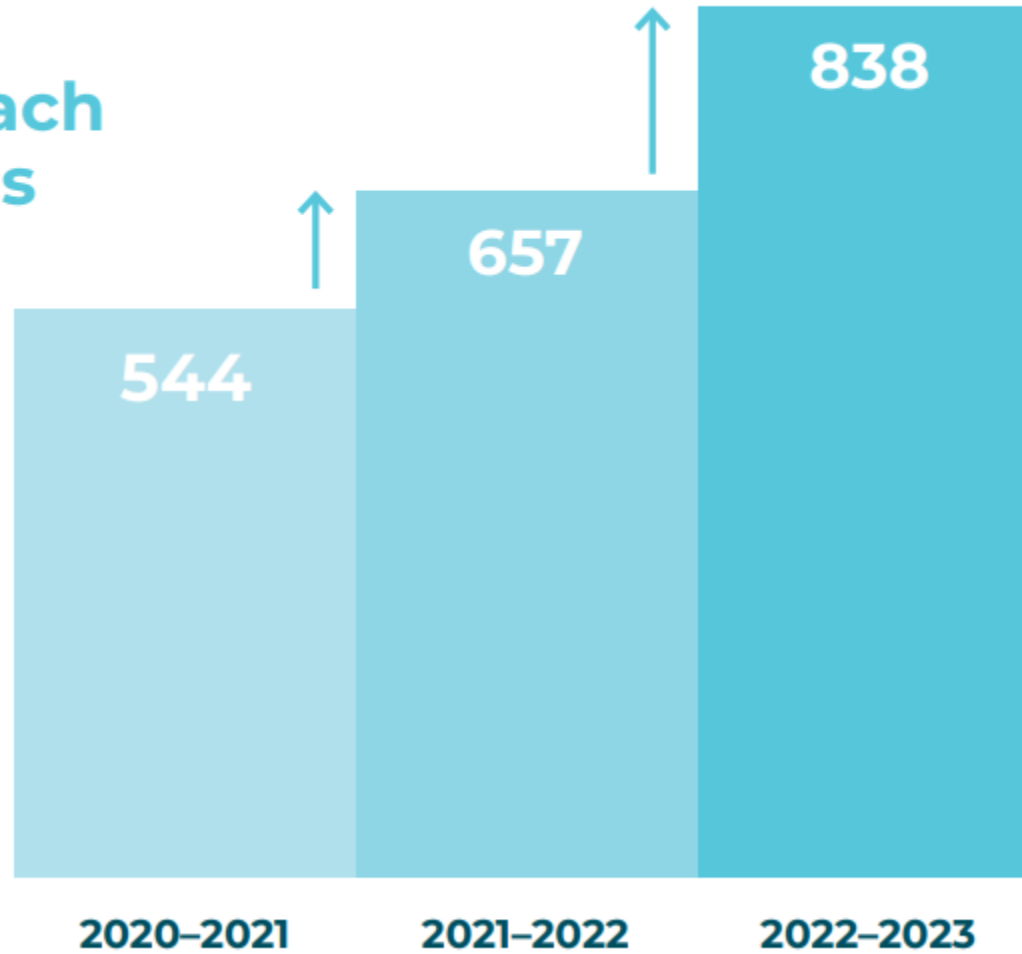
Key findings include:

- i. An area of good practice that was identified is:
Readiness – Preparing the organisation to detect, respond and recover from a cyber-security incident.
- ii. When an organisation becomes aware of an incident, being **ready** to respond can **reduce** its impact of a compromise.
- iii. Having an **up-to-date plan** allows an organisation to react **quickly and decisively** when an incident occurs and serves as a framework to **preserve evidence** in the event legal action is sought following an incident.
- iv. 63% of New Zealand's Nationally Significant Organisations have an incident response plan, but 33% have not **tested their plan** in the last year.

We are proud to be a 100% New Zealand owned and operated business.

