ANZIIF

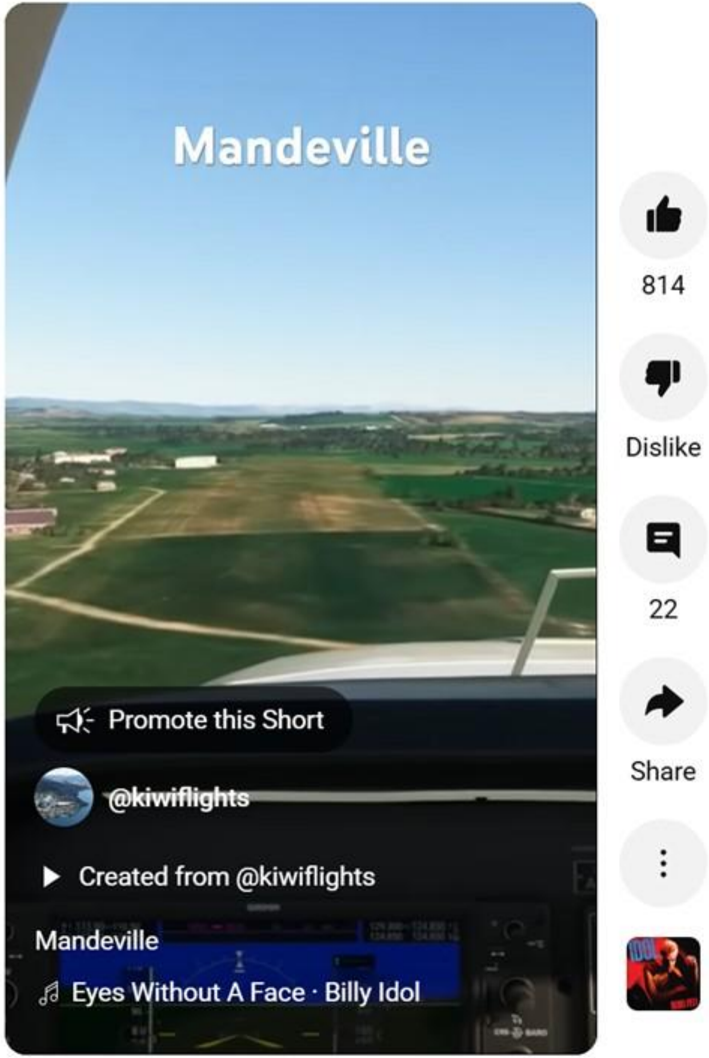
ANZIIF

Fidelity Fraud, Cybercrime & Emerging Threats

What Insurance Professionals Must Know

Bio

- Forensic technology expert witness and cybersecurity consultant
- Over 2,000 cases investigated
- Twice as old as when I started my forensic career
- Monthly forensic and cyber bulletin - 76th Edition
- C64 Basic (1984) – CyberSafeHQ.com (100% AI)
- Flight Simulator and newbie skipper

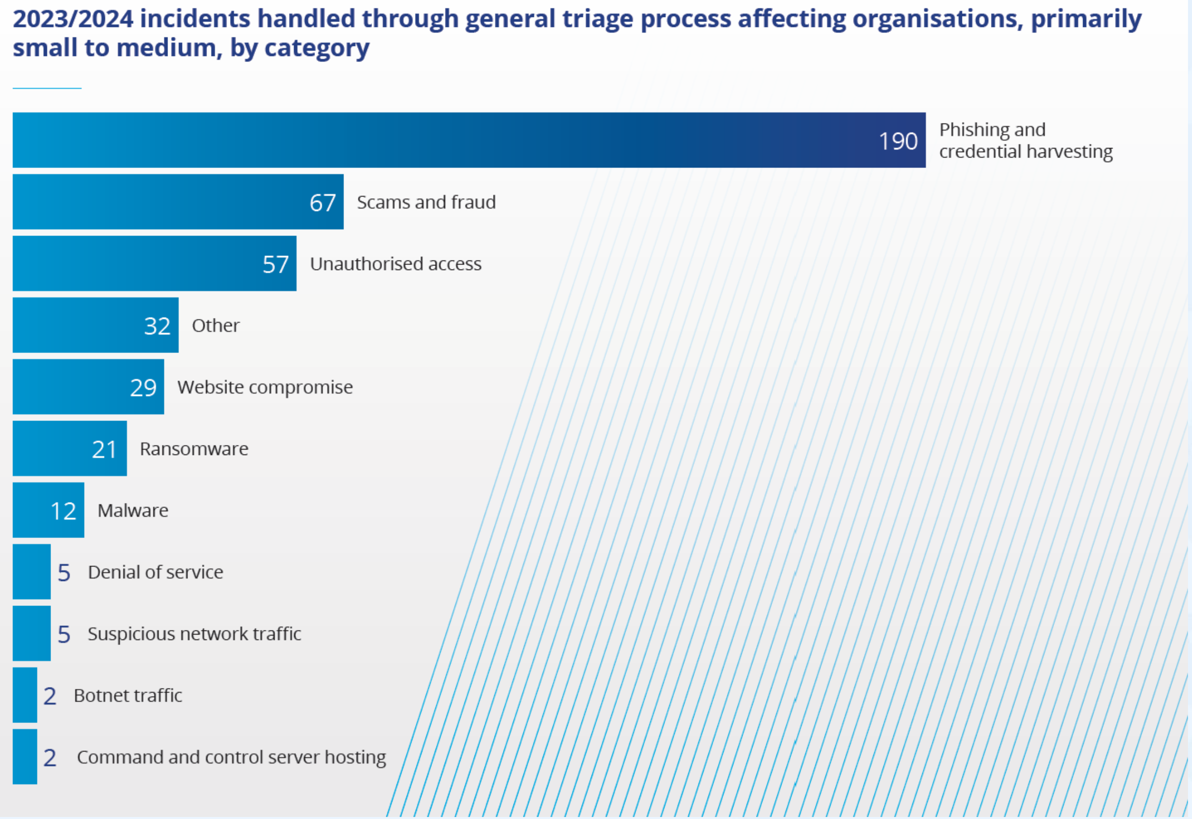

Mandeville
814
Dislike
22
Share
Promote this Short
@kiwiflights
Created from @kiwiflights
Mandeville
Eyes Without A Face · Billy Idol

60 Second Summary

- Threat Landscape – Cyber and Workplace
- Emerging Technologies
- Case Studies

Threat Landscape

NCSC - Cyber Snapshot

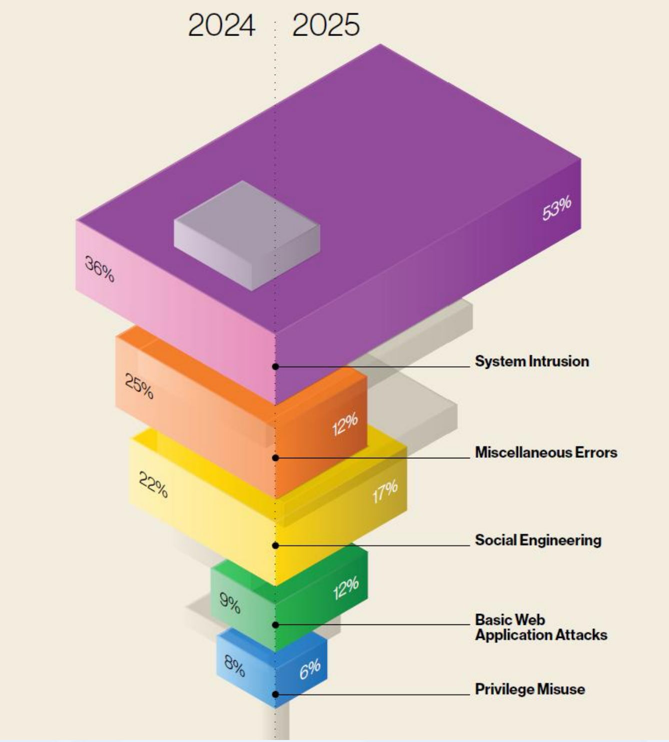


2023/2024 incidents handled through general triage process affecting organisations, primarily small to medium, by category

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

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.

