Cyber Incident Response

NZ Law General Meeting

March 2024

Todays 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

Checked your Voicemail

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.

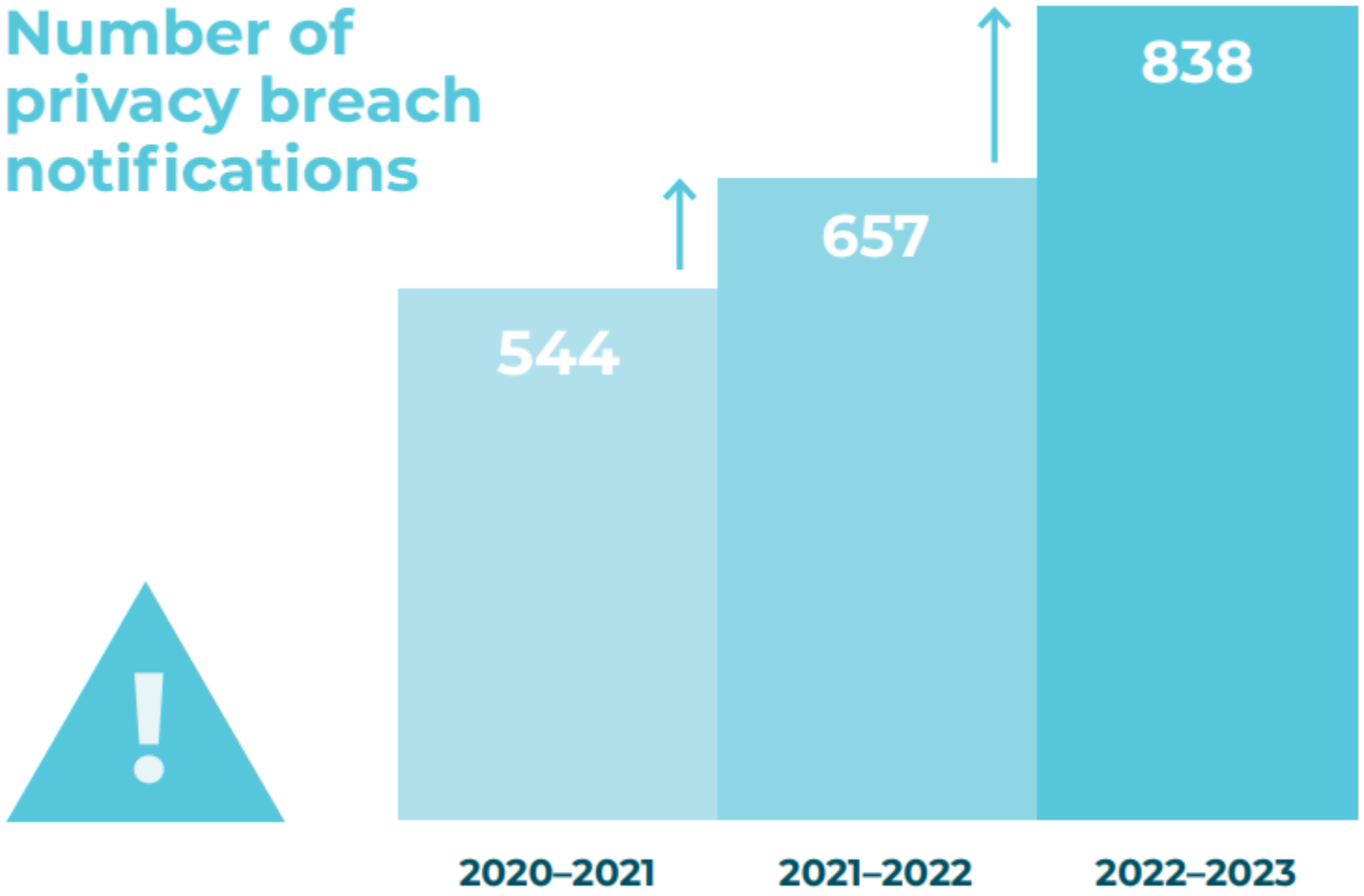
ii. When an organisation becomes aware of an incident, being **ready** to respond can **reduce** its impact of a compromise.