OPC Notifications

Number of
privacy breach
notifications



Statistics at a glance

Globally

40+ billion records

exposed by cyber incidents in 2021
78% up on 2020.

\$945 billion

Losses to businesses in 2020
from cybercrime.³

150% increase

in data breaches from a year earlier.

\$145 billion

spent on cyber security by businesses in
2020, more than double 2018.⁴

21,957

common vulnerabilities and exposures²

38%

of data breaches
reported are
ransomware attacks⁵

43%

of cyber
attacks target
small business.⁶

Australia⁷

\$33 billion

Losses to cybercrime by Australian
businesses in the 2020-21 financial year.

67,500 cybercrime reports

An increase of nearly 13% from the
previous financial year.

25% of cyber security incidents

responded to by the Australian Signals
Directorate last year were against critical
infrastructure, such as energy, water,
telcos and health.⁸

22,000 calls received

by the Cyber Security Hotline, an average
of 60 per day and an increase of more
than 310% from the previous financial year.

New Zealand

28%

The number of cyber incidents in New
Zealand linked to foreign state-sponsored
computer network exploitation groups.⁹

404 cyber incidents

Nationally significant organisations
impacted in the 2020-21 financial year, a
15% increase from a year earlier

8,831 incidents reported

The number of incidents reported
to CERT NZ in 2021, a 13% increase on
2020¹⁰

² [Tenable website](#). These figures are for the year to October 2021 and are based on an analysis of publicly disclosed information

³ [McAfee Hidden costs of cyber crime](#)

⁴ McAfee

⁵ [2020-2021 NCSC NZ Cyber Threat Report By the Numbers](#)

⁶ [PurpleSec 2021 Cyber Security Statistics The Ultimate List of Stats, Data & Trends](#)

⁷ [ACSC Annual Cyber Threat Report 2020-21](#)

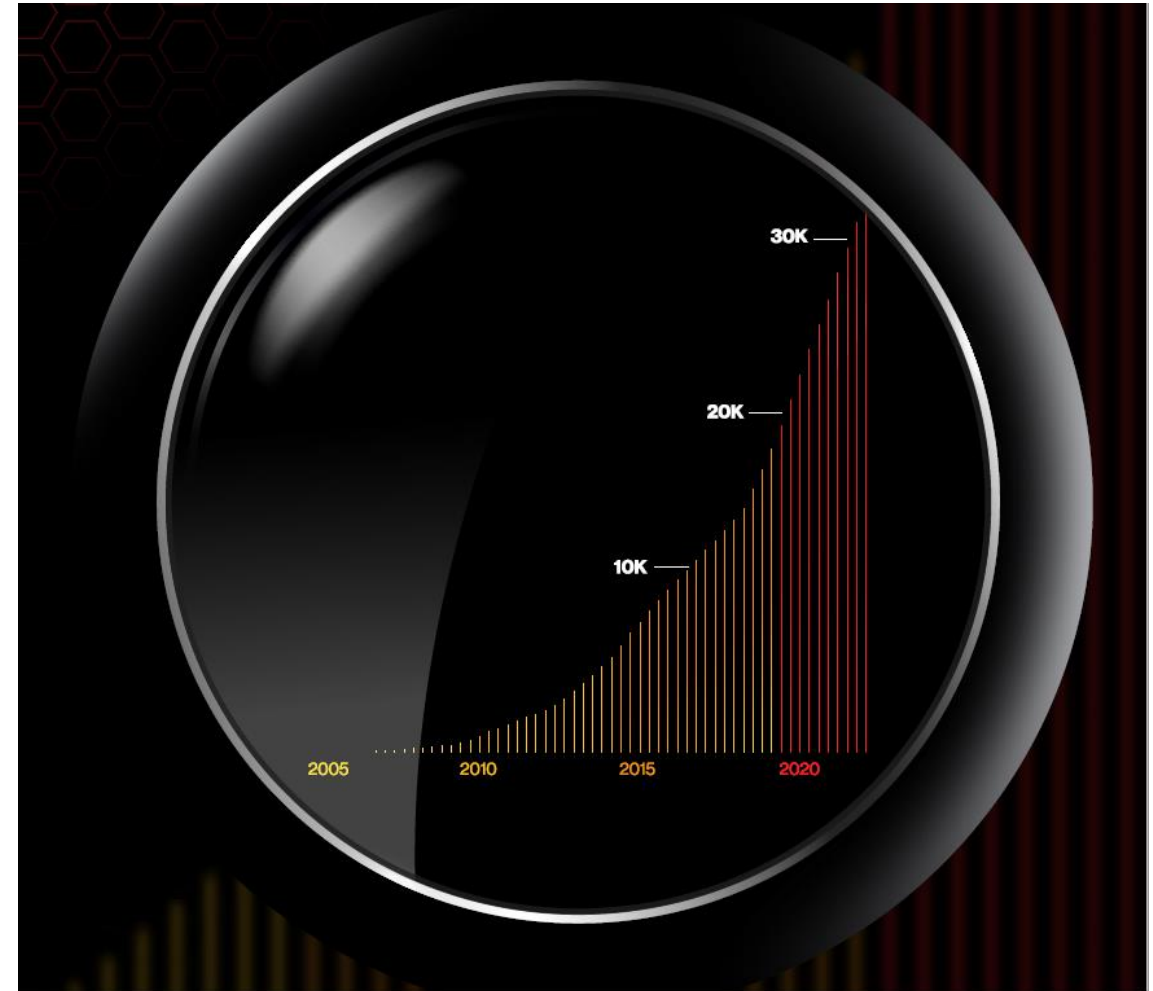
⁸ [Australian Signals Directorate website](#)