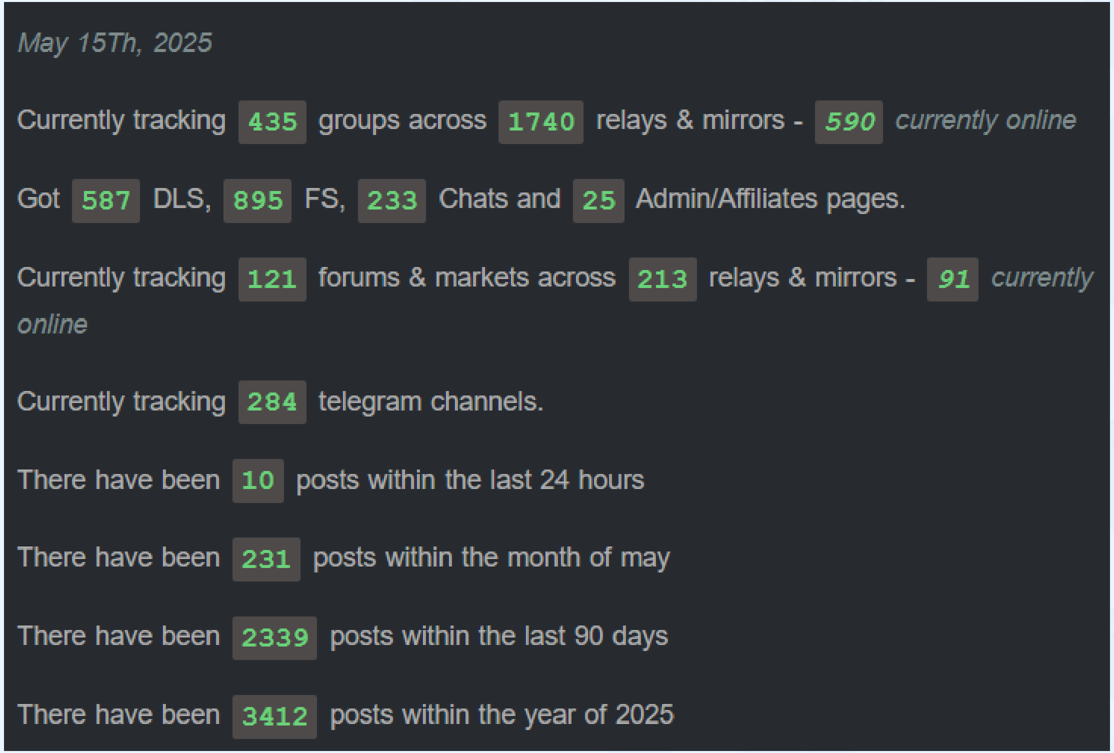


www.ransomlook.io

DBIR - Top takeaways

- 60% of breaches involved a human element
- 30% of breaches were linked to third-party involvement – double 2024
- 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

Ransomware - Dark Web



May 15Th, 2025

Currently tracking 435 groups across 1740 relays & mirrors - *590* *currently online*

Got 587 DLS, 895 FS, 233 Chats and 25 Admin/Affiliates pages.

Currently tracking 121 forums & markets across 213 relays & mirrors - *91* *currently online*

Currently tracking 284 telegram channels.

There have been 10 posts within the last 24 hours

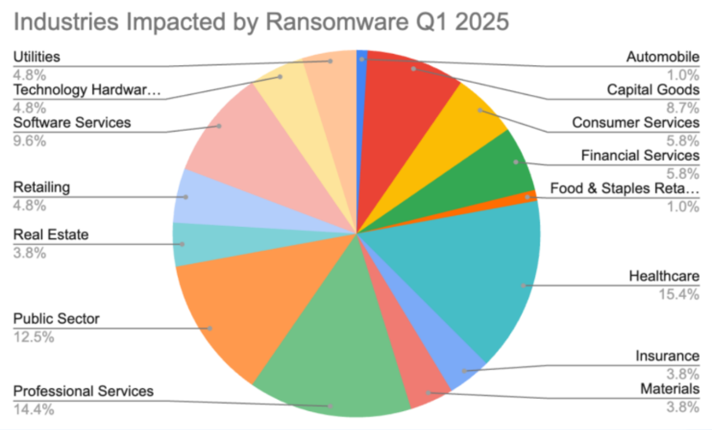
There have been 231 posts within the month of may

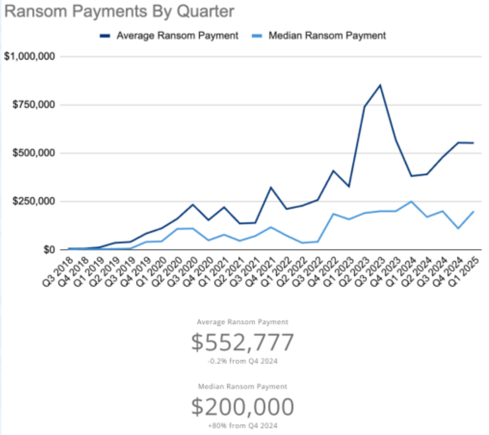
There have been 2339 posts within the last 90 days

There have been 3412 posts within the year of 2025

www.ransomlook.io

Ransomware Facilitator Statistics





Average Ransom Payment

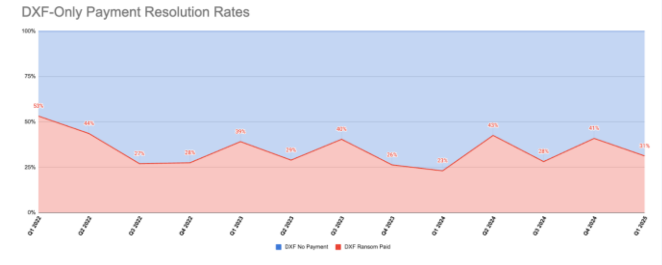
$552,777

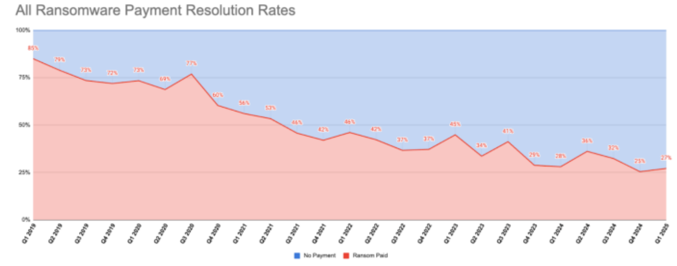
-0.2% from Q4 2024

Median Ransom Payment

$200,000

+80% from Q4 2024





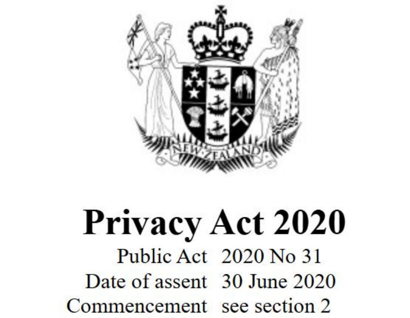
Coveware.com

Cyber Governance – NZ v Australia

New Zealand Government

New Zealand's cyber security strategy 2019

Enabling New Zealand to thrive online



Privacy Act 2020

Public Act	2020 No 31
Date of assent	30 June 2020
Commencement	see section 2

2023–2030
Australian Cyber
Security Strategy

Privacy Act 1988

No. 119, 1988

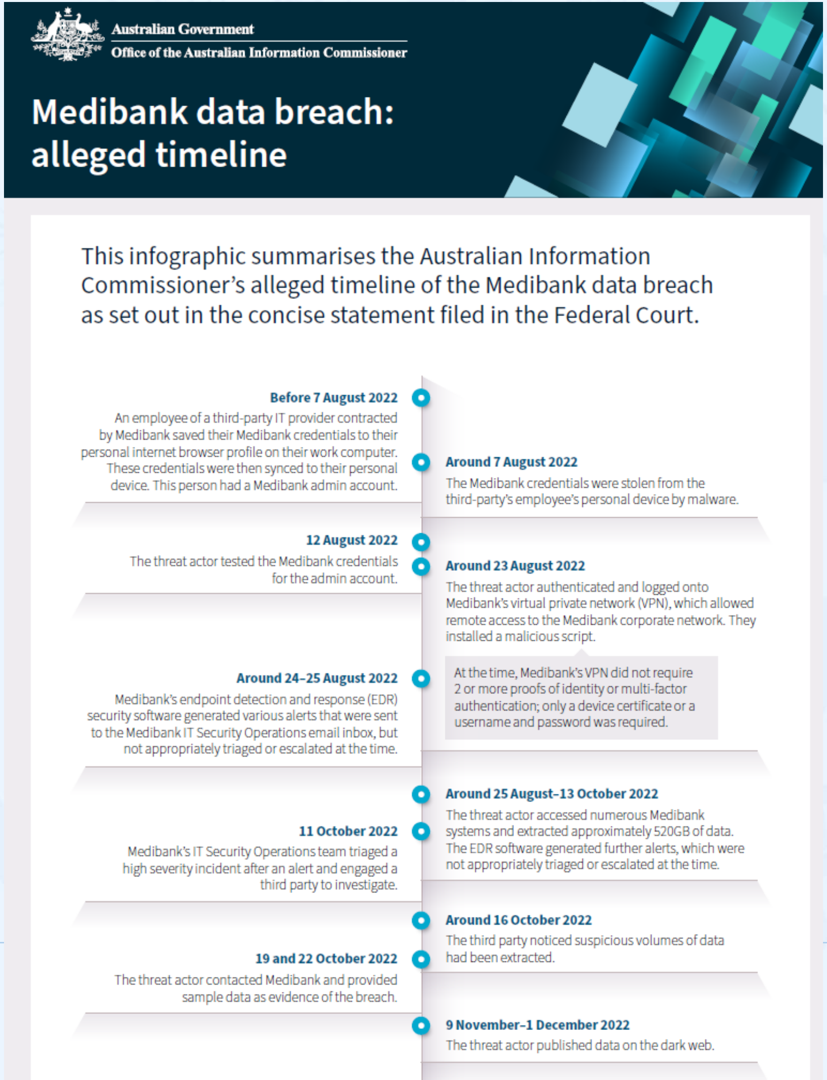
Cyber Security Act 2024

No. 98, 2024

FMA – Increasing Requirements

- In April 2024, the FMA introduced new standard conditions for business continuity and technology systems, along with a new process for reporting operational incidents, effective 1 July 2024.
- Key requirements:
  - Business Continuity Plans: Licence holders must maintain a plan covering response, recovery, and restoration following disruptions, including outsourced arrangements.
  - Critical Technology Systems: They must ensure resilience of systems critical to service provision and compliance, maintaining confidentiality, integrity, and availability.
  - Incident Notification: Licence holders must notify the FMA within 72 hours of any event that significantly impacts critical technology systems. The FMA provides an online notification template for rapid reporting and updates.

