Cyber Governance: A Legal Perspective and Best Practices

Chilli IQ – LawTech Forum NZ
June 2025

Incident Response
FORENSIC & CYBER

Todays Presentation – in 60 Seconds

- Balancing technology transformation and cyber risk management
- Cybersecurity controls that you need in your practice
- Keeping your data secure, lessons from the increasing cyber landscape targeting New Zealand law firms
- Incident response
- Latest advancements in document analysis and review tools

Cyber Risk Management

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

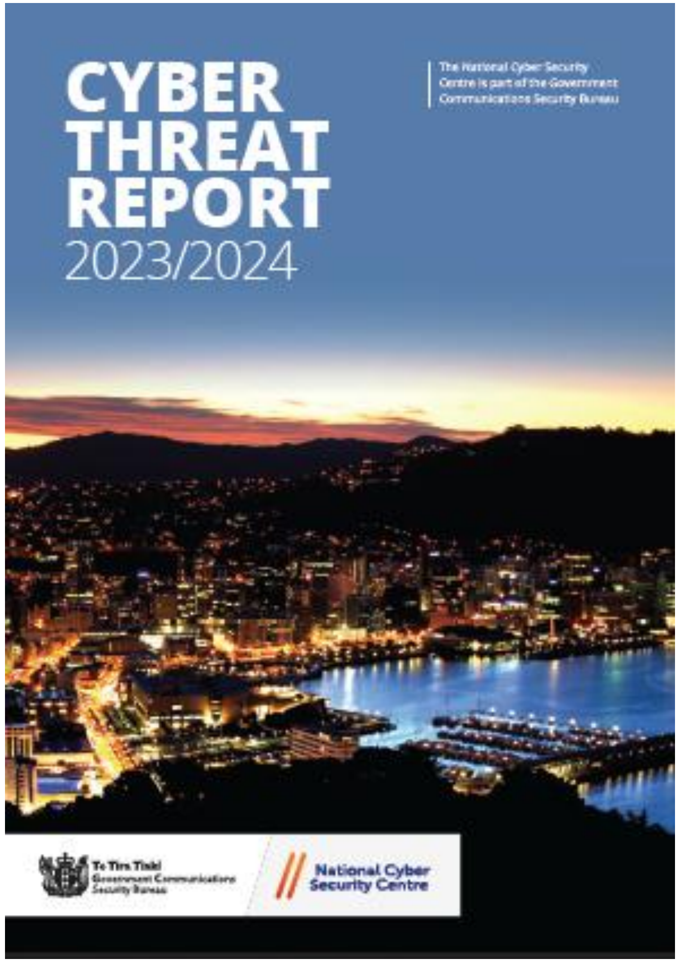
Data loss occurs due to natural events and accidents like fires and floods.

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

https://www.cisecurity.org/controls

Cyber Snapshot



CYBER THREAT REPORT 2023/2024

The National Cyber Security Centre is part of the Government Communications Security Bureau

Te Tira Tiaki Government Communications Security Bureau

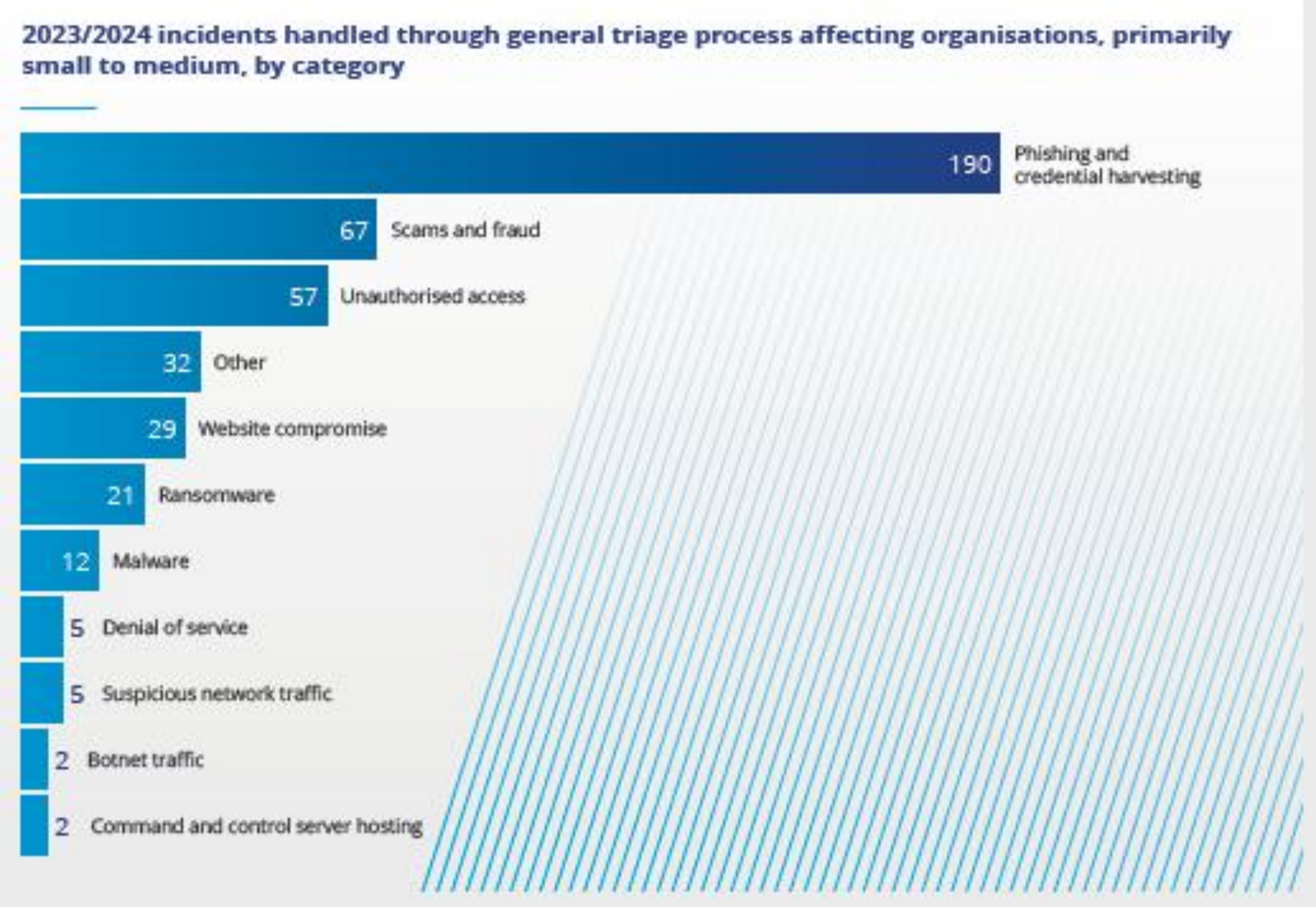
National Cyber Security Centre

The NCSC in a typical month:

- Detected 7 cyber incidents affecting one or more nationally significant organisations through the NCSC's cyber defence capabilities.
- Received 22 new incident reports or requests for assistance for incidents of potential national significance.
- Recorded 565 incidents handled through the NCSC's general triage process, often affecting individual New Zealanders and small to medium businesses and organisations.

https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-Cyber-Threat-Report-2024-FINAL.pdf

Cyber Snapshot



https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-Cyber-Threat-Report-2024-FINAL.pdf