⁹ NCSC

¹⁰ CERT NZ's [Quarter Four \(Q4\) Report](#)

Verizon Data Breach Investigations Report (16th Edition)

- 16,312 security incidents that compromised the integrity, confidentiality or availability of an information asset.
- 5,199 breaches that resulted in the confirmed disclosure of data to an unauthorised party.
- *Total Set*
 - 953,894 incidents
 - 254,968 breaches



What Verizon Found – Key Statistics

- **74%** of all breaches include the human element
Error, Privilege Misuse, stolen credentials or Social Engineering
- **50%** of all Social Engineering incidents used pretexting
An invented scenario that tricks someone, that may result in a breach
- **24%** of all breaches involved ransomware
Maliciously encrypting data and demanding a ransom to return or unlock it
- **19%** involved internal actors
Intentional and unintentional harm through misuse and simple human errors
- **95%** of breaches are financially driven
It's (almost) always about the money

What is Social Engineering



Social engineering is when an attacker gains a person's trust and tricks them into giving them access or information they shouldn't have; or

Researches a person and gets enough information to be able to either guess their passwords or get them reset.



WIKIPEDIA
The Free Encyclopedia

In the context of information security, social engineering is the psychological manipulation of people into performing actions or divulging confidential information.

A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme.

Social engineering attacks

Firms are frequently targeted because:

- They are perceived as wealthy
- Firms receive, control and process large sums of money
- Clients often have accounting firms act for them

Most of our cyber incident response work is conducted within the professional services sector, including Business Email Compromise and Ransomware, often perpetrated via Social Engineering.

Research



Attackers identify targets and objectives and get a list of email addresses.

Phishing page



The attacker creates a phishing page by compromising a domain or using a similar domain name to a common brand.

Email sent



The email targets are sent a message to trick them into visiting the website.

Request actioned



The target enters information into the phishing page (credentials information) or is tricked into downloading malware.

Information harvested



The attacker uses information in attacks or sells it. Attackers use malware to steal information or money, or to use the computer for other attacks.

Current Ransomware Activity

Welcome to  RansomLook  !