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



Cyber is Contextual – Law Firms

- Confidentiality
- Integrity
- Availability

Law Firm Cyber Security at a Glance

More than a quarter of law firms experienced a data breach. (*The American Bar Association's 2019 and 2022 Legal Technology Survey Report)*

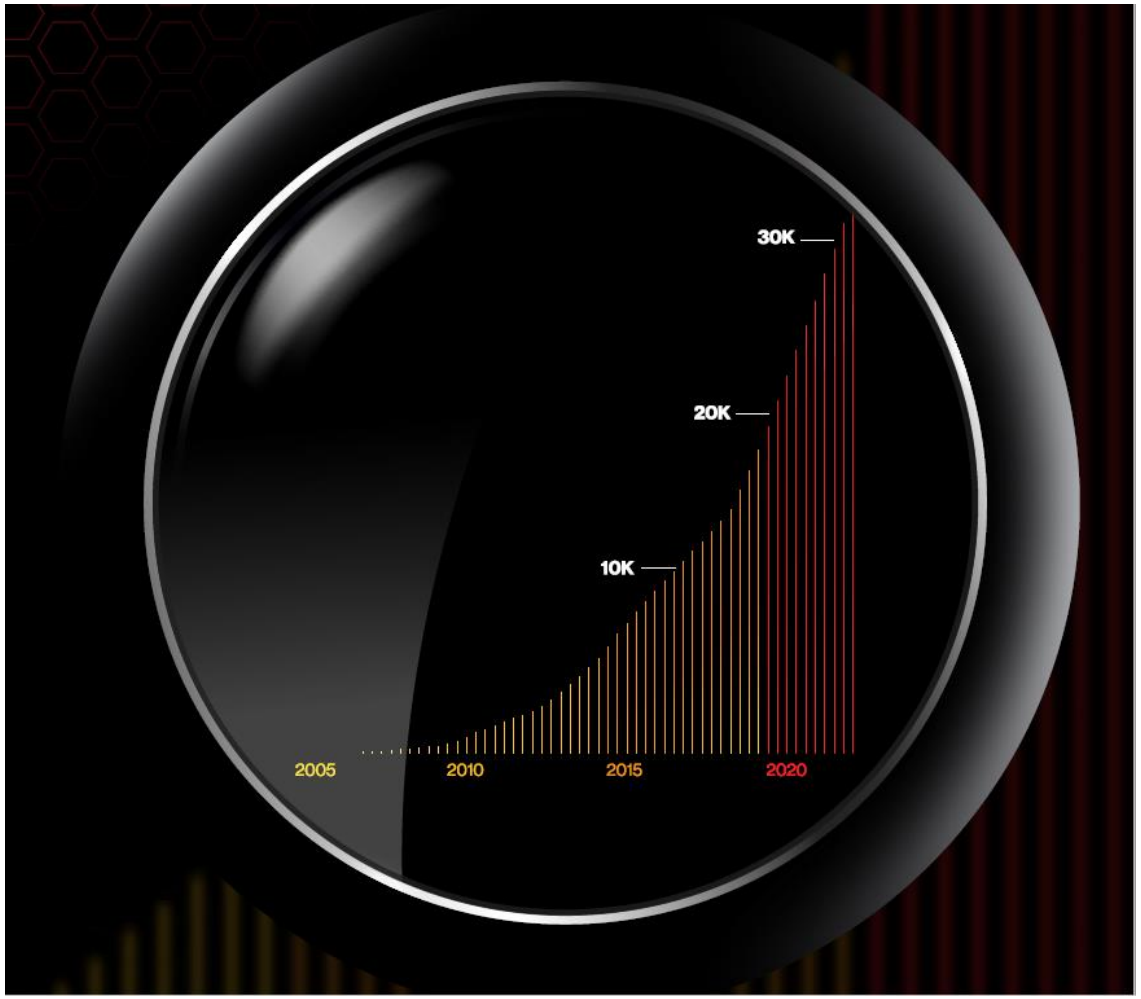
Every respondent suffered a security incident, with the most common attack being phishing. (*2019 Survey of Global Law Firm)*

The most significant cyber threats to a law firm are phishing, data breaches, ransomware and supply chain compromise. (The *UK's National Cyber Security Centre 2018 Report)*

Total or partial outsourcing of services and the use of automation and robotics to assist with repeatable activities using third-party services are both increasing. (*The Cyber Threat to UK Legal Sector 2018)*

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*



verizon.com/dbir

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

WIKIPEDIA
The Free Encyclopedia

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.