OAIC Prosecution of Medibank



Australian Government
Office of the Australian Information Commissioner

Medibank data breach: alleged timeline

This infographic summarises the Australian Information Commissioner's alleged timeline of the Medibank data breach as set out in the concise statement filed in the Federal Court.

Before 7 August 2022
An employee of a third-party IT provider contracted by Medibank saved their Medibank credentials to their personal internet browser profile on their work computer. These credentials were then synced to their personal device. This person had a Medibank admin account.

Around 7 August 2022
The Medibank credentials were stolen from the third-party's employee's personal device by malware.

12 August 2022
The threat actor tested the Medibank credentials for the admin account.

Around 23 August 2022
The threat actor authenticated and logged onto Medibank's virtual private network (VPN), which allowed remote access to the Medibank corporate network. They installed a malicious script.

At the time, Medibank's VPN did not require 2 or more proofs of identity or multi-factor authentication; only a device certificate or a username and password was required.

Around 24–25 August 2022
Medibank's endpoint detection and response (EDR) security software generated various alerts that were sent to the Medibank IT Security Operations email inbox, but not appropriately triaged or escalated at the time.

Around 25 August–13 October 2022
The threat actor accessed numerous Medibank systems and extracted approximately 520GB of data. The EDR software generated further alerts, which were not appropriately triaged or escalated at the time.

11 October 2022
Medibank's IT Security Operations team triaged a high severity incident after an alert and engaged a third party to investigate.

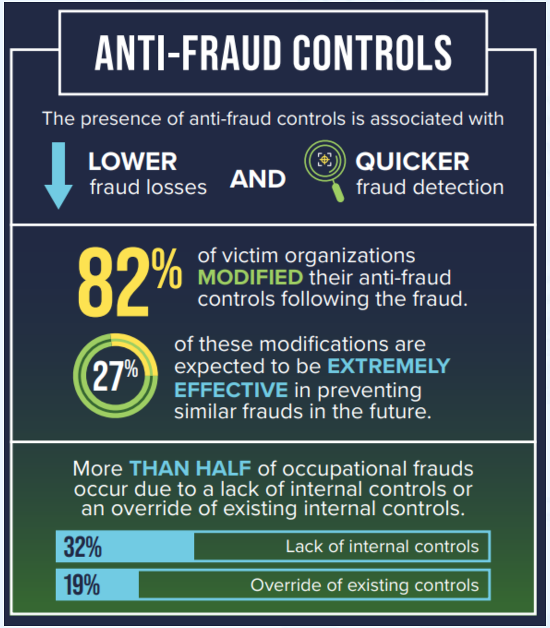
Around 16 October 2022
The third party noticed suspicious volumes of data had been extracted.

19 and 22 October 2022
The threat actor contacted Medibank and provided sample data as evidence of the breach.

9 November–1 December 2022
The threat actor published data on the dark web.

Workplace Risks – ACFE’s 2024 Findings

A TYPICAL FRAUD CASE lasts **12 MONTHS** before detection



ANTI-FRAUD CONTROLS

The presence of anti-fraud controls is associated with

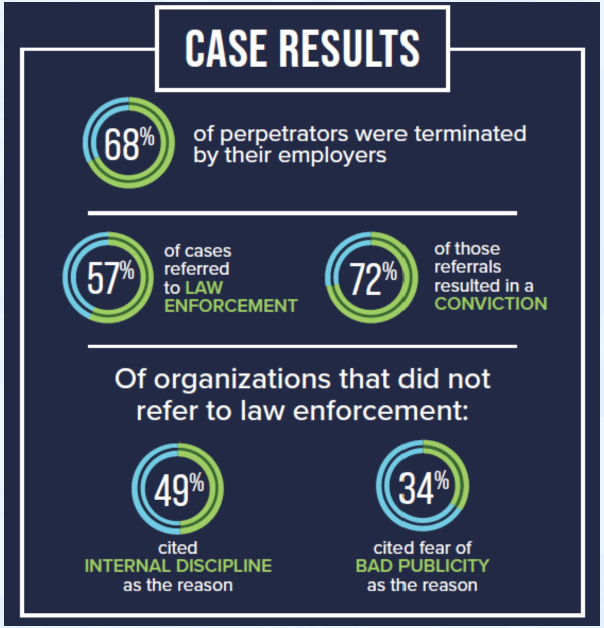
LOWER fraud losses **AND** **QUICKER** fraud detection

82% of victim organizations **MODIFIED** their anti-fraud controls following the fraud.

27% of these modifications are expected to be **EXTREMELY EFFECTIVE** in preventing similar frauds in the future.

More **THAN HALF** of occupational frauds occur due to a lack of internal controls or an override of existing internal controls.

32%	Lack of internal controls
19%	Override of existing controls



CASE RESULTS

68% of perpetrators were terminated by their employers

57% of cases referred to **LAW ENFORCEMENT**

72% of those referrals resulted in a **CONVICTION**

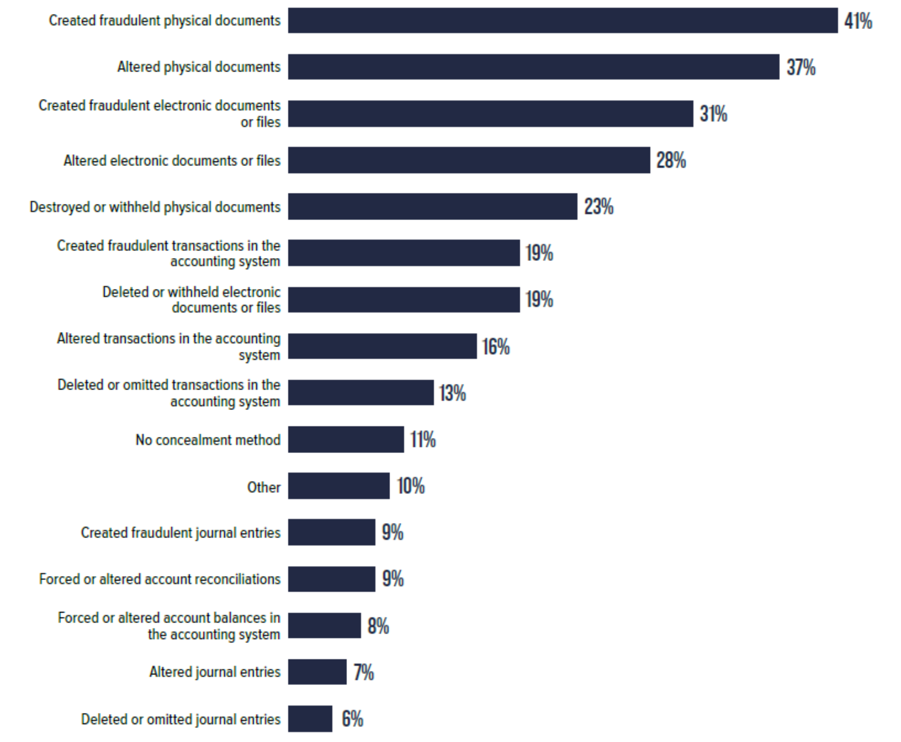
Of organizations that did not refer to law enforcement:

49% cited **INTERNAL DISCIPLINE** as the reason

34% cited fear of **BAD PUBLICITY** as the reason

www.acfe.com

ACFE – Fraudsters Concealment

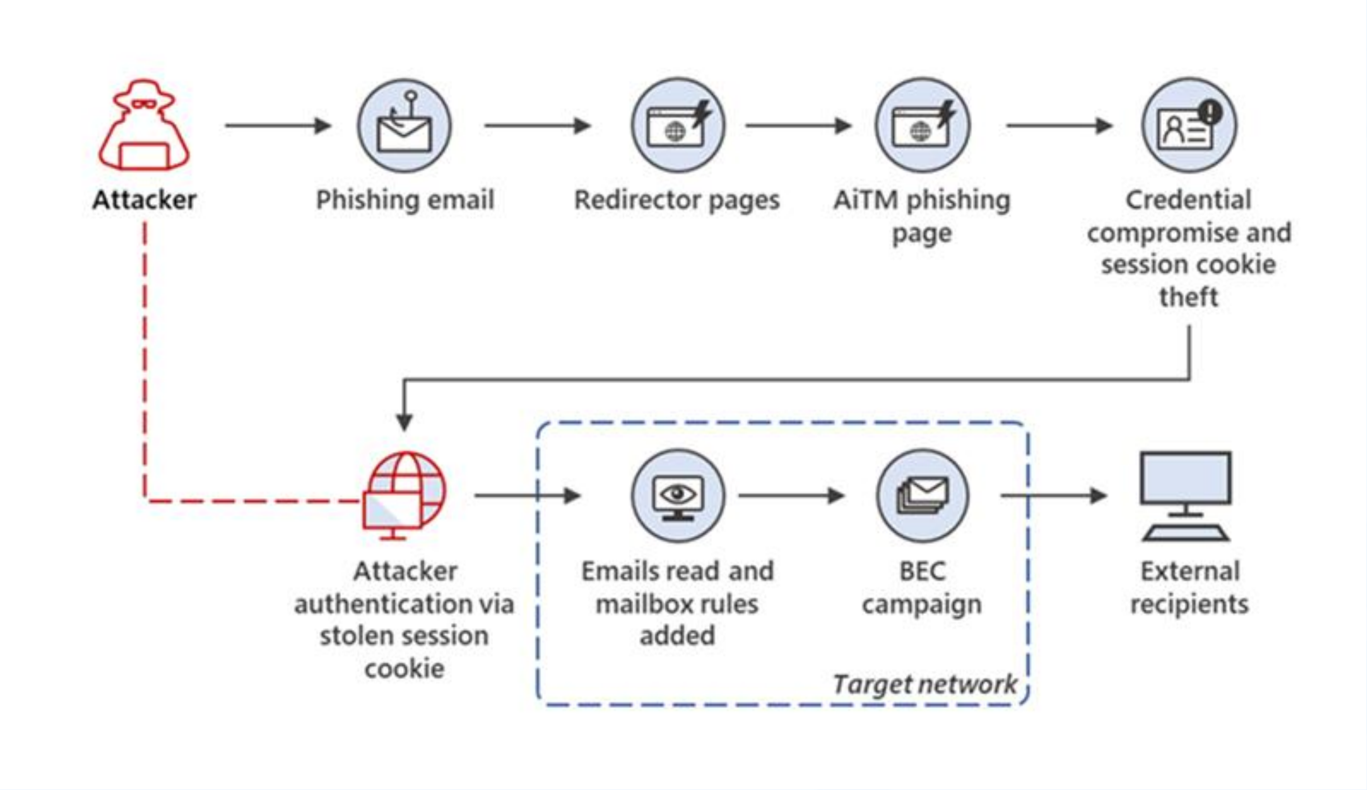


www.acfe.com

Emerging Technologies

Threats and Opportunities

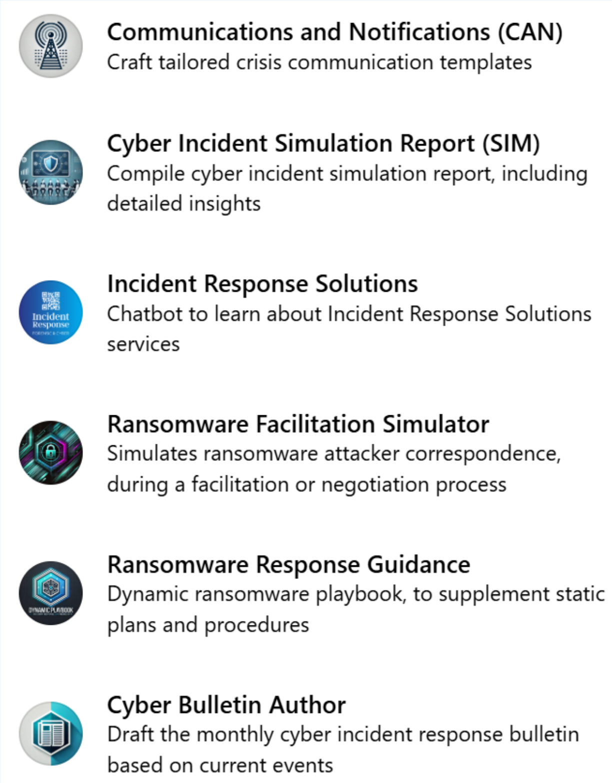
Business Email Compromise – Post MFA


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
Target network
External recipients

DBIR - AI

- Some evidence of use by threat actors.
- Synthetically generated text in malicious emails has doubled over the past two years.
- 15% of employees were routinely accessing GenAI systems on their corporate devices.
- Emerging threat is corporate-sensitive data leakage to the GenAI platforms.
- 72% using non-corporate emails as the identifiers of their accounts and 17% without integrated authentication systems, most likely suggesting use outside of corporate policy.

AI - Opportunities



Communications and Notifications (CAN)
Craft tailored crisis communication templates

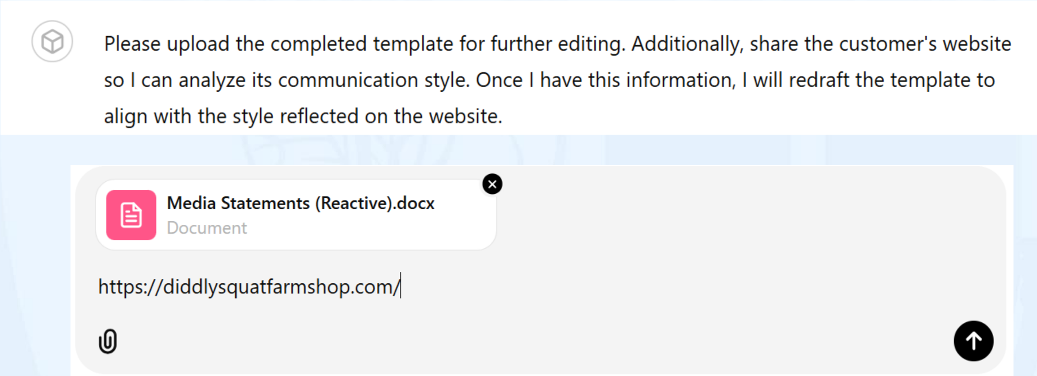
Cyber Incident Simulation Report (SIM)
Compile cyber incident simulation report, including detailed insights

Incident Response Solutions
Chatbot to learn about Incident Response Solutions services

Ransomware Facilitation Simulator
Simulates ransomware attacker correspondence, during a facilitation or negotiation process

Ransomware Response Guidance
Dynamic ransomware playbook, to supplement static plans and procedures

Cyber Bulletin Author
Draft the monthly cyber incident response bulletin based on current events