May 9Th, 2024

Currently tracking **188** groups across **336** relays & mirrors - **74**
currently online

There have been **18** posts within the last 24 hours

There have been **219** posts within the month of may

There have been **1382** posts within the last 90 days

There have been **1781** posts within the year of 2024

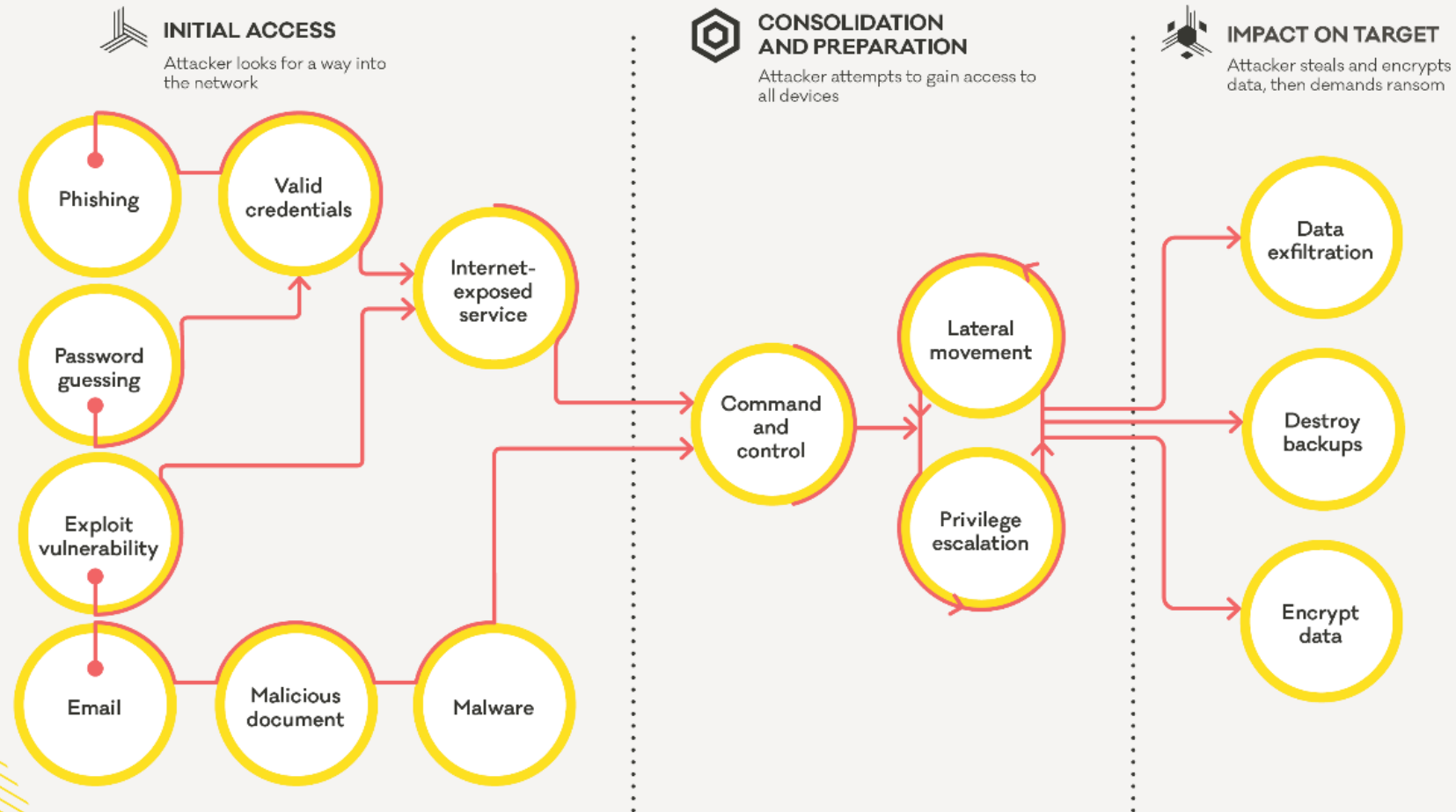
There have been **13851** posts since the dawn of ransomlook