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.

Why are social engineering attacks targeting law firms?

Law firms are frequently targeted because:

- They are perceived as wealthy
- Law firms receive, control and process large sums of money through trust accounts accounts
- Clients often have law firms act for them

Most of our cyber incident response work is conducted within the legal 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

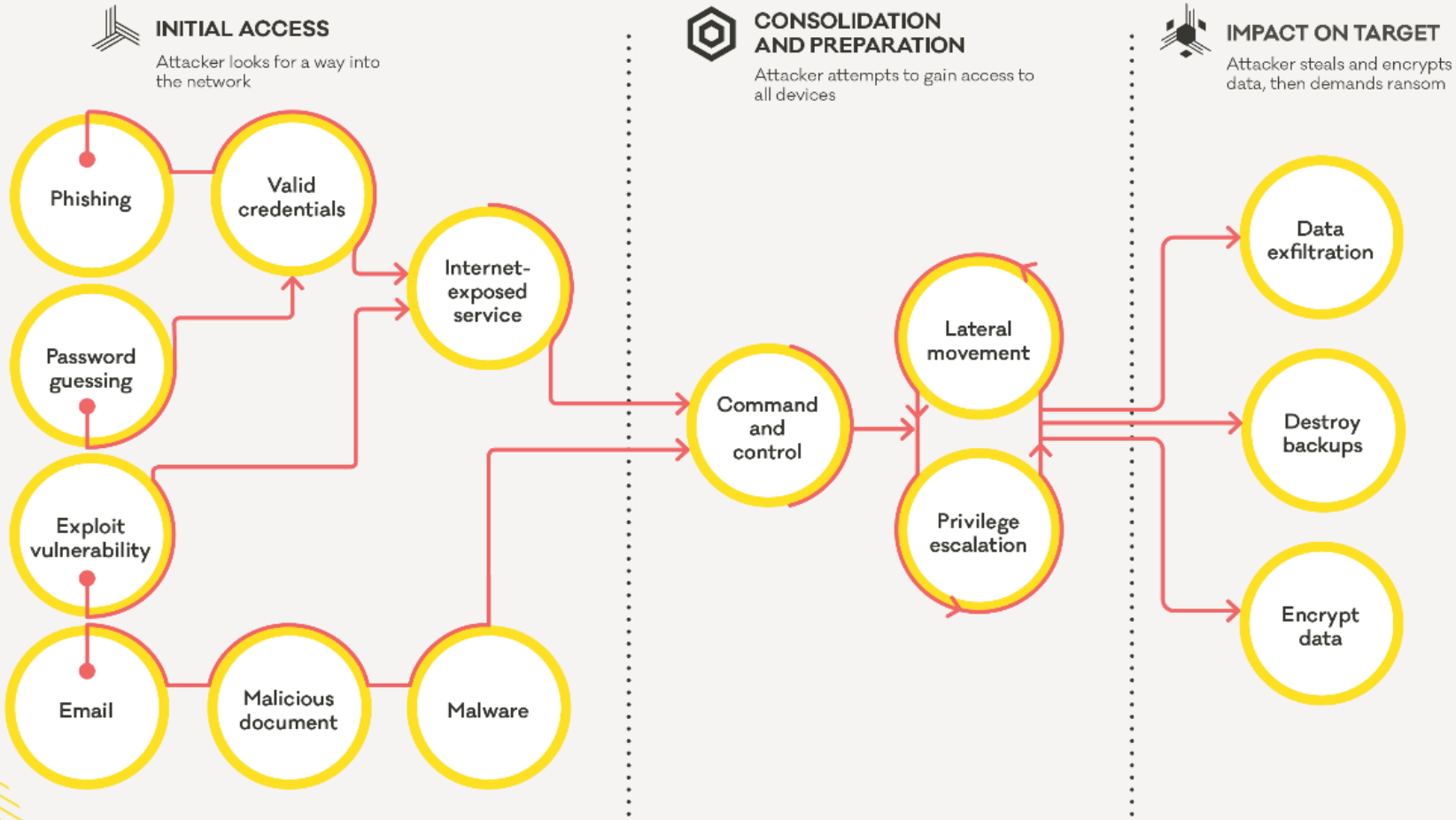
The attacker uses information in attacks or sells it. Attackers use malware to steal information or money, or to use the computer for other attacks.