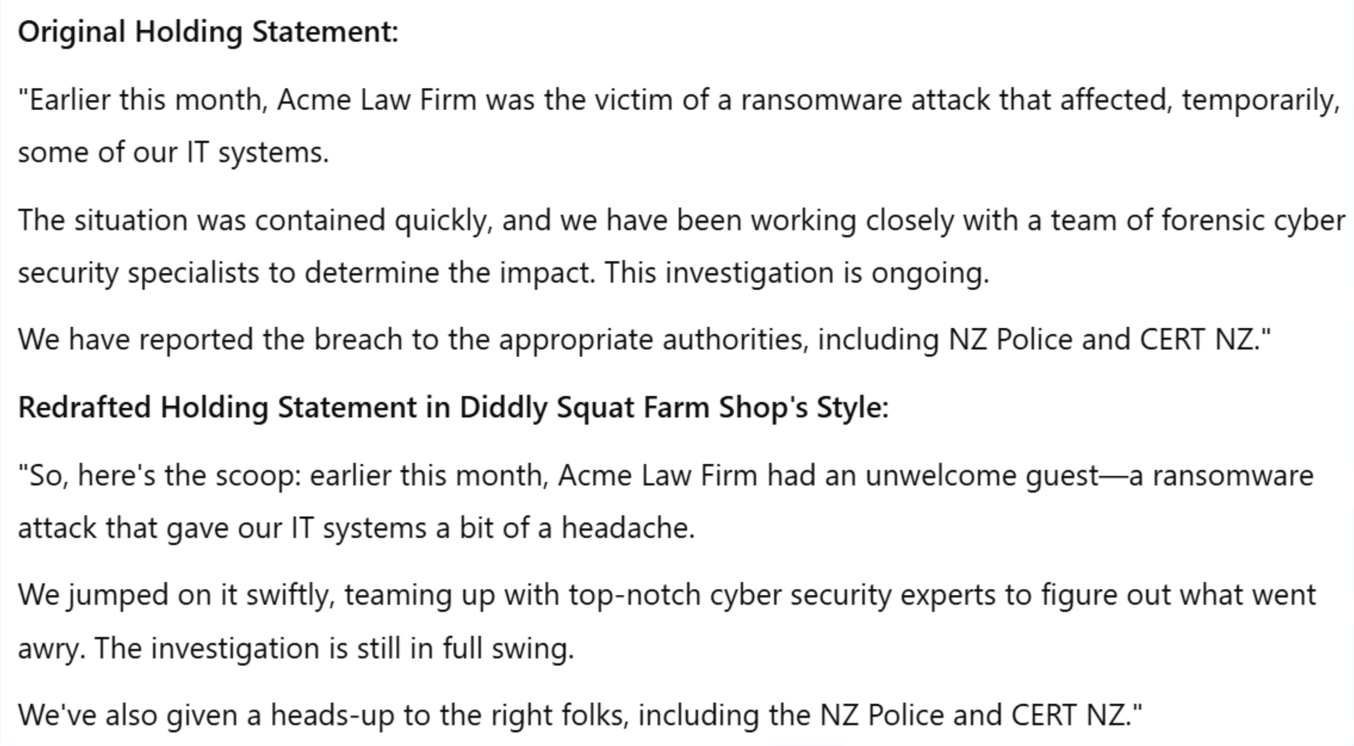


Please upload the completed template for further editing. Additionally, share the customer's website so I can analyze its communication style. Once I have this information, I will redraft the template to align with the style reflected on the website.

Media Statements (Reactive).docx
Document

https://diddlysquatfarmshop.com/

AI – Media Statements



Original Holding Statement:

"Earlier this month, Acme Law Firm was the victim of a ransomware attack that affected, temporarily, some of our IT systems.

The situation was contained quickly, and we have been working closely with a team of forensic cyber security specialists to determine the impact. This investigation is ongoing.

We have reported the breach to the appropriate authorities, including NZ Police and CERT NZ."

Redrafted Holding Statement in Diddly Squat Farm Shop's Style:

"So, here's the scoop: earlier this month, Acme Law Firm had an unwelcome guest—a ransomware attack that gave our IT systems a bit of a headache.

We jumped on it swiftly, teaming up with top-notch cyber security experts to figure out what went awry. The investigation is still in full swing.

We've also given a heads-up to the right folks, including the NZ Police and CERT NZ."

AI - Expert Witness

Example 1 - Courts

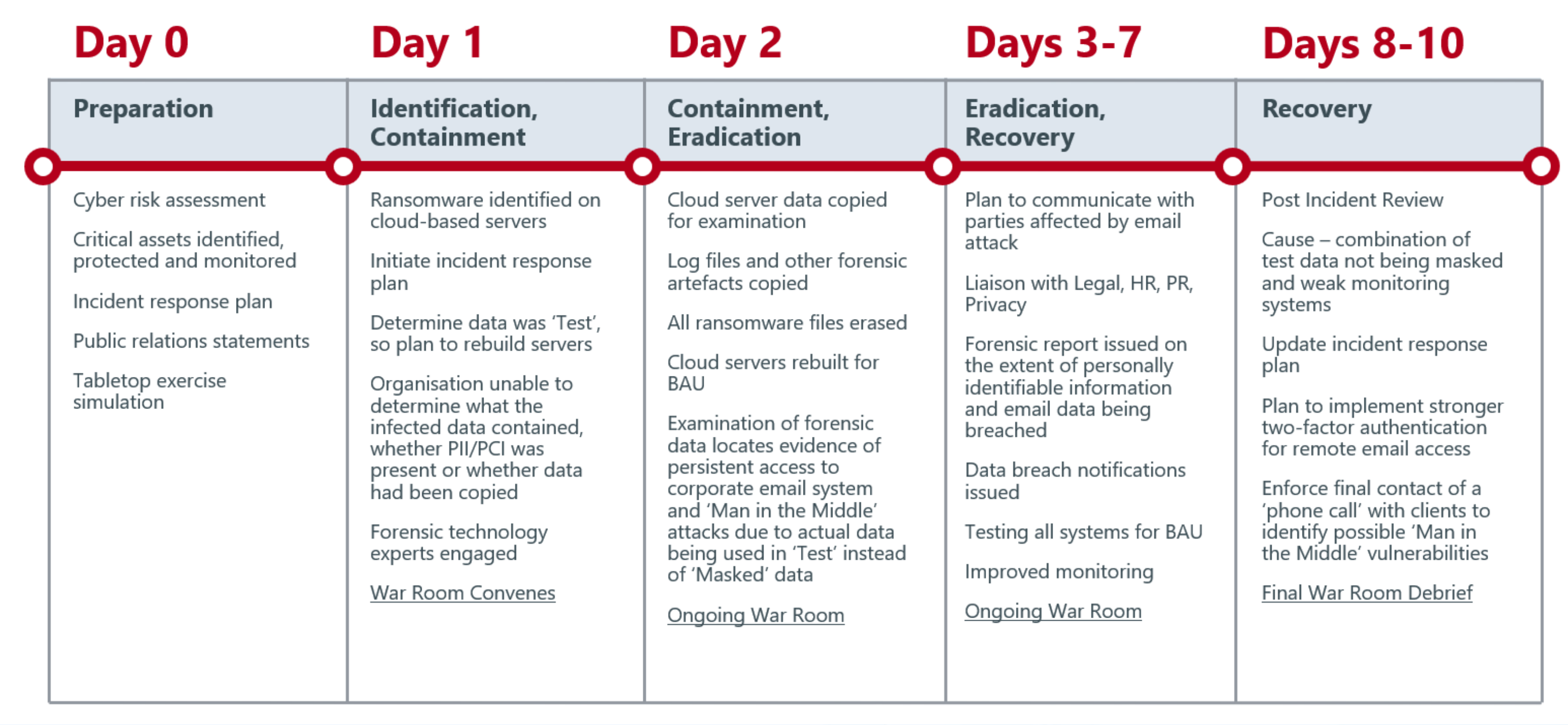
- Forensic Expert Witness consulting on eDiscovery to Law Firm and Client.
- Continuous Active Learning involving ~500,000 documents.
- Lawyers reviewed ~20% of the documents.

Example 2 - Regulator

- Forensic Expert Witness consulting on Privacy Breach to Insurers, Insured and Law Firm, for provision to OPC.
- AI involving ~200,000 documents.
- Lawyers reviewed ~4% of the documents.