There are **111** custom parsers indexing posts

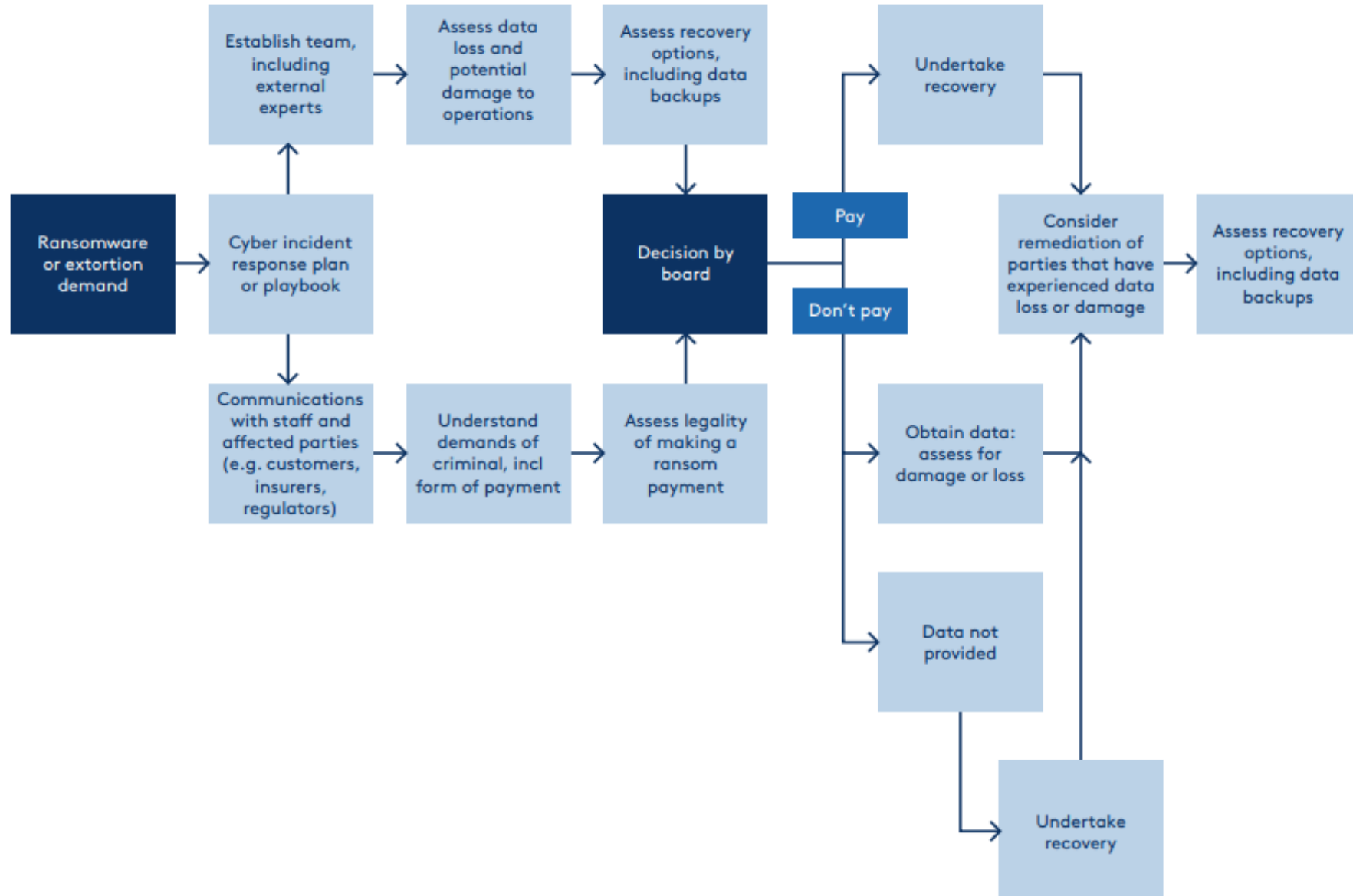
LIFECYCLE OF A RANSOMWARE INCIDENT



The common attack paths of a human-operated ransomware incident based on examples CERT NZ has seen.