Social engineering example

LIFECYCLE OF A RANSOMWARE INCIDENT

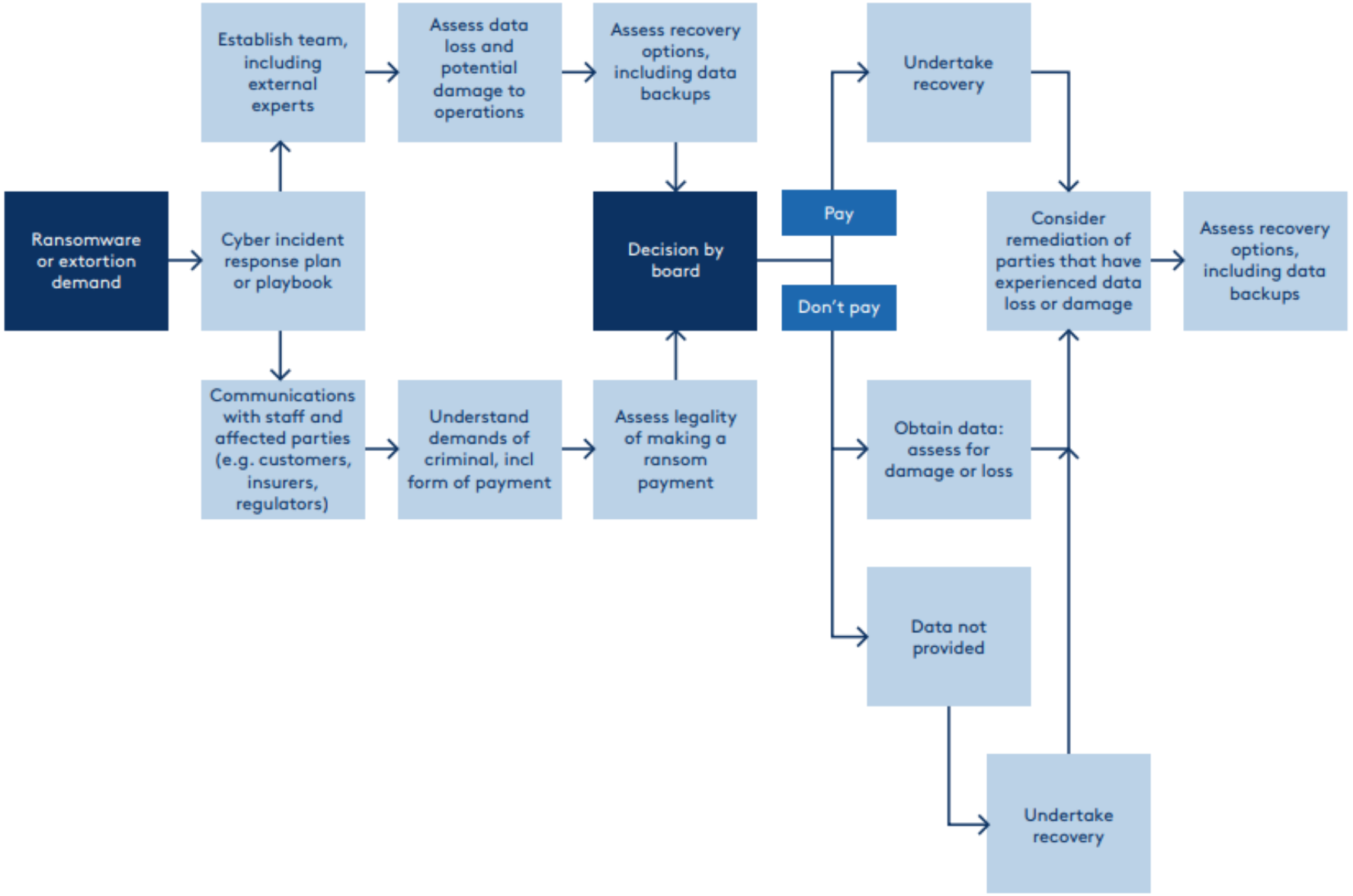
certnz

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



New Zealand Government

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 Incident Response for Law Firms - Poll