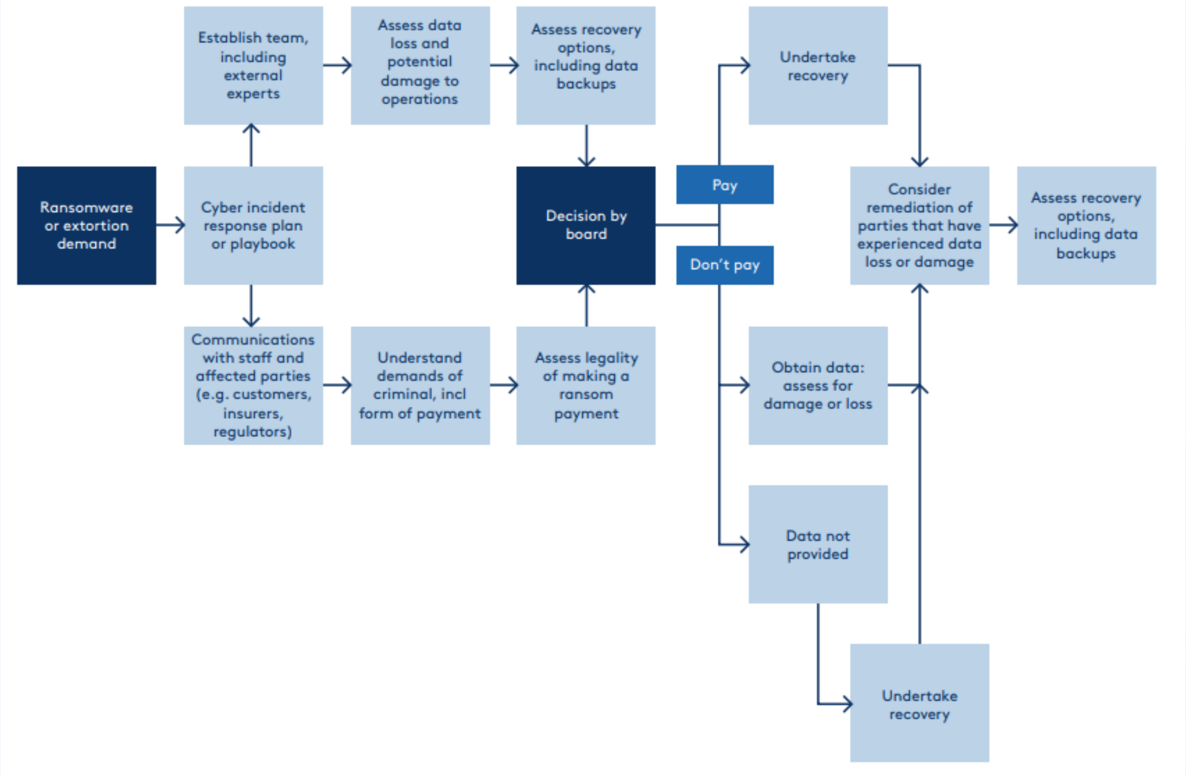
Case Studies

Ransomware – Availability and Confidentiality



Day 0	Day 1	Day 2	Days 3-7	Days 8-10
Preparation	**Identification, Containment**	**Containment, Eradication**	**Eradication, Recovery**	**Recovery**
Cyber risk assessment Critical assets identified, protected and monitored Incident response plan Public relations statements Tabletop exercise simulation	Ransomware identified on cloud-based servers Initiate incident response plan Determine data was 'Test', so plan to rebuild servers Organisation unable to determine what the infected data contained, whether PII/PCI was present or whether data had been copied Forensic technology experts engaged War Room Convenes	Cloud server data copied for examination Log files and other forensic artefacts copied All ransomware files erased Cloud servers rebuilt for BAU Examination of forensic data locates evidence of persistent access to corporate email system and 'Man in the Middle' attacks due to actual data being used in 'Test' instead of 'Masked' data Ongoing War Room	Plan to communicate with parties affected by email attack Liaison with Legal, HR, PR, Privacy Forensic report issued on the extent of personally identifiable information and email data being breached Data breach notifications issued Testing all systems for BAU Improved monitoring Ongoing War Room	Post Incident Review Cause – combination of test data not being masked and weak monitoring systems Update incident response plan Plan to implement stronger two-factor authentication for remote email access Enforce final contact of a 'phone call' with clients to identify possible 'Man in the Middle' vulnerabilities Final War Room Debrief

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

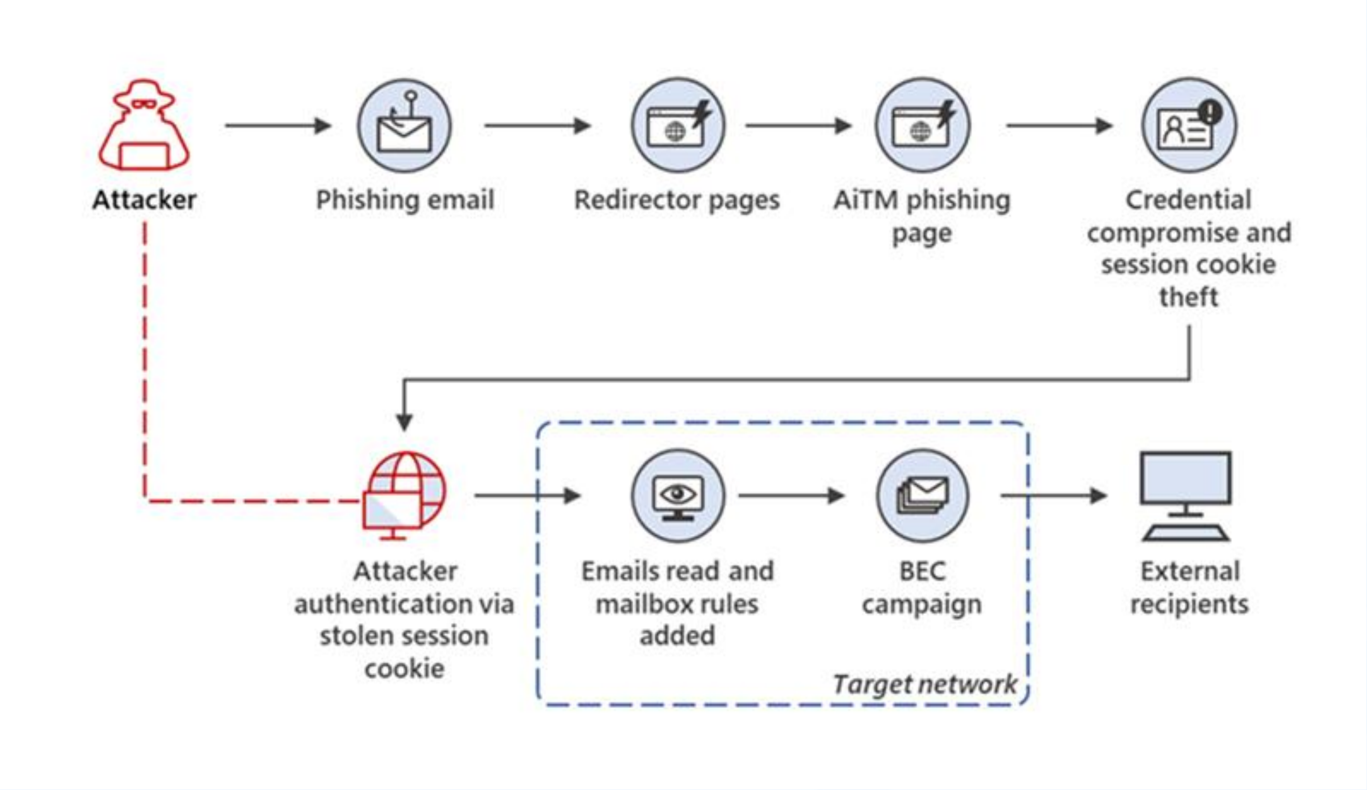
Undertake recovery

Consider remediation of parties that have experienced data loss or damage

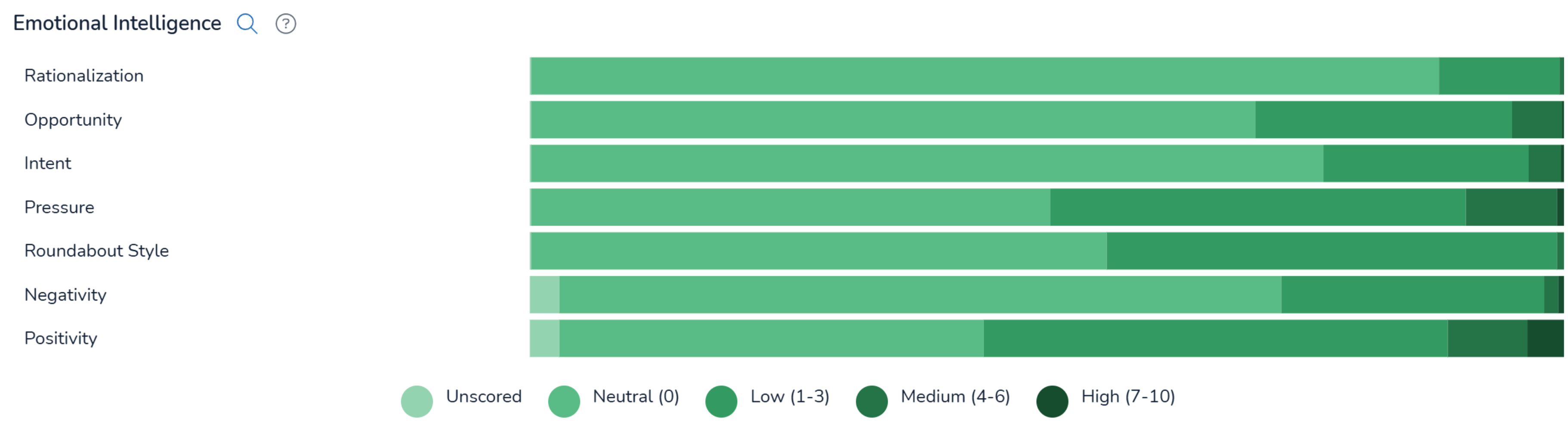
Assess recovery options, including data backups