Example Ransomware Decision Making Process - AICD



Technology Supply Chain Management



The House Loses: Caesar's Entertainment paid a ransom after being cyberattacked. GETTY

Within weeks, two of the world's largest casino-hotel companies—MGM Resorts and Caesars—were hit with ransomware attacks. One met the hackers' demands, while the other is resisting.

ALPHV reportedly bragged that it took 10 minutes to infiltrate MGM's system after identifying an MGM tech employee on LinkedIn and then calling the company's support desk.



























Scattered Spider gained entry to Caesars' system by deceiving an employee at a third-party vendor.

Cyber Governance and Risk Management - Controls

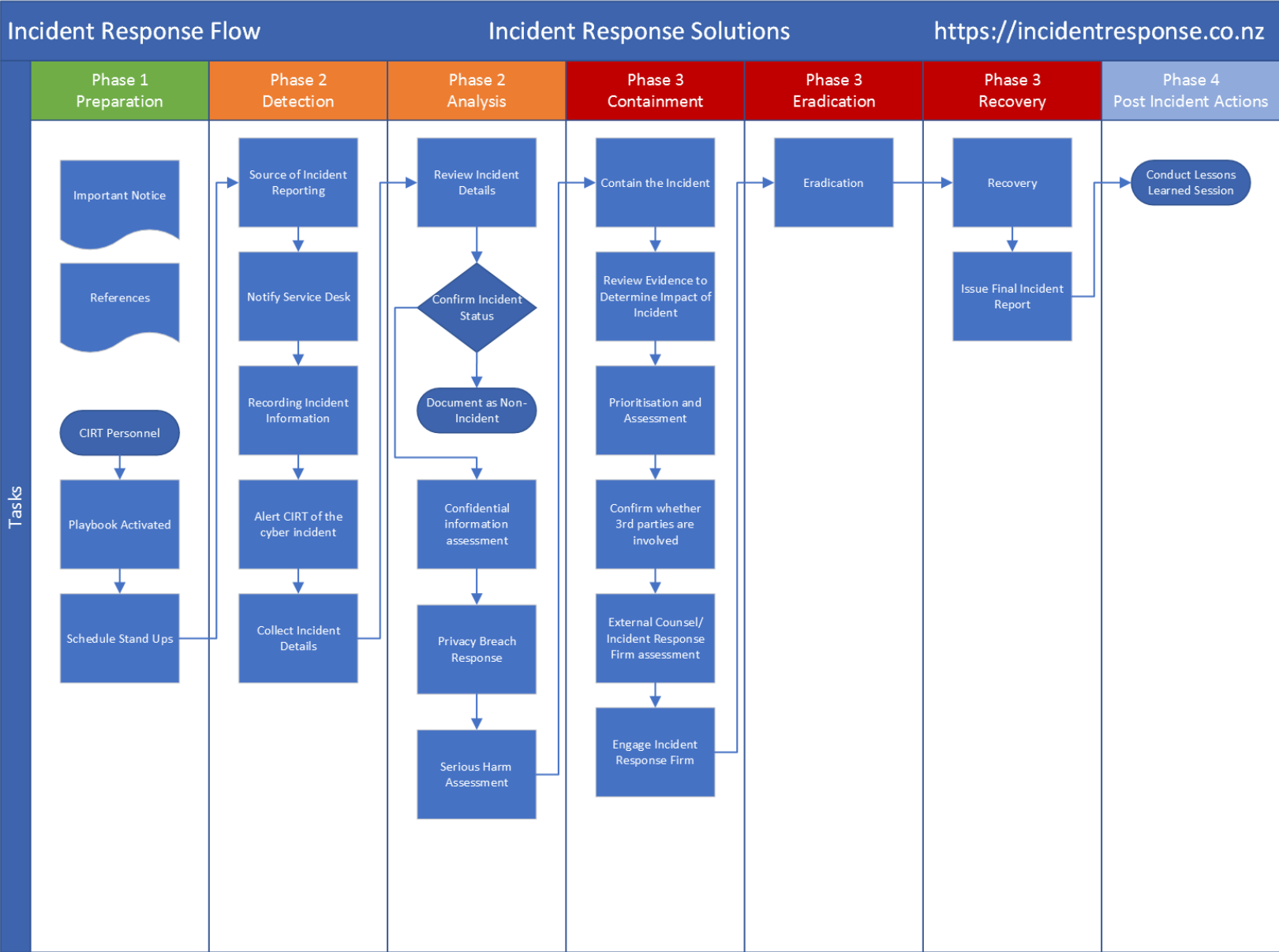


Cyber Risk Management – Security Awareness and Skills Training

14 Security Awareness and Skills Training

14.1	Establish and Maintain a Security Awareness Program			
14.2	Train Workforce Members to Recognize Social Engineering Attacks			
14.3	Train Workforce Members on Authentication Best Practices			
14.4	Train Workforce on Data Handling Best Practices			
14.5	Train Workforce Members on Causes of Unintentional Data Exposure			
14.6	Train Workforce Members on Recognizing and Reporting Security Incidents			
14.7	Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates			
14.8	Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks			
14.9	Conduct Role-Specific Security Awareness and Skills Training			

Incident Response Plans and Simulations



What services are clients engaging in

- Cyber Governance
- Cyber IR plans and testing
- Breach response
 - Incident controller
 - Data Breach assessment (DART)
 - Communications
 - Ransomware response
 - Dark web and data leak monitoring
- Forensic technology
- Hosting / eDiscovery / GPT “ASK”



Further Resources

CA ANZ

- [Why CFOs should take the lead on cyber security](#)
- [Cyber and the CFO](#)
- [Protect our cyber future](#)
- [Cyber security for SMEs and practitioners](#)

Standards