Poll 1 – Cyber security

- Understand the impact
- Mitigated the risks
- Sleep at night

Poll 2 – Incident response

- Plan
- Test
- Improve

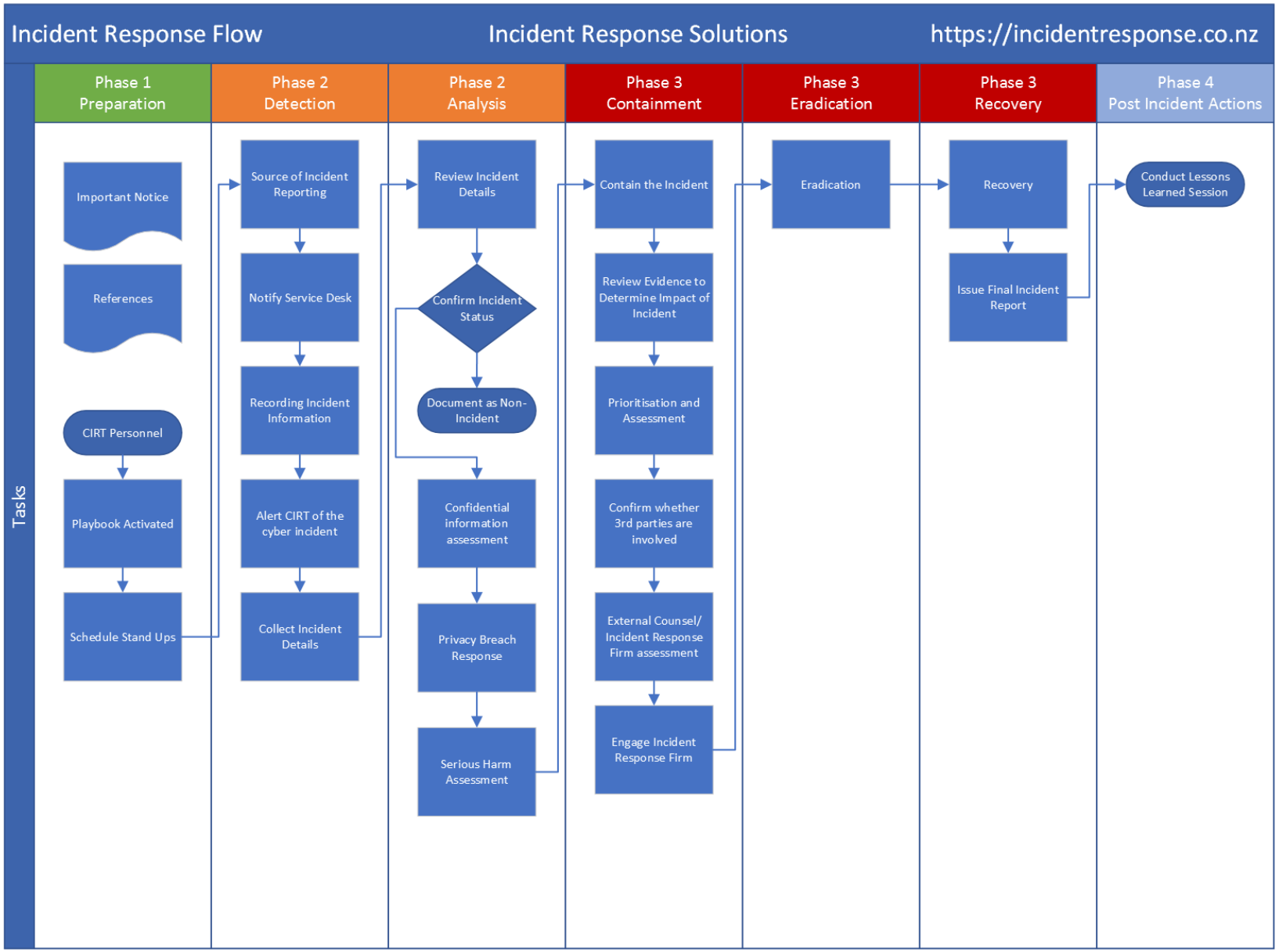
Cyber Governance and Risk Management - Controls