CISA Risk and Vulnerability Assessment

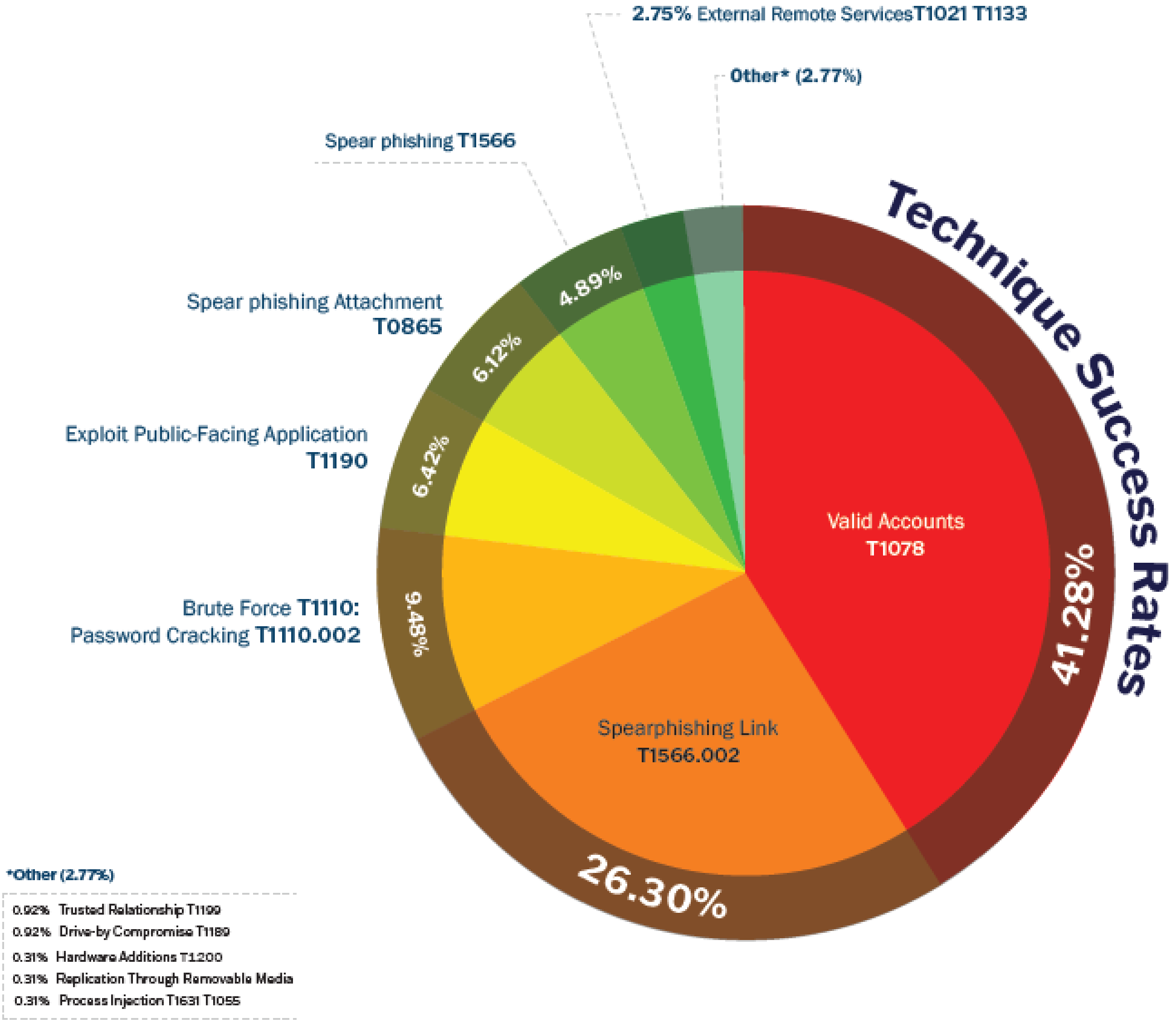
FY23 RVA Results

MITRE ATT&CK™ TACTICS AND TECHNIQUES

Initial Access

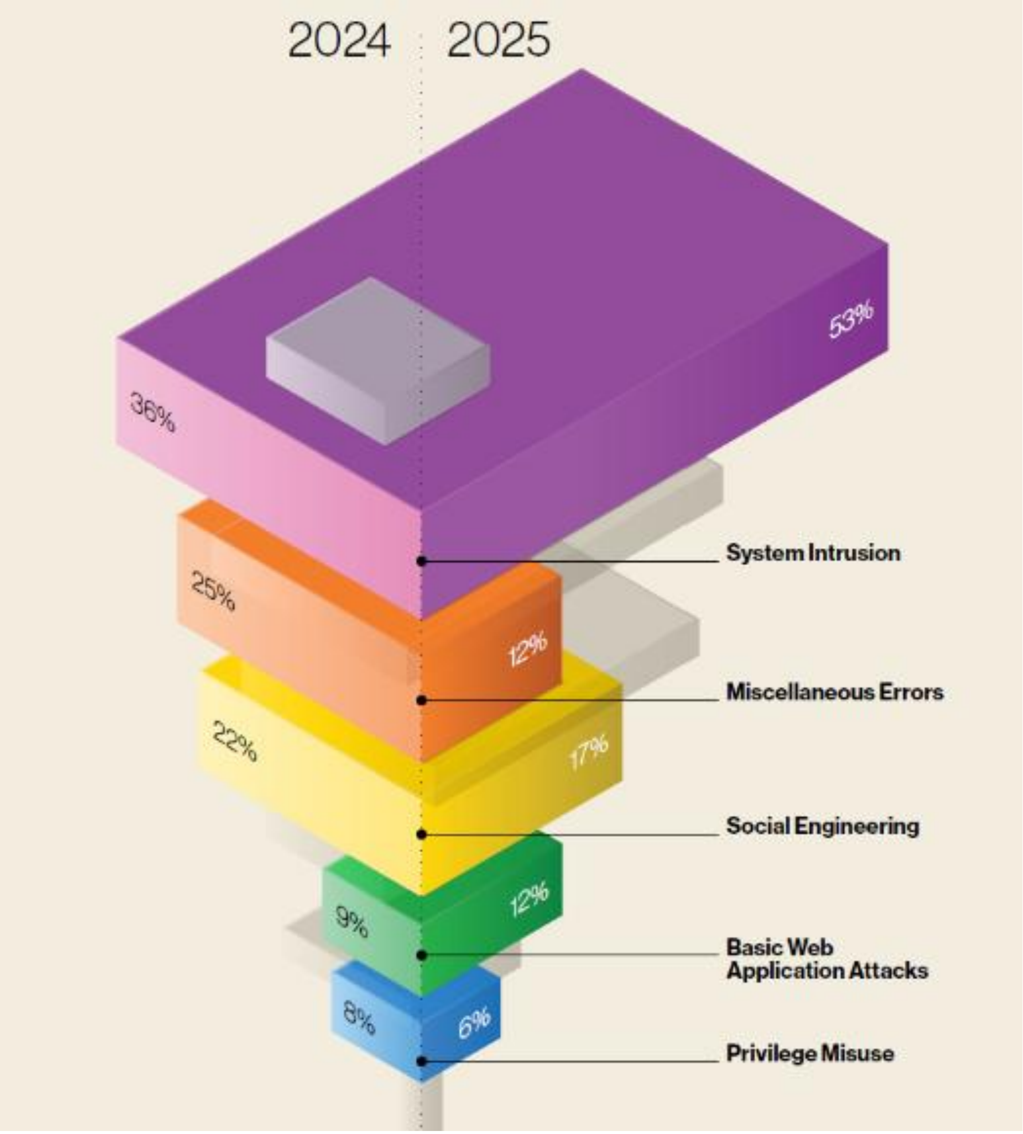
Threat actors attempt to obtain unauthorized initial access into a victim's network. Actors use techniques, such as Valid Accounts T1078 or Spear Phishing Link T1566.002s, to gain this access. After obtaining initial access, actors can then execute other techniques to move about the network.

- Cracking password hashes (89% Administrator accounts)
- Default or stolen administrator accounts
- Former employee accounts that have not been removed
- Initial access brokers that sell exploits and valid credentials



Verizon 2025 Data Breach Investigations Report

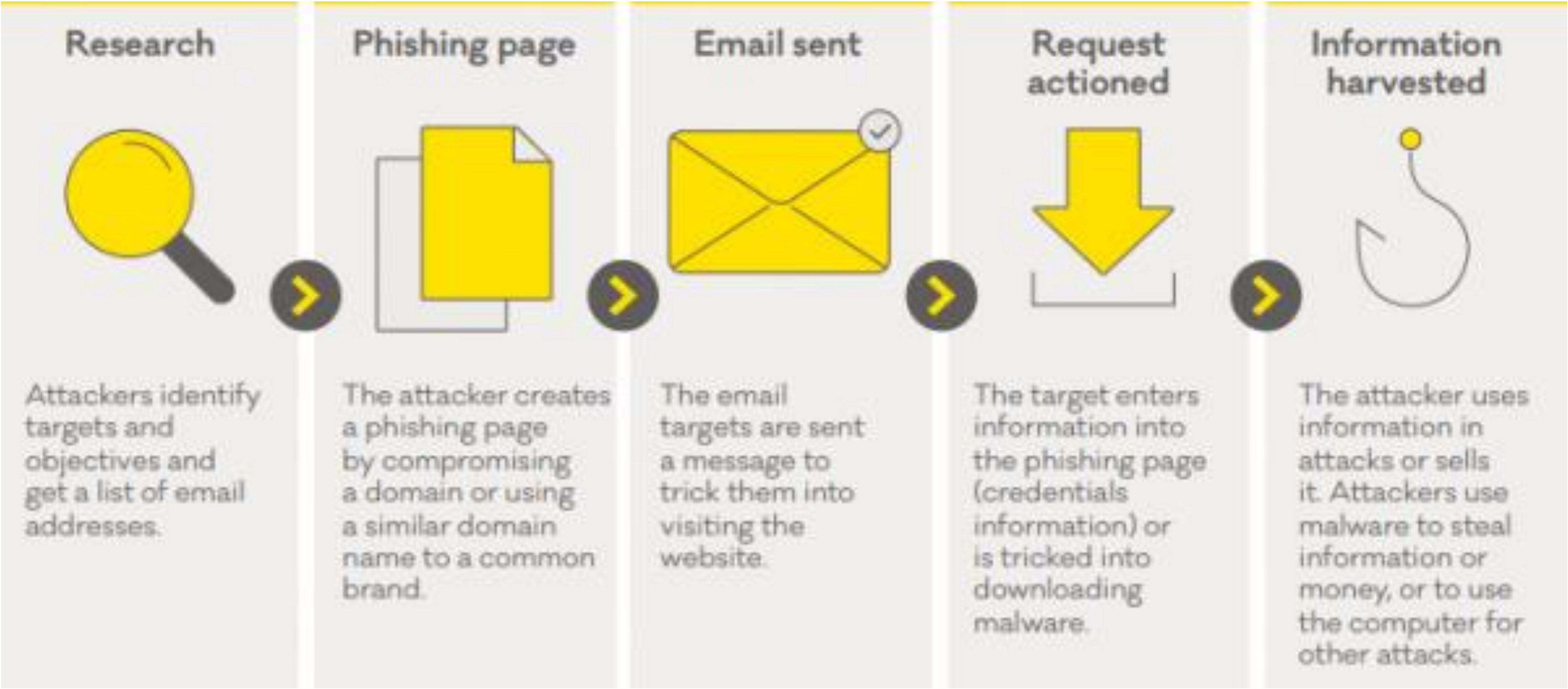
- 18th Edition
- Over 1 million datapoints
- 22,052 security incidents that compromised the integrity, confidentiality or availability of an information asset.
- 12,195 breaches that resulted in the confirmed disclosure of data to an unauthorised party.



What Verizon Found – Key Statistics

- 60% of breaches involved a human element
- 30% of breaches were linked to third-party involvement
- 34% increase in attackers exploiting vulnerabilities to gain initial access
- 54% of perimeter-device vulnerabilities were fully remediated
- 44% of all breaches analysed showed ransomware was present, a notable rise

Traditional Business Email Compromise – Pre MFA



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.