- [ISO 27001](#) is an internationally recognised Information Security Management System (ISMS) standard.
- [National Institute of Standards and Technology \(NIST\) Cyber Security Framework](#)

New Zealand

New Zealand Cyber Security Centre

- [Guides | CERT NZ](#)
- [Charting Your Course](#)

New Zealand RASCI approach to cyber security

- [A Guide to the Project Management Body of Knowledge \(PMBOK Guide\) \(5th ed.\) Project Management Institute.](#)

United Kingdom

UK's National Cyber Security Centre (NCSC)

- [10 Steps to Cyber Security 2021](#)
- [Small Business Guide 2020](#)

Singapore

The Singapore Government's Cyber Security Awareness Alliance Go Safe Online website [SMEs](#)

Australia

Australian Cyber Security Centre

- [Small & medium businesses Cyber.gov.au](#)
- [Essential Eight](#)

Australian Tax Office resources

- [Top cyber security tips for businesses | Australian Taxation Office](#)
- [How to prepare for a cyber security incident | Australian Taxation Office](#)

Australian Government Department of Business

- [Create a cyber security policy](#)

Office of the Australian Information Commissioner

- [About the Notifiable Data Breaches scheme](#)

Australian Securities and Investments Commission

- [Cyber resilience good practices | ASIC - Australian Securities and Investments Commission](#)

United States

US's National Institute of Standards and Technology

- [Framework for Improving Critical Infrastructure Cyber Security, 2018](#)

Assessment Tool

- [Self-assessment tool](#) compiled by Continuum Cyber for CA ANZ

Reporting Obligations

Office of the Australian Information Commissioner

- [About the Notifiable Data Breaches scheme](#)
- [Australian Privacy Principles](#) listed in the Privacy Act of 1988

New Zealand, the Privacy Act 2020

- [Principle 5](#)

Thank you

Campbell McKenzie

0800 WITNESS or 021 779 310
campbell@incidentresponse.co.nz

incidentresponse.co.nz
whistleblowers.co.nz

<https://incidentresponse.co.nz/demos>
Password: *Bulletin*