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



IRS – Document Analysis Review Tool

reveal | brainspace

Evidence of Identity Standards - Example

New Zealand Birth Certificate

Purpose

A New Zealand Birth Certificate is an official document containing registered information about a person's birth as at the date of issue.

Quick steps

Over the years there have been a number of different designs and layouts of the New Zealand Birth Certificate.

Check that the certificate has been stamped with a Registrar's seal, or signed by the Registrar, or have both the Registrar's seal and signature.

Check for watermark. From 1985 certificates contain a 'black wave watermark' visible when the certificate is held up to the light. From late 2011 certificates have a watermark of a kiwi and two ferns visible when the certificate is held up to the light and there is a red map of New Zealand in the bottom right-hand corner.

Check paper and embossing. Between late 2011 and mid 2017 certificates were printed on glossy paper.

Check registration number. From 1 October 1999 certificates will have a 10-digit registration number. The first four digits will usually be the year of birth or a subsequent year.

Information

Information contained in the document includes:

- Registration number

Child details

- Given name(s) and surname(s)
- Given name(s) and surname(s) at birth*
- Sex
- Still-birth/Multiple birth (if applicable)
- Date of birth
- Place of birth
- New Zealand citizen by birth**
- Name changes (if applicable)

Details for each parent

- Given name(s) and surname(s)
- Given name(s) and surname(s) at birth*
- Date of birth
- Place of birth

* If name has changed

** All certificates issued on or after 01/01/2006 will contain one of the following: Yes, No or Not applicable to births that occurred prior to 01 January 2006.

Evidence of Identity Standards – Example (Saved Searches)

HR62 - "i whanau kahu mai"	2023-04-16
HR62 - "ingoa tapa i te whanautanga mai"	2023-04-16
HR62 - "first/given name(s) at birth"	2023-04-16