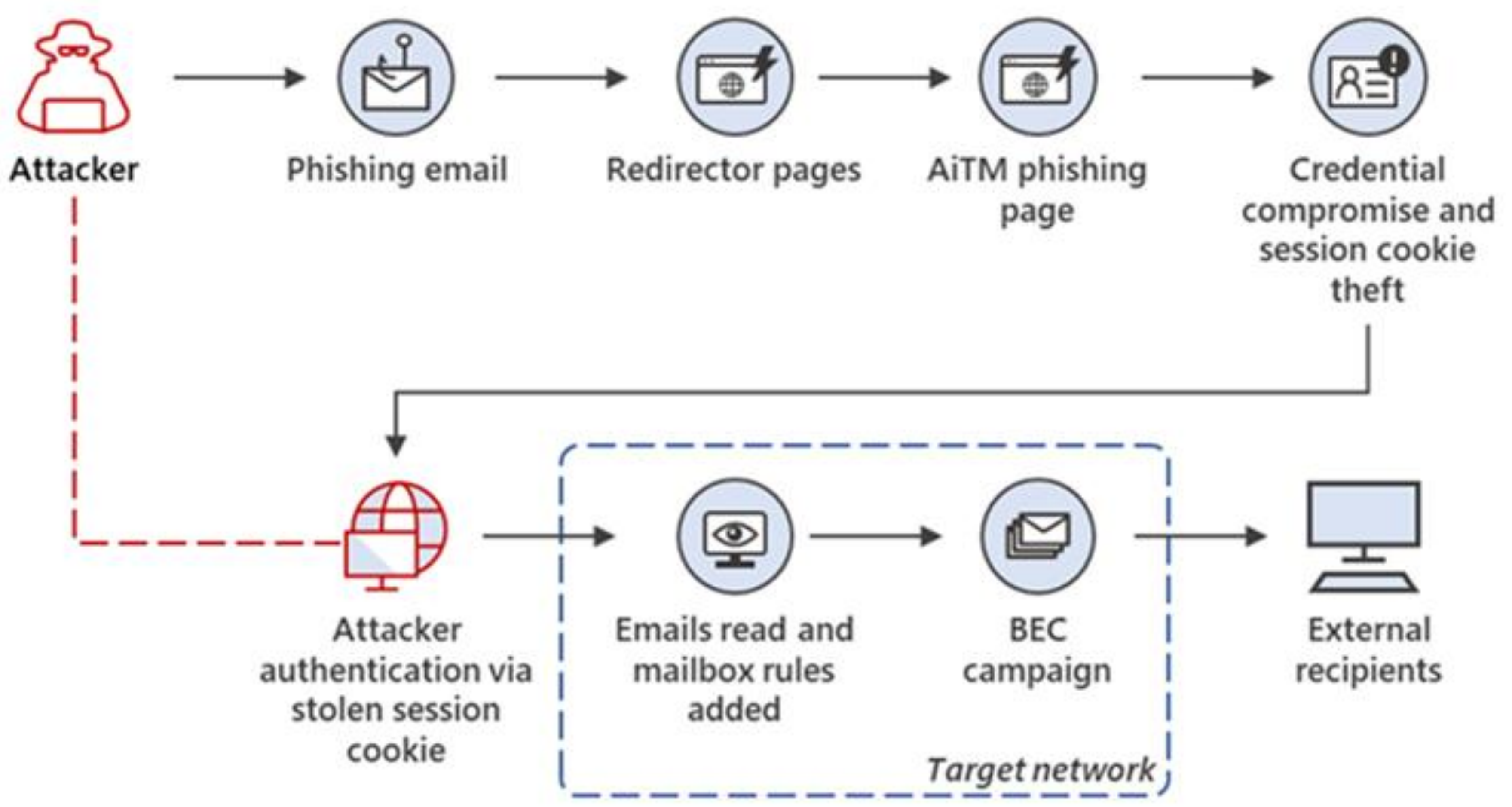
Request actioned

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

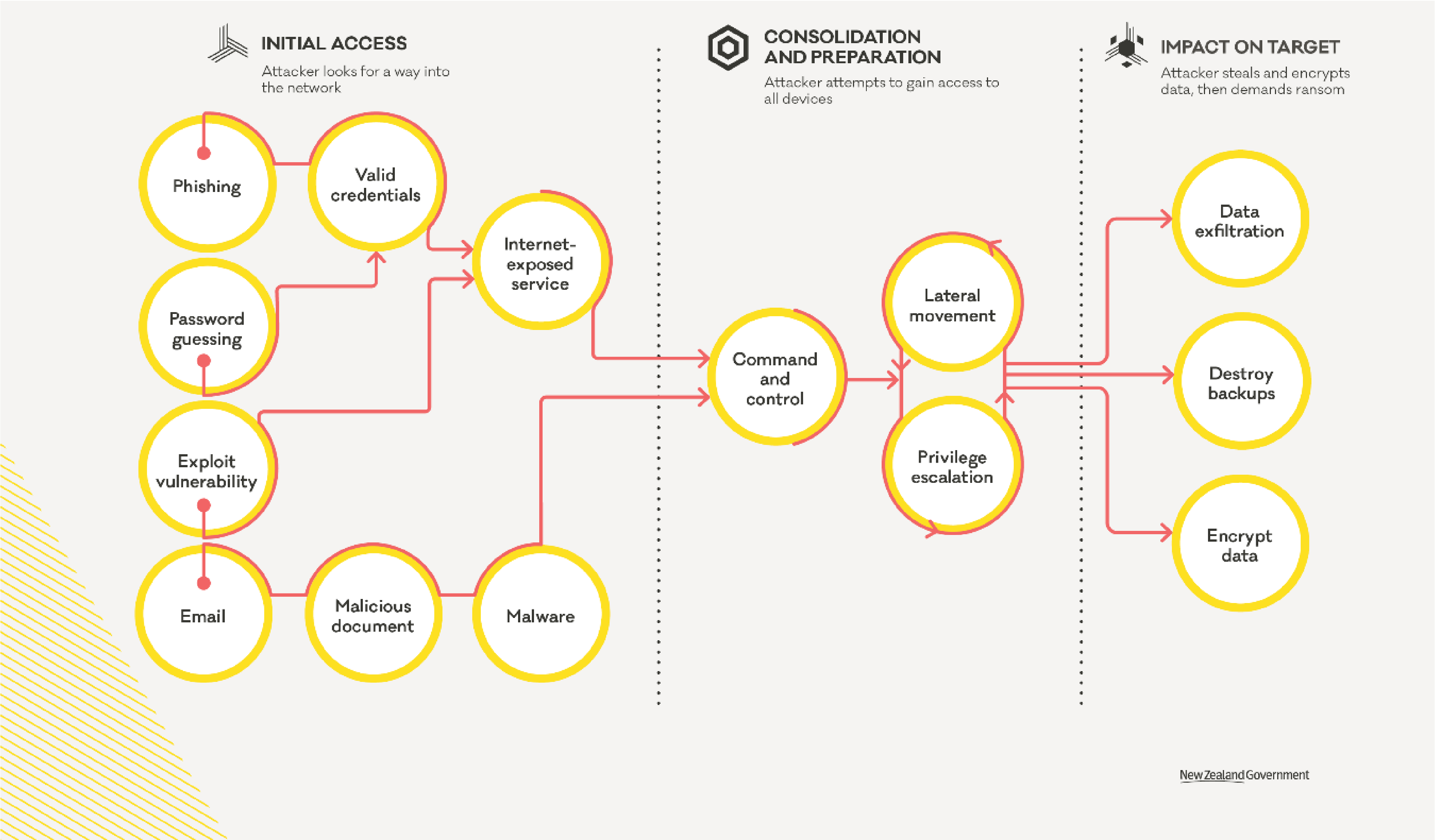
Information harvested

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.

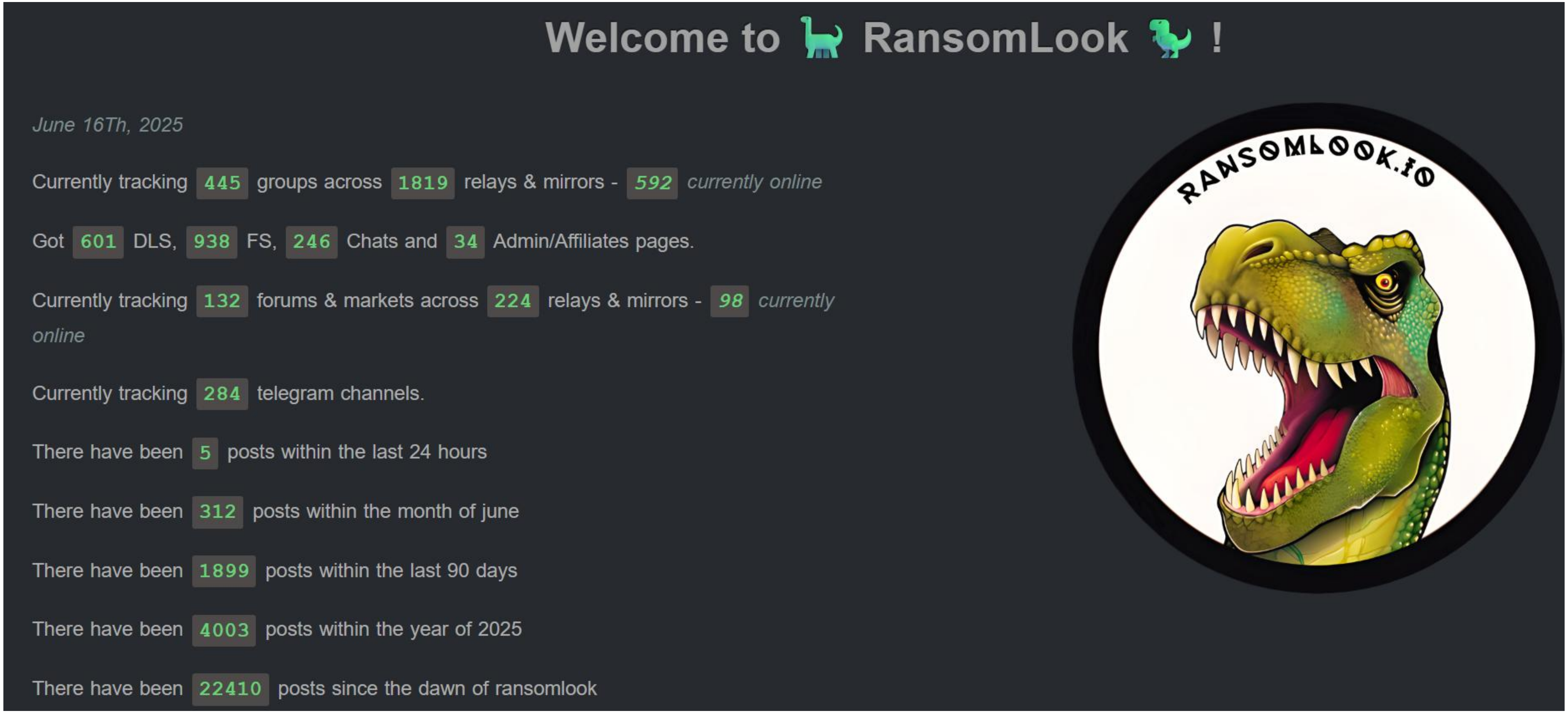
Evolving Business Email Compromise – Post MFA


Attacker
Phishing email
Redirector pages
AiTM phishing page
Credential compromise and session cookie theft
Attacker authentication via stolen session cookie
Emails read and mailbox rules added
BEC campaign
External recipients
Target network

Lifecycle of a Ransomware Incident



Current Ransomware Activity



Welcome to 🦕 RansomLook 🦖 !

June 16Th, 2025

Currently tracking 445 groups across 1819 relays & mirrors - *592* *currently online*

Got 601 DLS, 938 FS, 246 Chats and 34 Admin/Affiliates pages.

Currently tracking 132 forums & markets across 224 relays & mirrors - *98* *currently online*

Currently tracking 284 telegram channels.

There have been 5 posts within the last 24 hours

There have been 312 posts within the month of june

There have been 1899 posts within the last 90 days

There have been 4003 posts within the year of 2025

There have been 22410 posts since the dawn of ransomlook

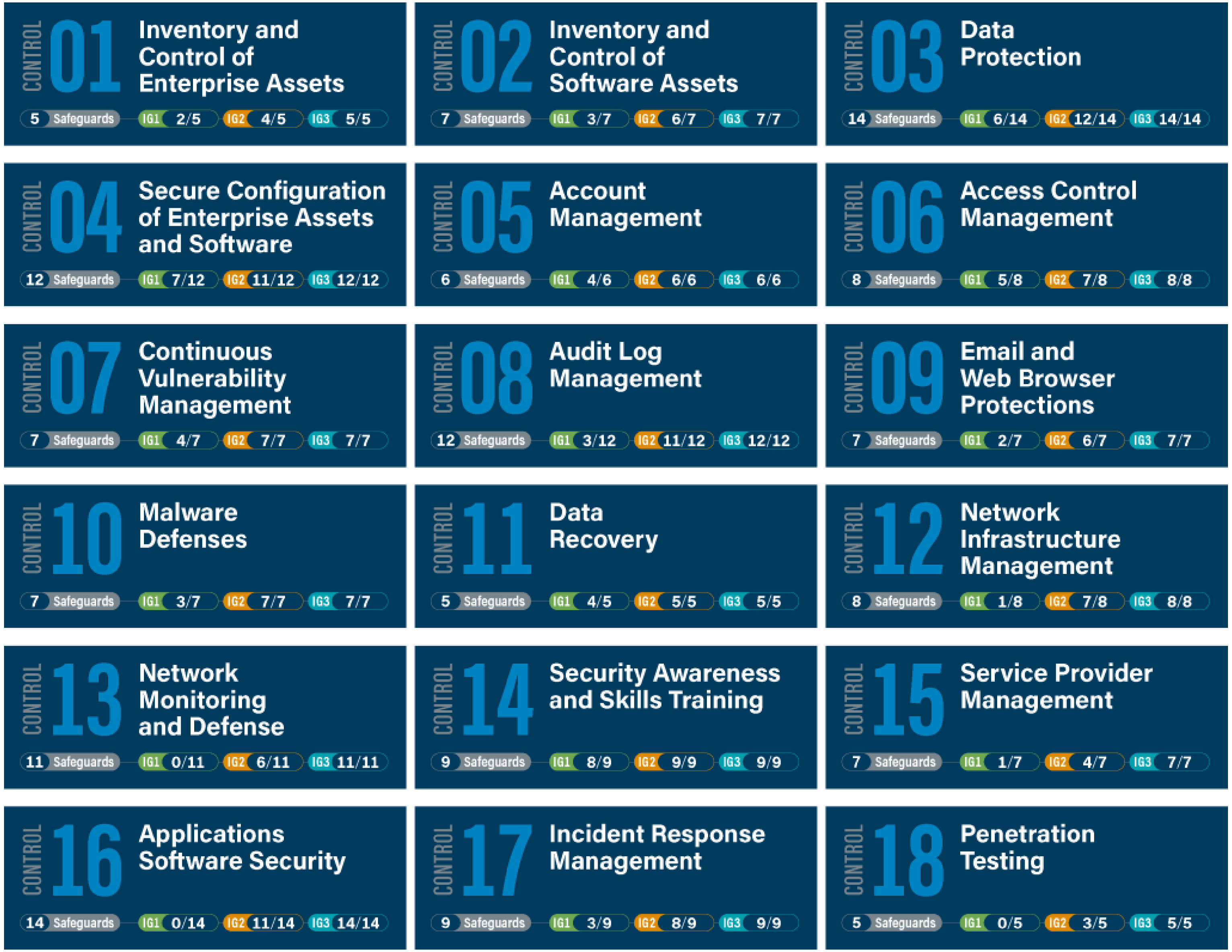
Governance and Controls

Cyber Risk Management - Controls

The CIS Controls are a set of 18 prioritised, well-vetted, and supported security actions that organisations can take to assess and improve their current security state.