www.aicd.com.au

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

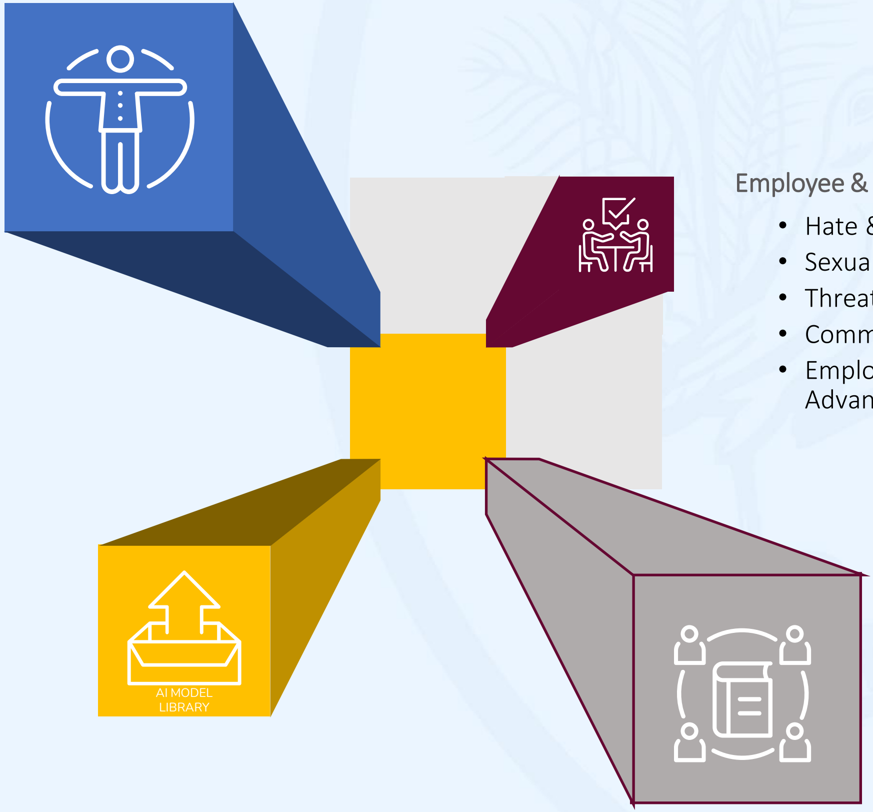
Fraud Investigation



Supervised / Continuous Active Learning

Fraud, Ethics, FCPA Investigations, & Litigation

- Employment & Career Advancement
- Contracts
- Gifts & Entertainment Kickbacks
- Work Events
- Advertisements & Promotions
- Pricing & Fees
- Asking for Advice



Employee & HR Issues

- Hate & Discrimination
- Sexually Explicit Comments
- Threatening Behavior
- Comments on Appearance
- Employment & Career Advancement

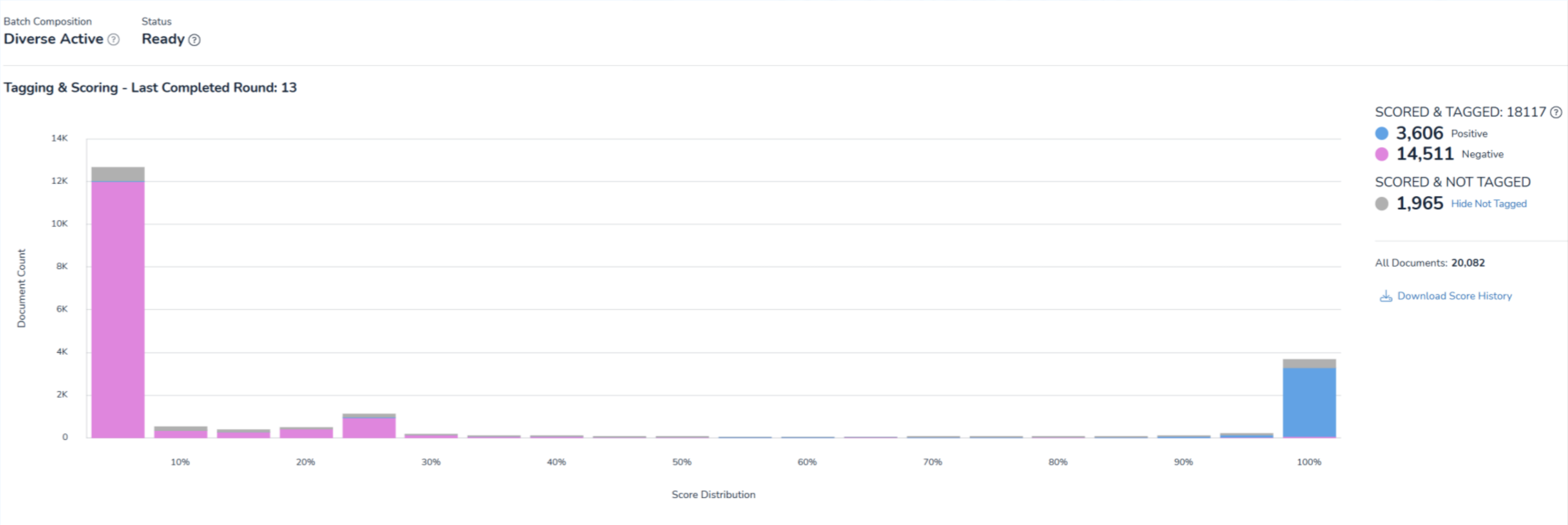
IRS Custom AI Models

- Privacy Breach
- Fraud
- Cartel
- Conflict of Interest
- Employment
- Health and Safety

Data Breach & Sensitive Data

- Privileged Content
- Contracts

Supervised / Continuous Active Learning



Batch Composition

Diverse Active ⓘ

Status

Ready ⓘ

Tagging & Scoring - Last Completed Round: 13

SCORED & TAGGED: 18117 ⓘ

● 3,606 Positive

● 14,511 Negative

SCORED & NOT TAGGED

● 1,965 Hide Not Tagged

All Documents: **20,082**

Download Score History

Image Labeling

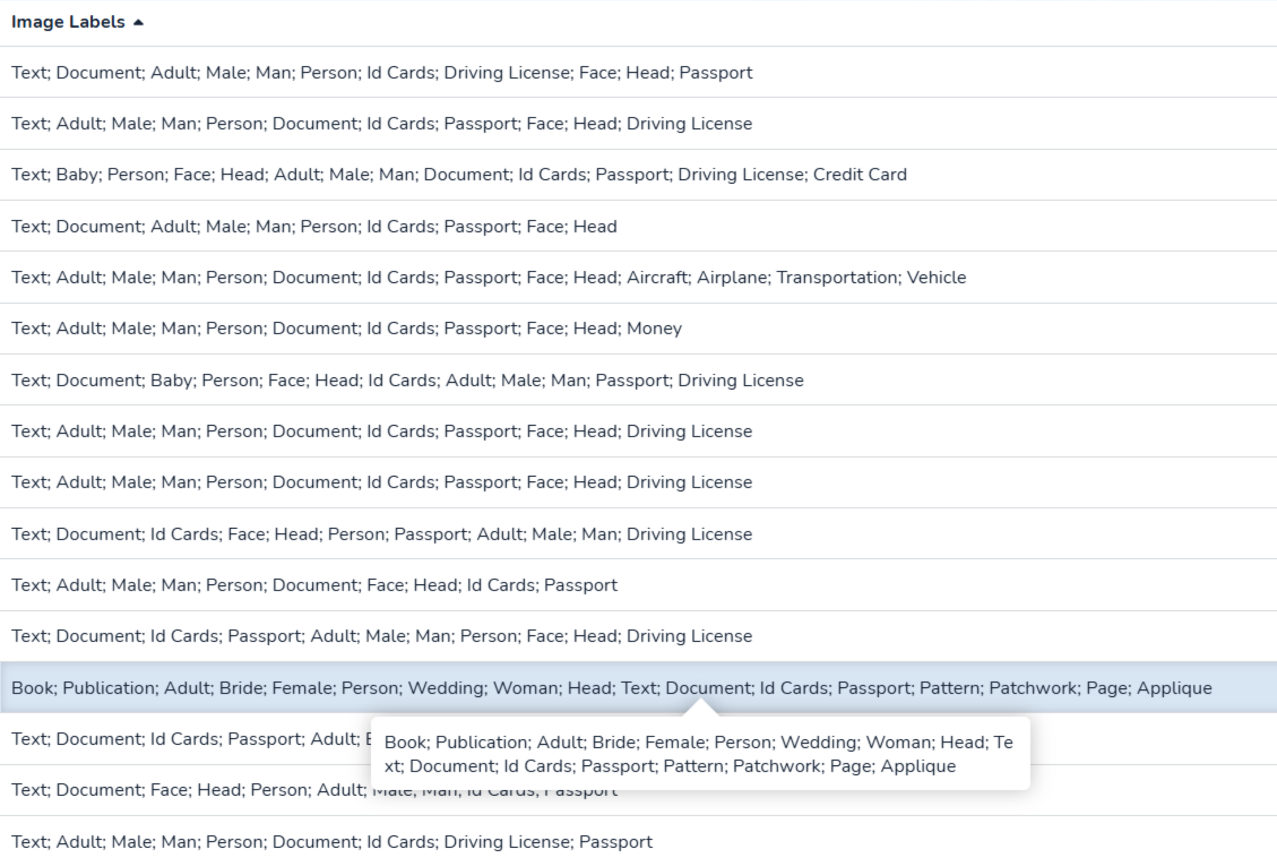
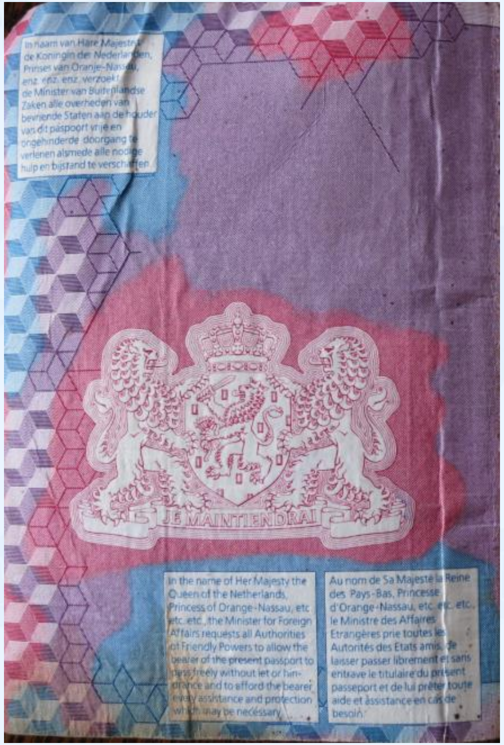