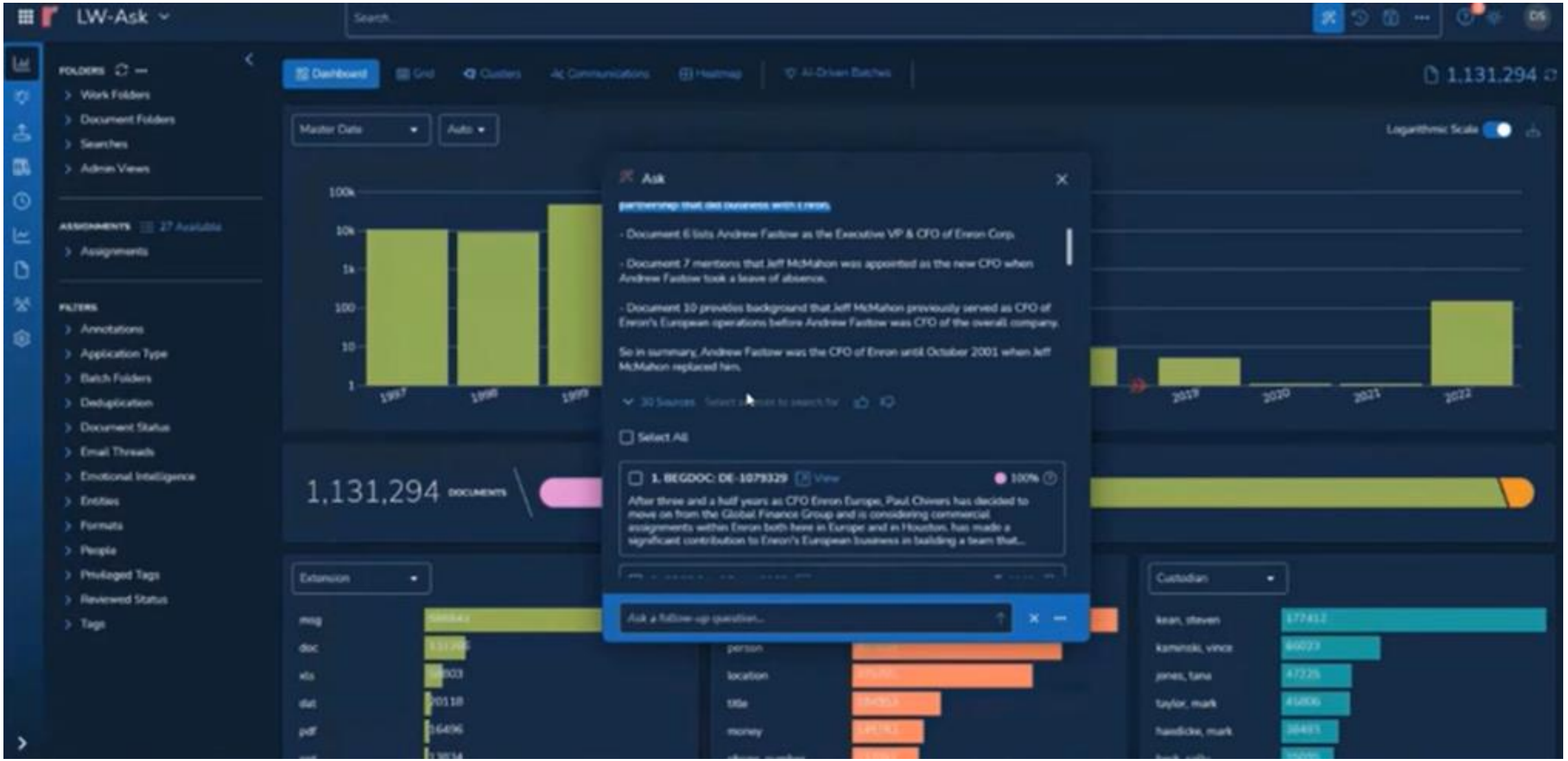
IS (

IS **Keyword:** "ingoa tapa i te whanautanga mai"

)

WARNING: THIS CERTIFICATE IS NOT EVIDENCE OF THE IDENTITY OF THE PERSON PRESENTING IT
KIA TOPATO: EHARA TA TENEI TIWHIKETE i TE TAUNAKI i TE TUAKIRI 0 TE TANGATA KA TAPAE ATU
Certified to be a true copy of the above particulars included in an entry recorded in this office.
E pono ana te kT he tauira tuturu tenei o nga korero o runga ake nei kua tuhia ki tetahi puka i tenei tari.
* If name has changed / Mena kua rereke te ingoa
** If different from above / Mena he rerekS ki tera o runga ake
Issued under the seal of the Registrar on 7 July 2004
i tukuna i raro i te maru o te Poutoki i te 7 Hongongoi 2004
Surname/family name at birth**
Ingoa whanau i te whanautanga mai**
Surname/family name at birth**
Ingoa whanau i te whanautanga mai**
First/given name(s) at birth*
Ingoa tapa i te whanautanga mai*
Date of birth
Te ra i whanau ai
Place of birth
Te wShi i whanau ai
Occupation, profession or job

Generative Pre-training Transformer (GPT) - ASK



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”

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*

Incident Response
FORENSIC & CYBER