The controls are designed using knowledge of actual attacks to help an organisation prioritise their investment in controls that will provide the greatest risk reduction and protection against the most dangerous threat actors, and that can be feasibly implemented.

Cyber Risk Management - Controls



CONTROL 01 Inventory and Control of Enterprise Assets
5 Safeguards IG1 2/5 IG2 4/5 IG3 5/5

CONTROL 02 Inventory and Control of Software Assets
7 Safeguards IG1 3/7 IG2 6/7 IG3 7/7

CONTROL 03 Data Protection
14 Safeguards IG1 6/14 IG2 12/14 IG3 14/14

CONTROL 04 Secure Configuration of Enterprise Assets and Software
12 Safeguards IG1 7/12 IG2 11/12 IG3 12/12

CONTROL 05 Account Management
6 Safeguards IG1 4/6 IG2 6/6 IG3 6/6

CONTROL 06 Access Control Management
8 Safeguards IG1 5/8 IG2 7/8 IG3 8/8

CONTROL 07 Continuous Vulnerability Management
7 Safeguards IG1 4/7 IG2 7/7 IG3 7/7

CONTROL 08 Audit Log Management
12 Safeguards IG1 3/12 IG2 11/12 IG3 12/12

CONTROL 09 Email and Web Browser Protections
7 Safeguards IG1 2/7 IG2 6/7 IG3 7/7

CONTROL 10 Malware Defenses
7 Safeguards IG1 3/7 IG2 7/7 IG3 7/7

CONTROL 11 Data Recovery
5 Safeguards IG1 4/5 IG2 5/5 IG3 5/5

CONTROL 12 Network Infrastructure Management
8 Safeguards IG1 1/8 IG2 7/8 IG3 8/8

CONTROL 13 Network Monitoring and Defense
11 Safeguards IG1 0/11 IG2 6/11 IG3 11/11

CONTROL 14 Security Awareness and Skills Training
9 Safeguards IG1 8/9 IG2 9/9 IG3 9/9

CONTROL 15 Service Provider Management
7 Safeguards IG1 1/7 IG2 4/7 IG3 7/7

CONTROL 16 Applications Software Security
14 Safeguards IG1 0/14 IG2 11/14 IG3 14/14

CONTROL 17 Incident Response Management
9 Safeguards IG1 3/9 IG2 8/9 IG3 9/9

CONTROL 18 Penetration Testing
5 Safeguards IG1 0/5 IG2 3/5 IG3 5/5

New Zealand Legal Landscape

Cyber is Contextual – Law Firms

Incident Response

FORENSIC & CYBER

INCIDENT RESPONSE
SOLUTIONS

Cyber Security Guide for NZ Law Firms

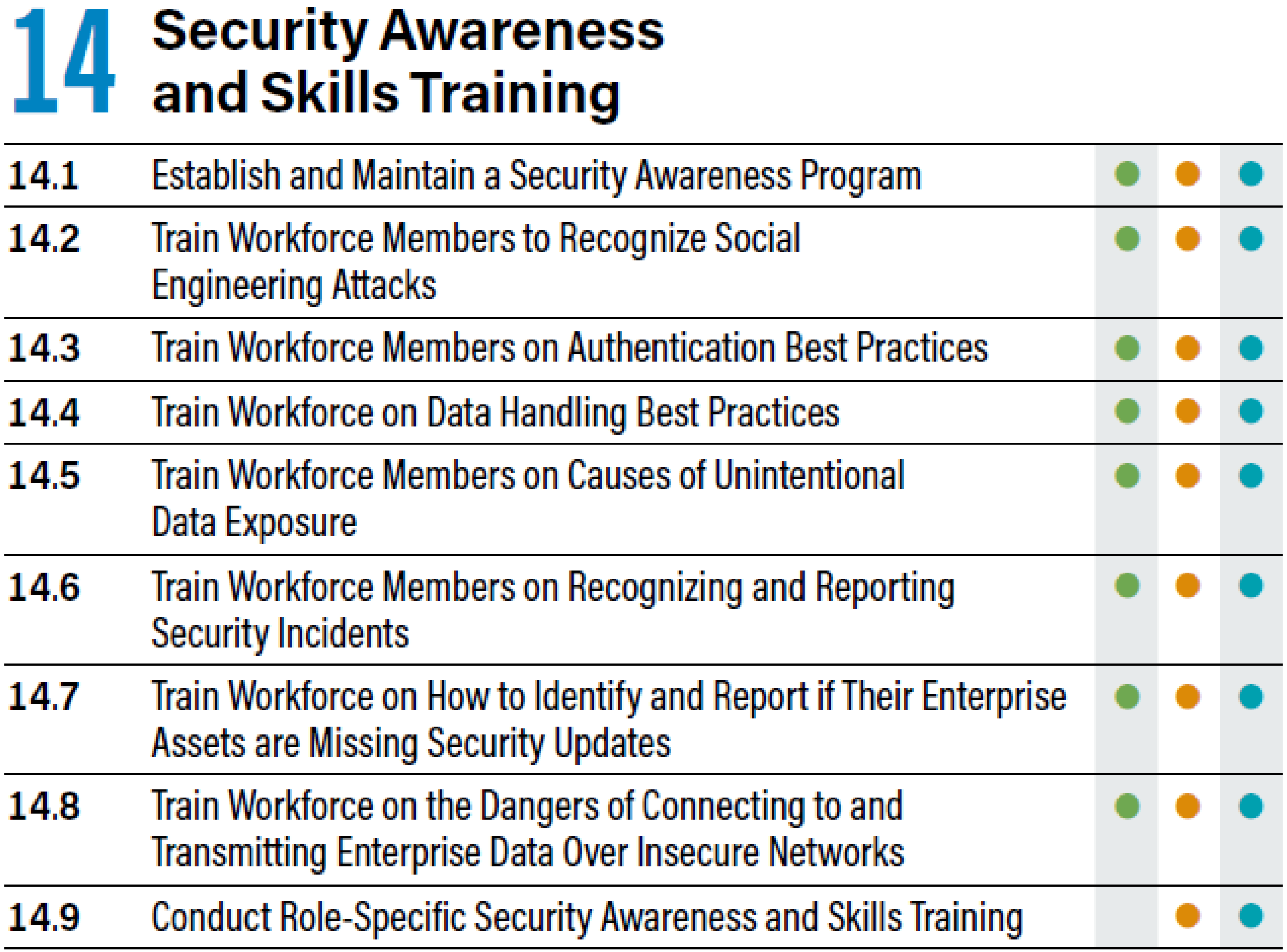
2020 Edition

https://incidentresponse.co.nz/cyber-security-for-law-firms

Law Firm Cyber Security at a Glance

- 27% have been breached (from a minor loss laptop to a major data breach). 42% of law firm business leaders rated security breaches, data loss, hacking and ransomware as a high risk to firm profitability. (*The American Bar Association's 2022 Legal Technology Survey Report)*
- 78% are extremely or somewhat concerned about cyber risk, leading to increased spend and appointments of dedicated Cyber Security Chief as it becomes more difficult to insure against cyber risk, managing cyber threats is likely to remain a key challenge with a heightened focus in the future. (*2022 Survey of Global Law Firms)*
- 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)*

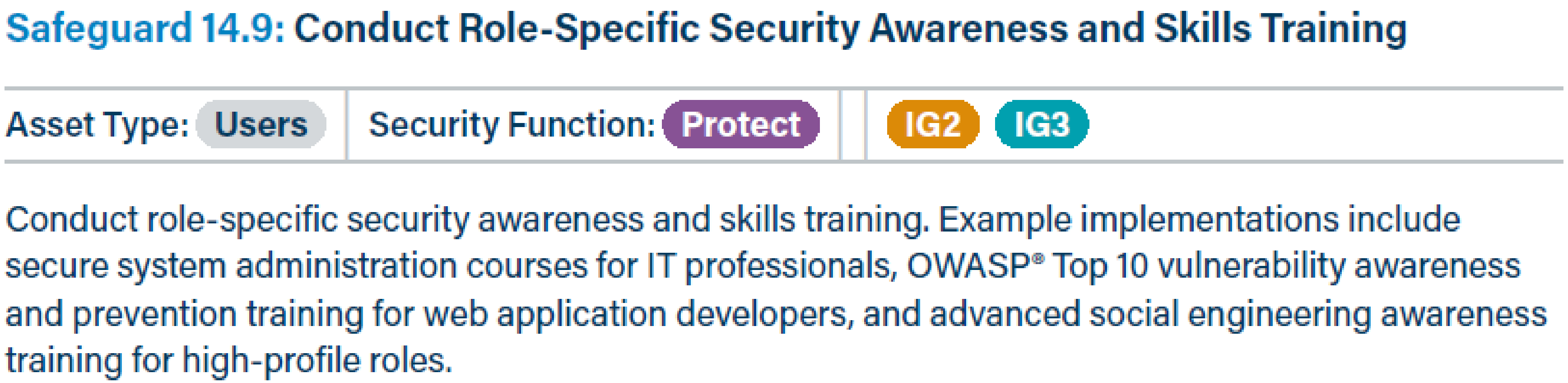
Cyber Risk Management – Security Awareness and Skills Training



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		●	●

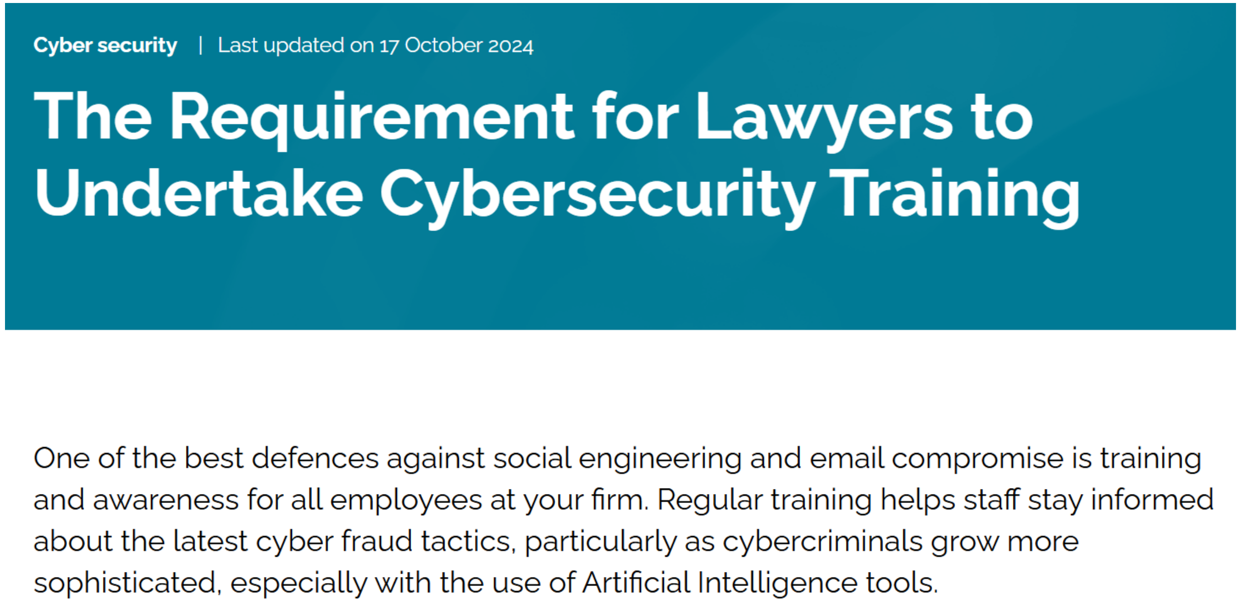
Role Specific Staff Training and Awareness



Safeguard 14.9: Conduct Role-Specific Security Awareness and Skills Training

Asset Type: Users | Security Function: Protect | IG2 IG3

Conduct role-specific security awareness and skills training. Example implementations include secure system administration courses for IT professionals, OWASP® Top 10 vulnerability awareness and prevention training for web application developers, and advanced social engineering awareness training for high-profile roles.