Image Labels ▲
Text; Document; Adult; Male; Man; Person; Id Cards; Driving License; Face; Head; Passport
Text; Adult; Male; Man; Person; Document; Id Cards; Passport; Face; Head; Driving License
Text; Baby; Person; Face; Head; Adult; Male; Man; Document; Id Cards; Passport; Driving License; Credit Card
Text; Document; Adult; Male; Man; Person; Id Cards; Passport; Face; Head
Text; Adult; Male; Man; Person; Document; Id Cards; Passport; Face; Head; Aircraft; Airplane; Transportation; Vehicle
Text; Adult; Male; Man; Person; Document; Id Cards; Passport; Face; Head; Money
Text; Document; Baby; Person; Face; Head; Id Cards; Adult; Male; Man; Passport; Driving License
Text; Adult; Male; Man; Person; Document; Id Cards; Passport; Face; Head; Driving License
Text; Adult; Male; Man; Person; Document; Id Cards; Passport; Face; Head; Driving License
Text; Document; Id Cards; Face; Head; Person; Passport; Adult; Male; Man; Driving License
Text; Adult; Male; Man; Person; Document; Face; Head; Id Cards; Passport
Text; Document; Id Cards; Passport; Adult; Male; Man; Person; Face; Head; Driving License
Book; Publication; Adult; Bride; Female; Person; Wedding; Woman; Head; Text; Document; Id Cards; Passport; Pattern; Patchwork; Page; Applique
Text; Document; Id Cards; Passport; Adult; E
Text; Document; Face; Head; Person; Adult; Male; Man; Id Cards; Passport
Text; Adult; Male; Man; Person; Document; Id Cards; Driving License; Passport

Book; Publication; Adult; Bride; Female; Person; Wedding; Woman; Head; Text; Document; Id Cards; Passport; Pattern; Patchwork; Page; Applique

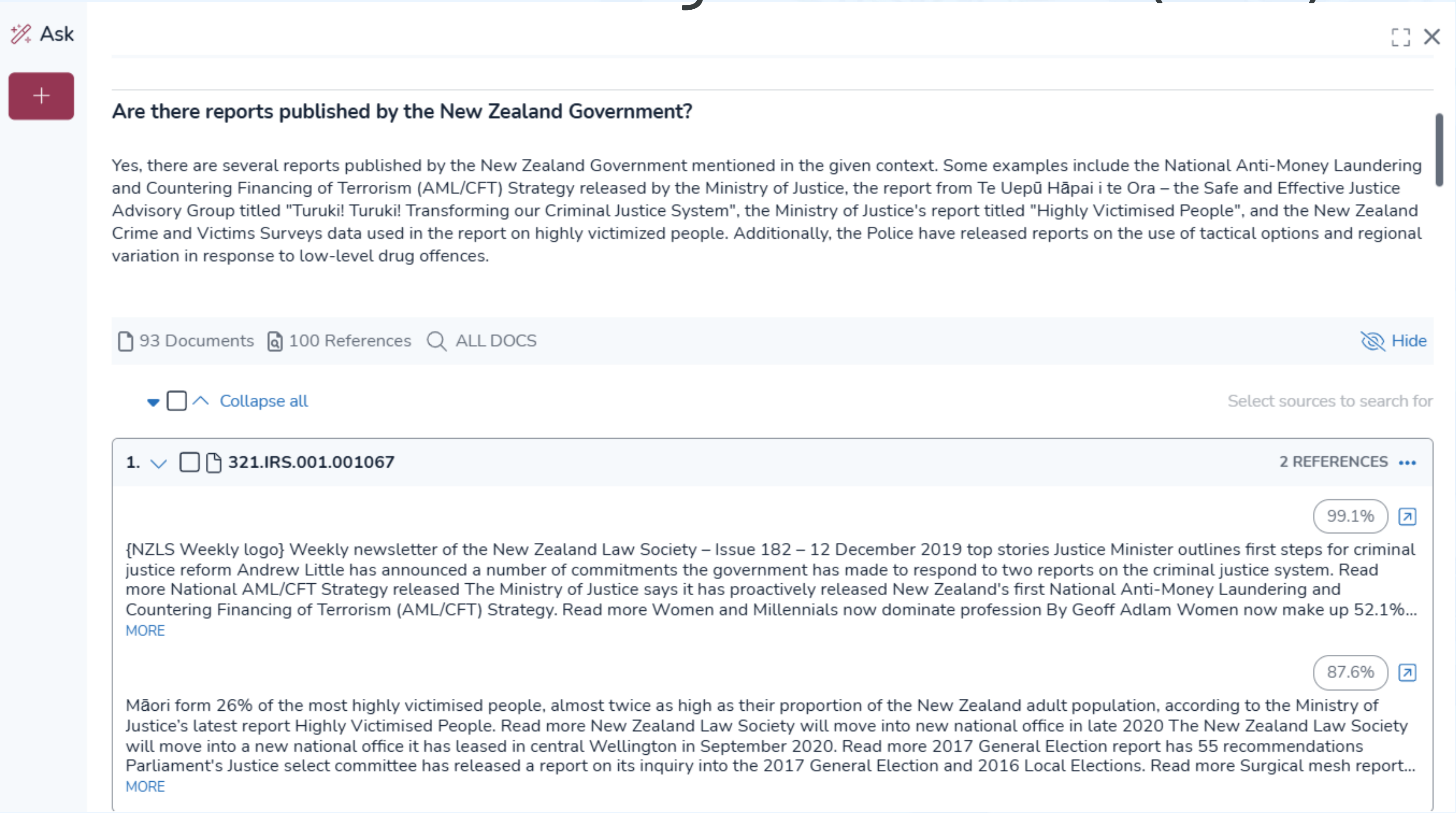


In naam van Hare Majesteit de Koningin der Nederlanden, Prinses van Oranje-Nassau, enz. enz. enz. verzoekt de Minister van Buitenlandse Zaken alle overheden van bevriende Staten aan de houder van dit paspoort vrije en ongehinderde doorgang te verlenen alsmede alle nodige hulp en bijstand te verschaffen

In the name of Her Majesty the Queen of the Netherlands, Princess of Orange-Nassau, etc etc. etc., the Minister for Foreign Affairs requests all Authorities of Friendly Powers to allow the bearer of the present passport to pass freely without let or hindrance and to afford the bearer every assistance and protection which may be necessary

Au nom de Sa Majesté la Reine des Pays-Bas, Princesse d'Orange-Nassau, etc. etc. etc., le Ministre des Affaires Etrangères prie toutes les Autorités des Etats amis de laisser passer librement et sans entrave le titulaire du présent passeport et de lui prêter toute aide et assistance en cas de besoin

Generative Pre-training Transformer (GPT)



Are there reports published by the New Zealand Government?

Yes, there are several reports published by the New Zealand Government mentioned in the given context. Some examples include the National Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT) Strategy released by the Ministry of Justice, the report from Te Uepū Hāpai i te Ora – the Safe and Effective Justice Advisory Group titled "Turuki! Turuki! Transforming our Criminal Justice System", the Ministry of Justice's report titled "Highly Victimised People", and the New Zealand Crime and Victims Surveys data used in the report on highly victimized people. Additionally, the Police have released reports on the use of tactical options and regional variation in response to low-level drug offences.

93 Documents 100 References ALL DOCS

1. 321.IRS.001.001067 2 REFERENCES

99.1%

{NZLS Weekly logo} Weekly newsletter of the New Zealand Law Society – Issue 182 – 12 December 2019 top stories Justice Minister outlines first steps for criminal justice reform Andrew Little has announced a number of commitments the government has made to respond to two reports on the criminal justice system. Read more National AML/CFT Strategy released The Ministry of Justice says it has proactively released New Zealand's first National Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT) Strategy. Read more Women and Millennials now dominate profession By Geoff Adlam Women now make up 52.1%...
MORE

87.6%

Māori form 26% of the most highly victimised people, almost twice as high as their proportion of the New Zealand adult population, according to the Ministry of Justice's latest report Highly Victimised People. Read more New Zealand Law Society will move into new national office in late 2020 The New Zealand Law Society will move into a new national office it has leased in central Wellington in September 2020. Read more 2017 General Election report has 55 recommendations Parliament's Justice select committee has released a report on its inquiry into the 2017 General Election and 2016 Local Elections. Read more Surgical mesh report...
MORE

Final Recommendations