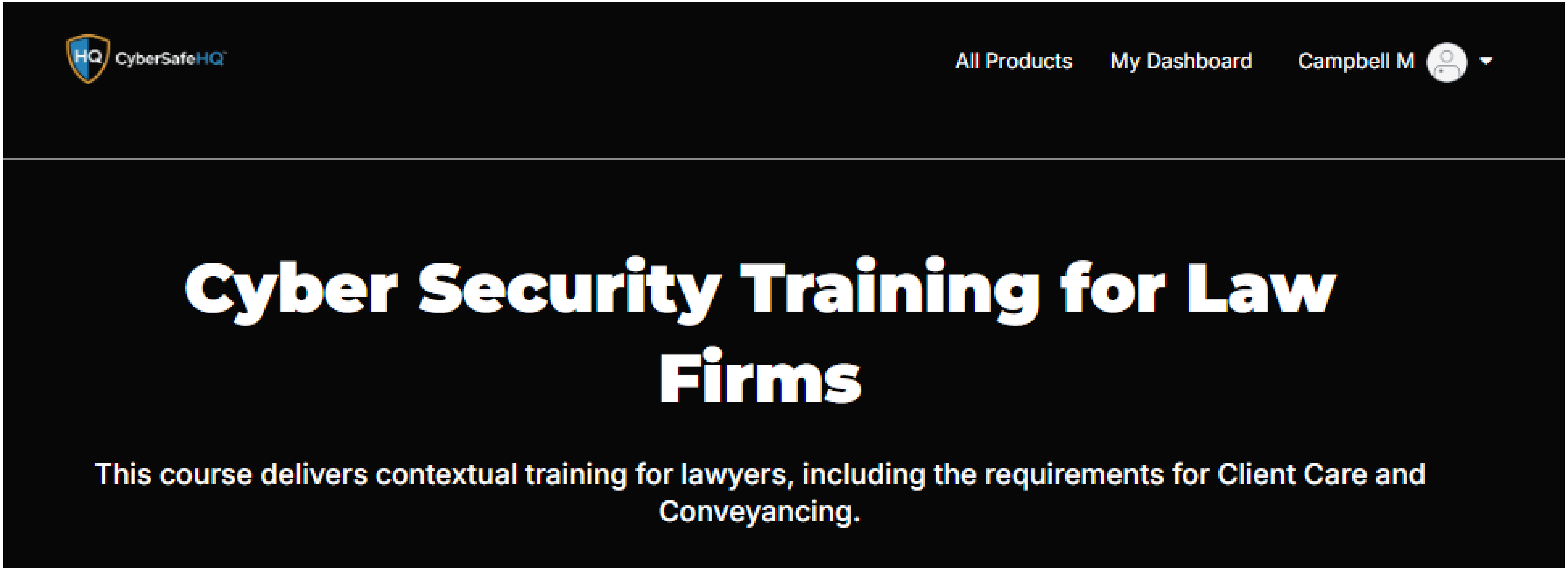


Cyber security | Last updated on 17 October 2024

The Requirement for Lawyers to Undertake Cybersecurity Training

One of the best defences against social engineering and email compromise is training and awareness for all employees at your firm. Regular training helps staff stay informed about the latest cyber fraud tactics, particularly as cybercriminals grow more sophisticated, especially with the use of Artificial Intelligence tools.

Cyber Training and Awareness for Lawyers



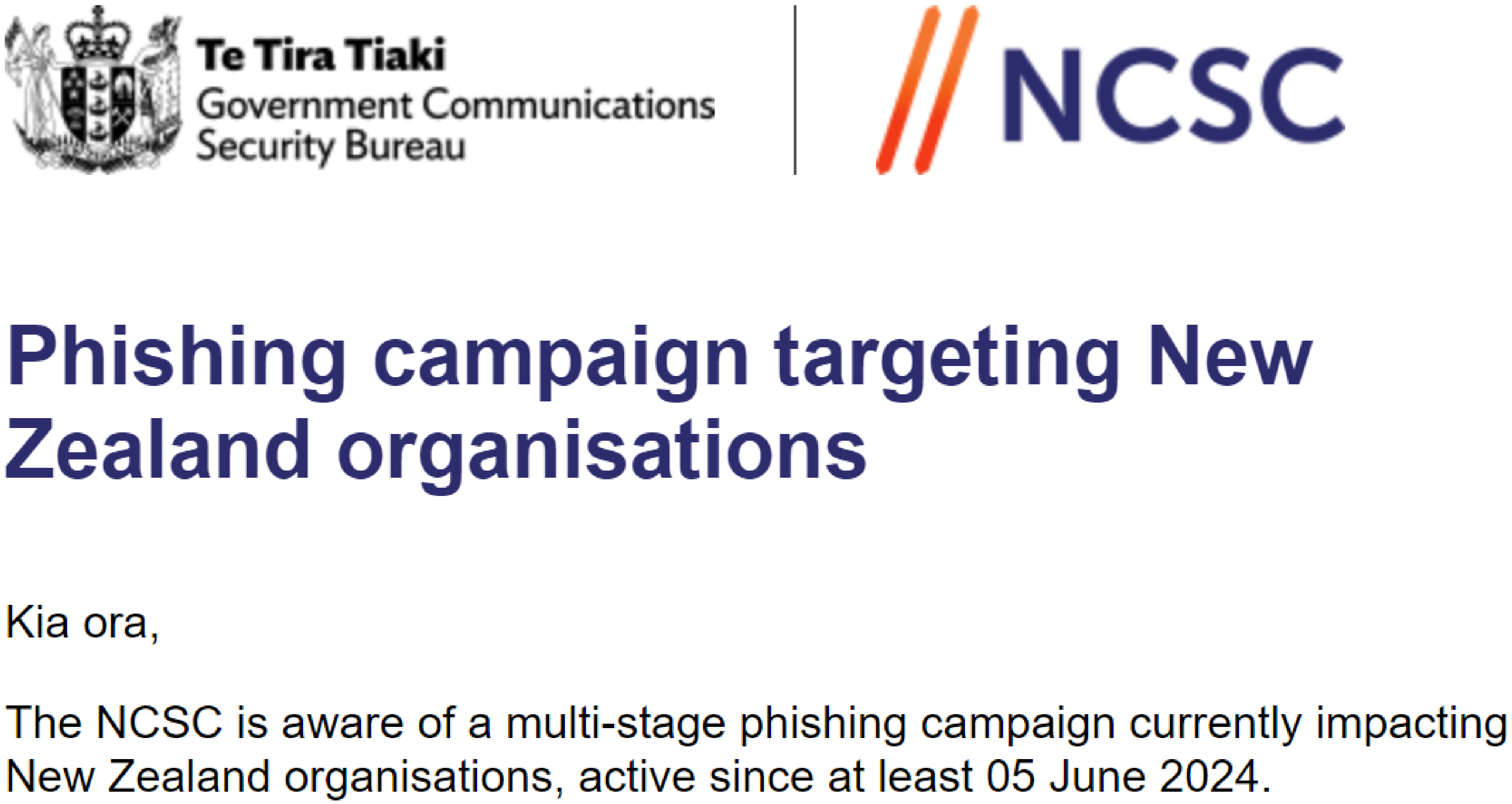
Cyber Security Training for Law Firms

This course delivers contextual training for lawyers, including the requirements for Client Care and Conveyancing.

Cybersafehq.com

Incident Response

Adversary-in-the-Middle (AiTM) – Business Email Compromise



Te Tira Tiaki
Government Communications
Security Bureau

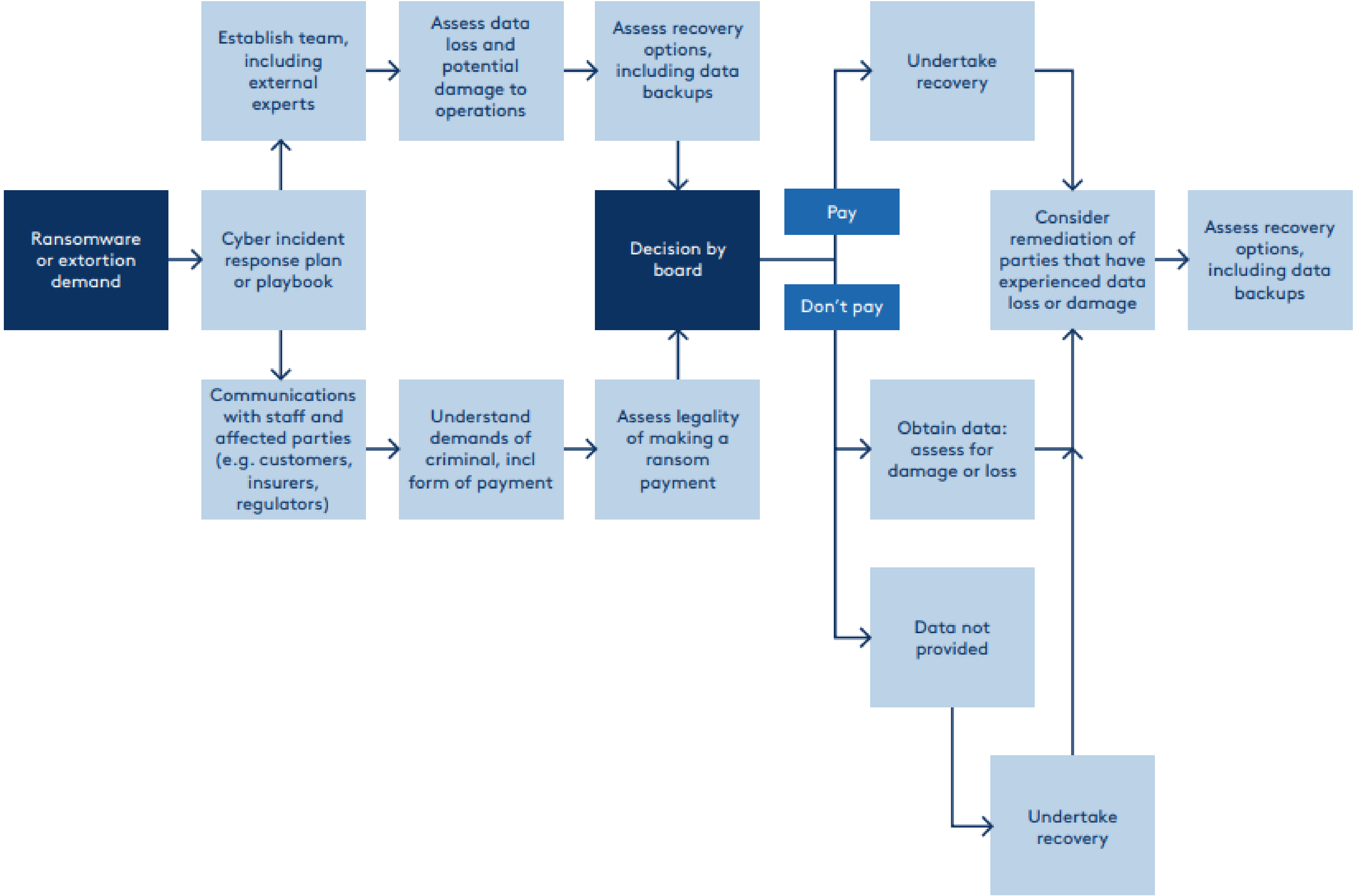
NCSC

Phishing campaign targeting New Zealand organisations

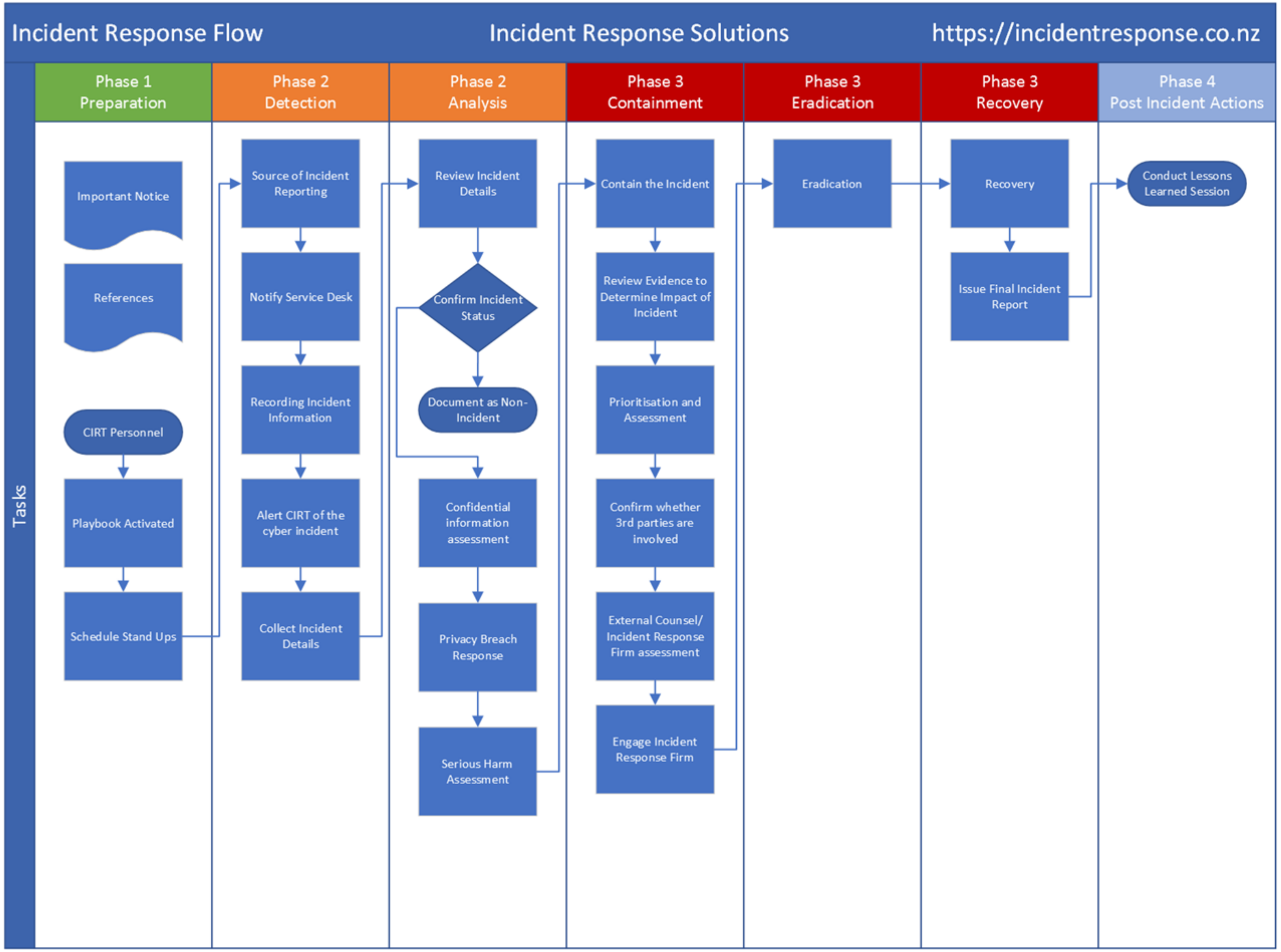
Kia ora,

The NCSC is aware of a multi-stage phishing campaign currently impacting New Zealand organisations, active since at least 05 June 2024.

Example Ransomware Decision Making Process - AICD


Ransomware or extortion demand
Cyber incident response plan or playbook
Establish team, including external experts
Assess data loss and potential damage to operations
Assess recovery options, including data backups
Communications with staff and affected parties (e.g. customers, insurers, regulators)
Understand demands of criminal, incl form of payment
Assess legality of making a ransom payment
Decision by board
Pay
Don't pay
Undertake recovery
Obtain data: assess for damage or loss
Data not provided
Undertake recovery
Consider remediation of parties that have experienced data loss or damage
Assess recovery options, including data backups

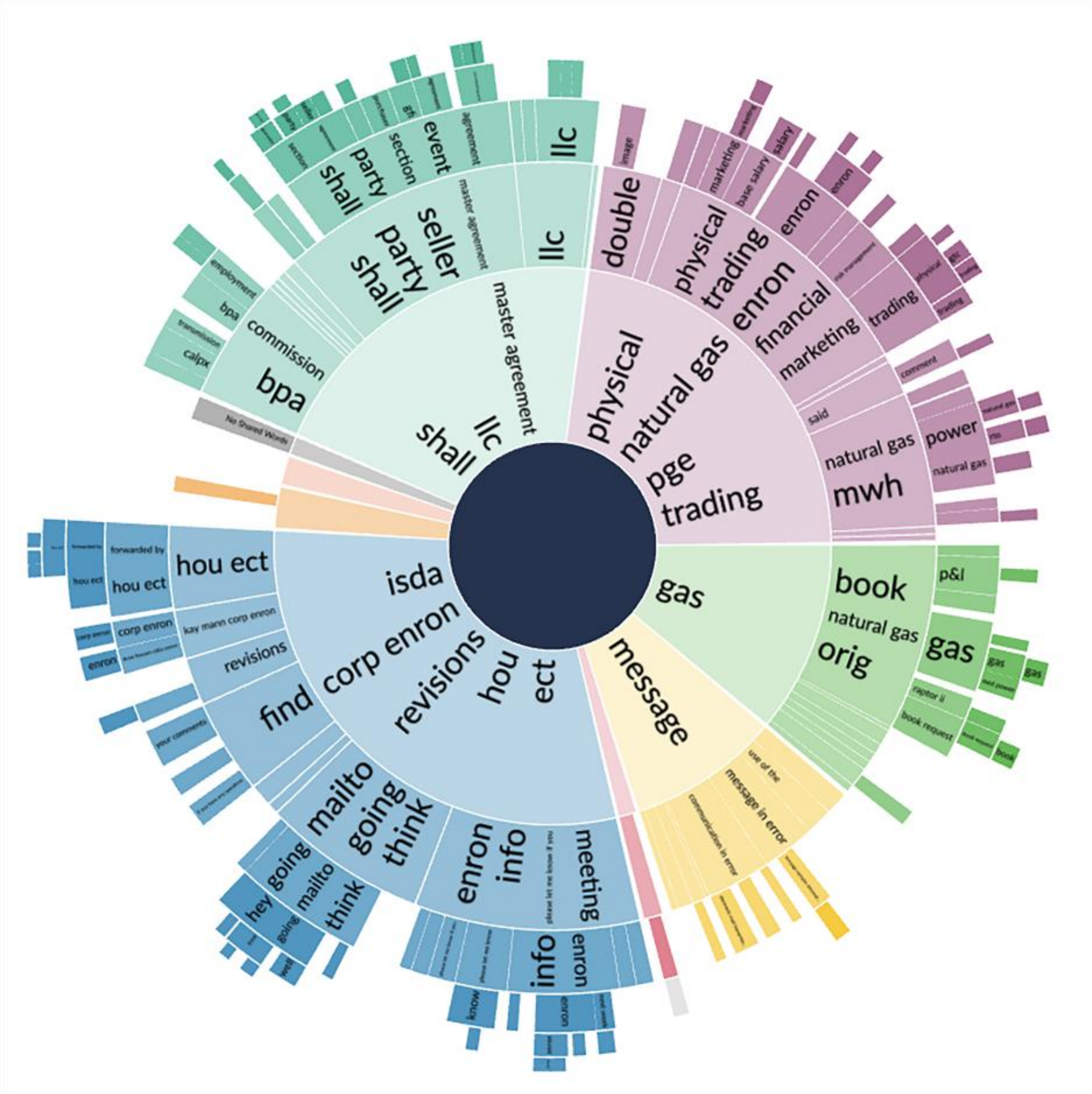
Routine Response and Investigation Methodology


Incident Response Flow
Incident Response Solutions
https://incidentresponse.co.nz
Tasks
Phase 1 Preparation
Phase 2 Detection
Phase 2 Analysis
Phase 3 Containment
Phase 3 Eradication
Phase 3 Recovery
Phase 4 Post Incident Actions
Important Notice
References
CIRT Personnel
Playbook Activated
Schedule Stand Ups
Source of Incident Reporting
Notify Service Desk
Recording Incident Information
Alert CIRT of the cyber incident
Collect Incident Details
Review Incident Details
Confirm Incident Status
Document as Non-Incident
Confidential information assessment
Privacy Breach Response
Serious Harm Assessment
Contain the Incident
Review Evidence to Determine Impact of Incident
Prioritisation and Assessment
Confirm whether 3rd parties are involved
External Counsel/ Incident Response Firm assessment
Engage Incident Response Firm
Eradication
Recovery
Issue Final Incident Report
Conduct Lessons Learned Session

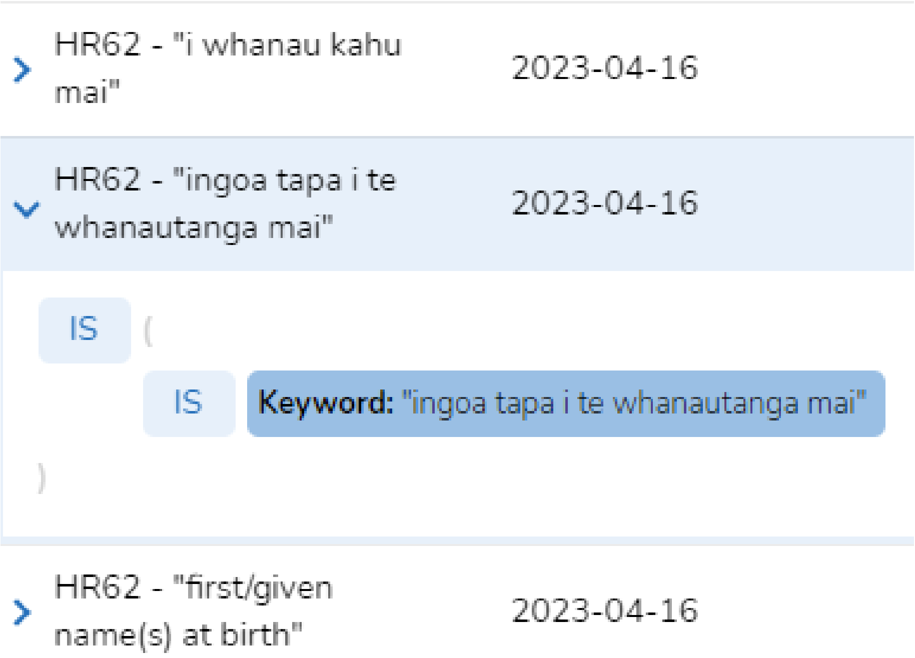
Cyber Security

Latest advancements in document analysis and review tools

Concept Searching and Clustering Technology



Preconfigured Search Sets – Privacy Breach



HR62 - "i whanau kahu mai" 2023-04-16

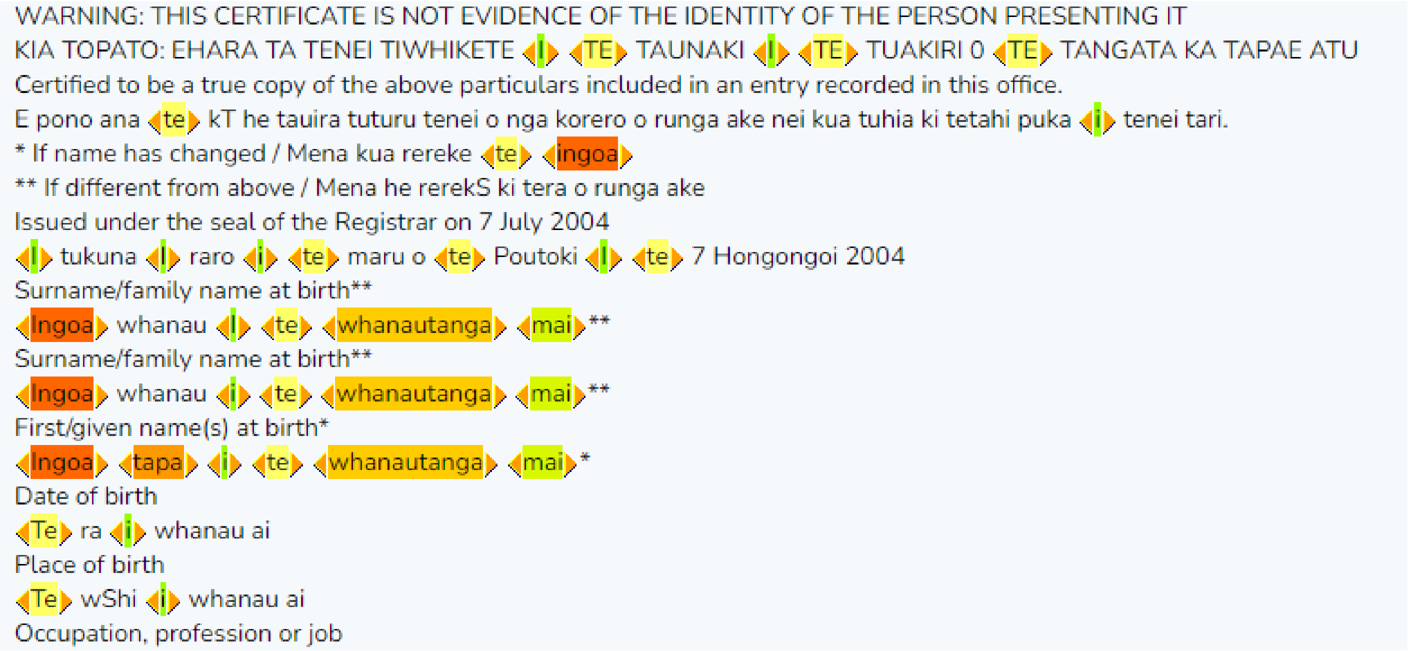
HR62 - "ingoa tapa i te whanautanga mai" 2023-04-16

IS (

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

)

HR62 - "first/given name(s) at birth" 2023-04-16



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

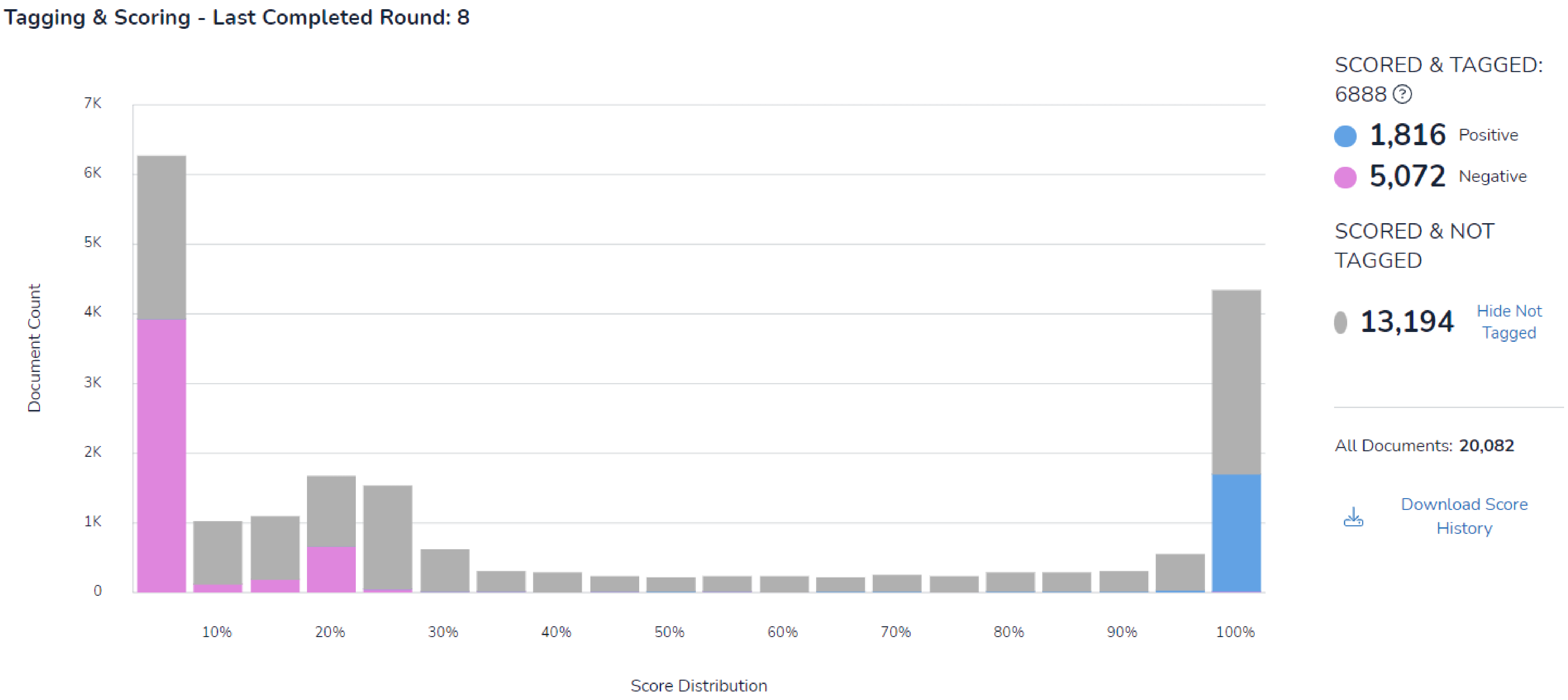
Te ra i whanau ai

Place of birth

Te wShi i whanau ai

Occupation, profession or job

Document prioritisation – Continuous Active Learning



Tagging & Scoring - Last Completed Round: 8

SCORED & TAGGED: 6888 ⓘ

● **1,816** Positive

● **5,072** Negative

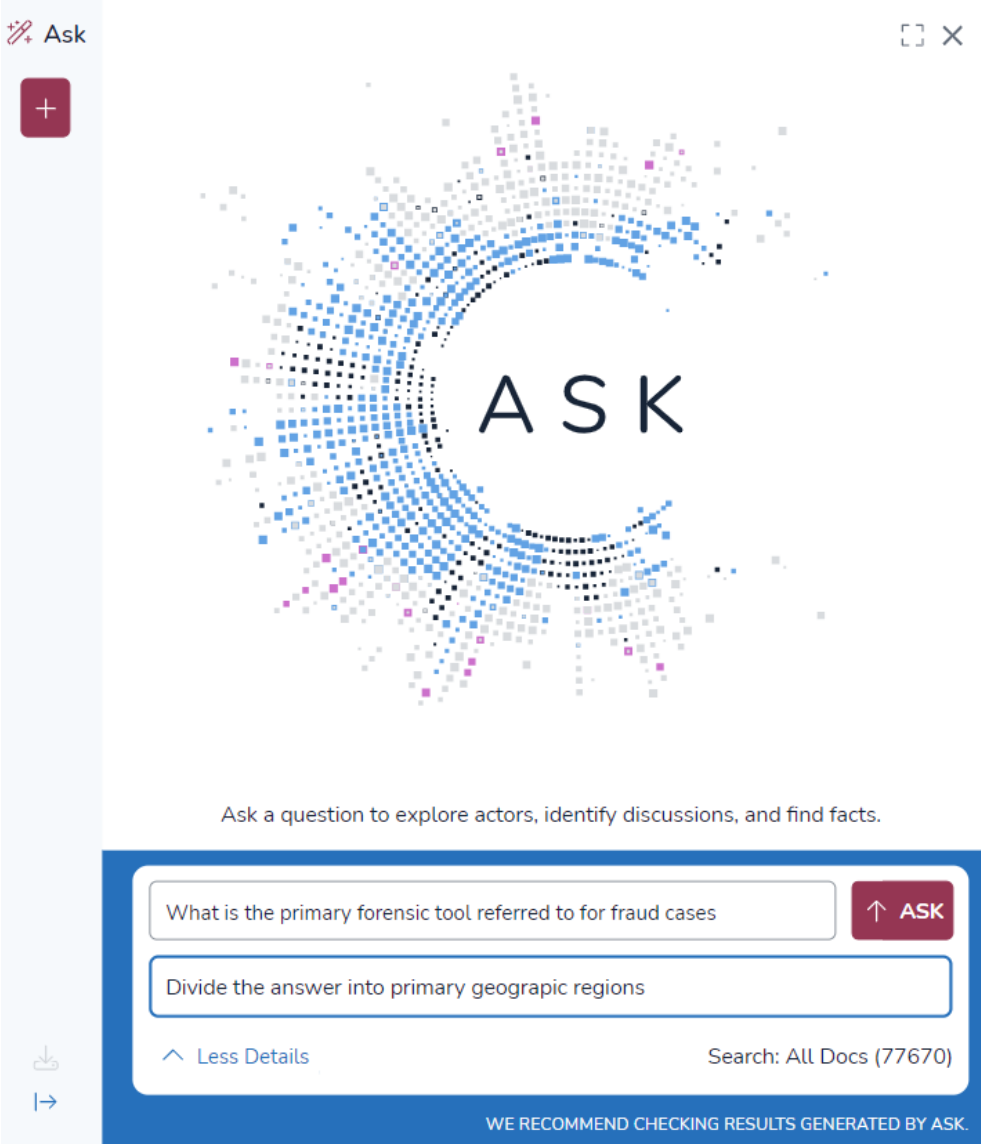
SCORED & NOT TAGGED

● **13,194** Hide Not Tagged

All Documents: **20,082**

Download Score History

Semantic Search –Generate Results Securely



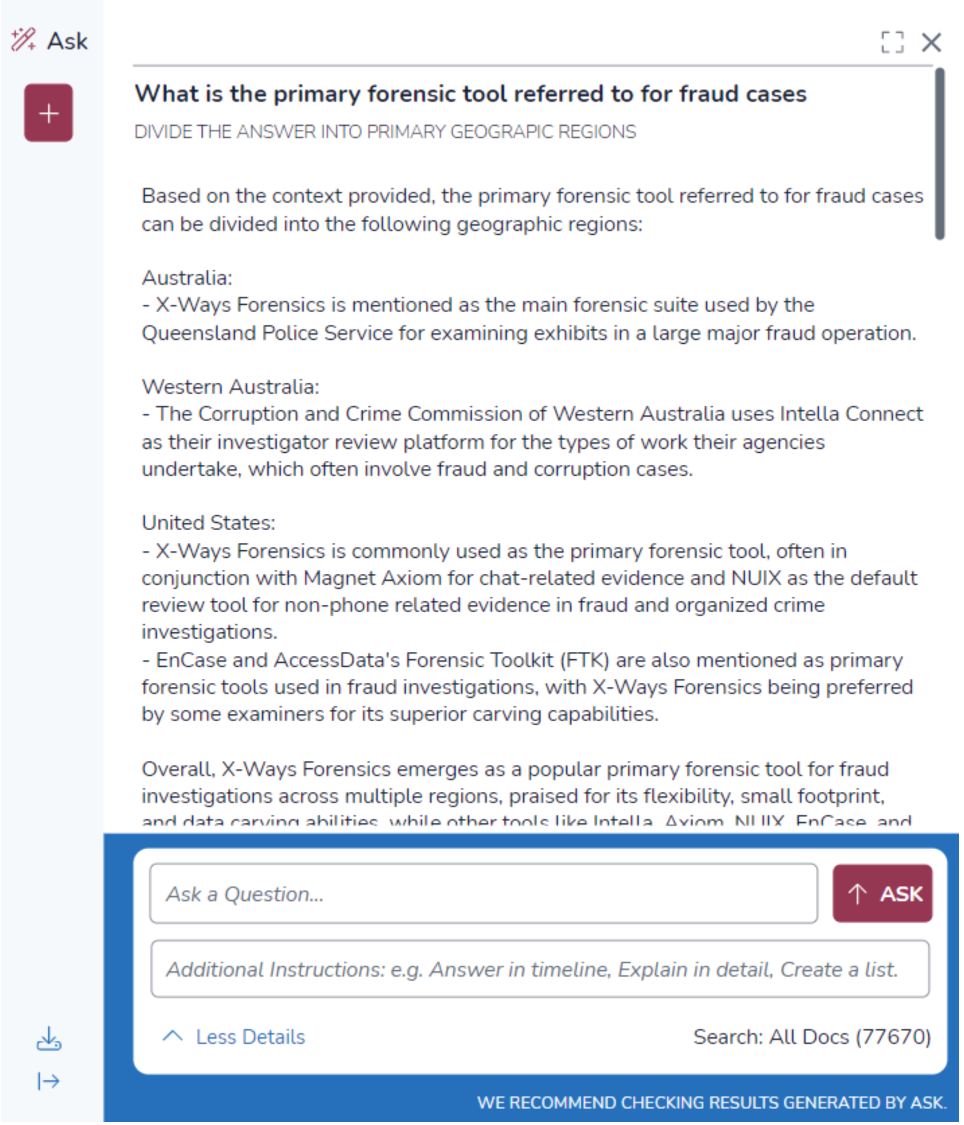
Ask a question to explore actors, identify discussions, and find facts.

What is the primary forensic tool referred to for fraud cases

Divide the answer into primary geograpic regions

Search: All Docs (77670)

WE RECOMMEND CHECKING RESULTS GENERATED BY ASK.



What is the primary forensic tool referred to for fraud cases

DIVIDE THE ANSWER INTO PRIMARY GEOGRAPIC REGIONS

Based on the context provided, the primary forensic tool referred to for fraud cases can be divided into the following geographic regions:

Australia:
- X-Ways Forensics is mentioned as the main forensic suite used by the Queensland Police Service for examining exhibits in a large major fraud operation.

Western Australia:
- The Corruption and Crime Commission of Western Australia uses Intella Connect as their investigator review platform for the types of work their agencies undertake, which often involve fraud and corruption cases.

United States:
- X-Ways Forensics is commonly used as the primary forensic tool, often in conjunction with Magnet Axiom for chat-related evidence and NUIX as the default review tool for non-phone related evidence in fraud and organized crime investigations.
- EnCase and AccessData's Forensic Toolkit (FTK) are also mentioned as primary forensic tools used in fraud investigations, with X-Ways Forensics being preferred by some examiners for its superior carving capabilities.

Overall, X-Ways Forensics emerges as a popular primary forensic tool for fraud investigations across multiple regions, praised for its flexibility, small footprint, and data carving abilities, while other tools like Intella, Axiom, NUIX, EnCase, and

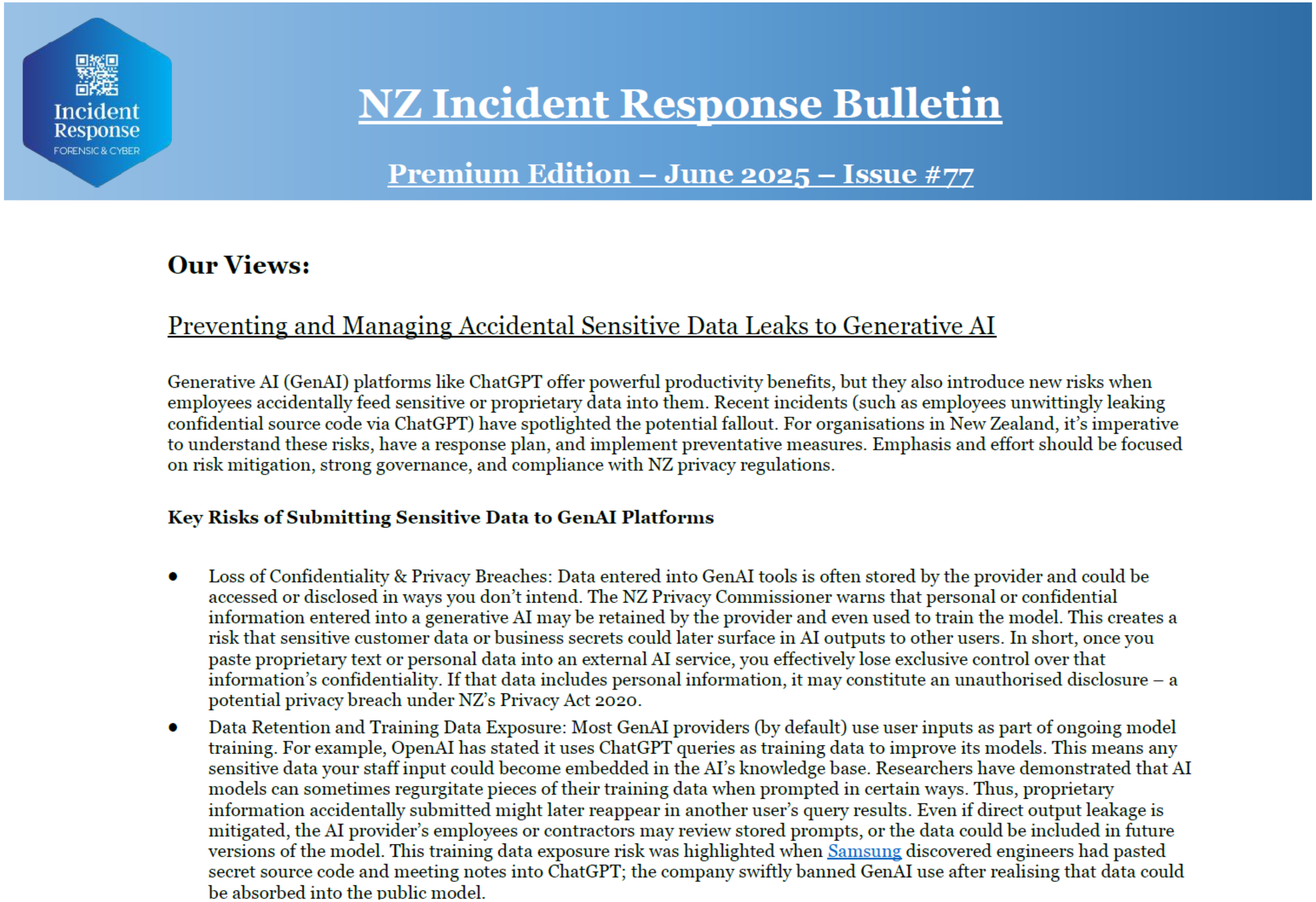
Ask a Question...

Additional Instructions: e.g. Answer in timeline, Explain in detail, Create a list.

Search: All Docs (77670)

WE RECOMMEND CHECKING RESULTS GENERATED BY ASK.

AI – The commons questions



Incident Response
FORENSIC & CYBER

NZ Incident Response Bulletin

Premium Edition – June 2025 – Issue #77

Our Views:

Preventing and Managing Accidental Sensitive Data Leaks to Generative AI

Generative AI (GenAI) platforms like ChatGPT offer powerful productivity benefits, but they also introduce new risks when employees accidentally feed sensitive or proprietary data into them. Recent incidents (such as employees unwittingly leaking confidential source code via ChatGPT) have spotlighted the potential fallout. For organisations in New Zealand, it's imperative to understand these risks, have a response plan, and implement preventative measures. Emphasis and effort should be focused on risk mitigation, strong governance, and compliance with NZ privacy regulations.

Key Risks of Submitting Sensitive Data to GenAI Platforms

- Loss of Confidentiality & Privacy Breaches: Data entered into GenAI tools is often stored by the provider and could be accessed or disclosed in ways you don't intend. The NZ Privacy Commissioner warns that personal or confidential information entered into a generative AI may be retained by the provider and even used to train the model. This creates a risk that sensitive customer data or business secrets could later surface in AI outputs to other users. In short, once you paste proprietary text or personal data into an external AI service, you effectively lose exclusive control over that information's confidentiality. If that data includes personal information, it may constitute an unauthorised disclosure – a potential privacy breach under NZ's Privacy Act 2020.
- Data Retention and Training Data Exposure: Most GenAI providers (by default) use user inputs as part of ongoing model training. For example, OpenAI has stated it uses ChatGPT queries as training data to improve its models. This means any sensitive data your staff input could become embedded in the AI's knowledge base. Researchers have demonstrated that AI models can sometimes regurgitate pieces of their training data when prompted in certain ways. Thus, proprietary information accidentally submitted might later reappear in another user's query results. Even if direct output leakage is mitigated, the AI provider's employees or contractors may review stored prompts, or the data could be included in future versions of the model. This training data exposure risk was highlighted when Samsung discovered engineers had pasted secret source code and meeting notes into ChatGPT; the company swiftly banned GenAI use after realising that data could be absorbed into the public model.

Incident
Response
FORENSIC & CYBER

Thank you

Campbell McKenzie
0800 WITNESS
021 779 310
campbell@incidentresponse.co.nz
incidentresponse.co.nz

We help you Prepare, Respond and Recover from Forensic and Cyber Incidents