Incident
Response
FORENSIC & CYBER

“Cyber”

NZCA

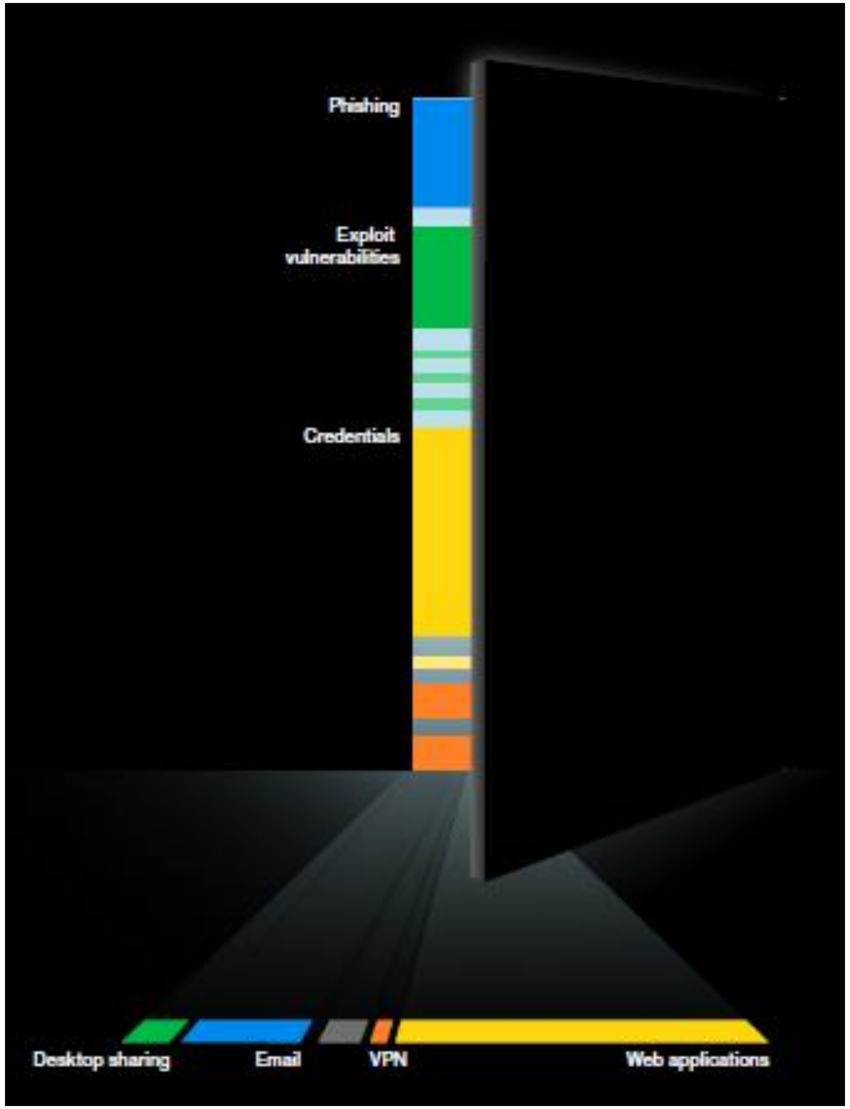
About Incident Response Solutions

- 6 Fulltime staff + Contractors and Wider Ecosystem
- Insurance, Law Firms, IT/Security Firms, Direct
- Digital Forensic Incident Response (DFIR)
- Technology Stack – Google, Microsoft, Nuix, Axiom, Cellebrite, etc – Thinkific
- AI – GPT and other uses
- Solutions for Insureds

Case Study – Accounting Firm Ransomware Attack and BEC

Verizon 2024 Data Breach Investigations Report

- 17th Edition
- Over 1 million datapoints
- 30,458 security incidents that compromised the integrity, confidentiality or availability of an information asset.
- 10,626 breaches that resulted in the confirmed disclosure of data to an unauthorised party.



verizon.com/dbir

What Verizon Found – Key Statistics

- **68%** of all breaches include the human element

  Error, stolen credentials or Social Engineering (Privilege Misuse removed)

- **40%** of all Social Engineering incidents used pretexting

  Phishing and Pretexting via email make up 73% of social engineering attacks - targeting users with existing email chains and context

- **32%** of all breaches involved ransomware & extortion

  Maliciously encrypting data and demanding a ransom to return or unlock it

- **35%** involved internal actors

  Intentional and unintentional harm through misuse and simple human errors

- **68%** increase in breaches involving a third party
- **95%** of breaches are financially driven

  It's (almost) always about the money

Statistics at a glance

Globally

40+ billion records

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

150% increase

in data breaches from a year earlier.

21,957

common vulnerabilities and exposures[2]

$945 billion

Losses to businesses in 2020
from cybercrime.[3]

$145 billion

spent on cyber security by businesses in 2020, more than double 2018.[4]

38%

of data breaches reported are ransomware attacks[5]

43%

of cyber attacks target small business.[6]

Australia[7]

$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 2020[10]

[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

CHARTERED ACCOUNTANTS™
AUSTRALIA + NEW ZEALAND

DIFFERENCE MAKERS™

US Government - Risk Vulnerability Analysis 2023

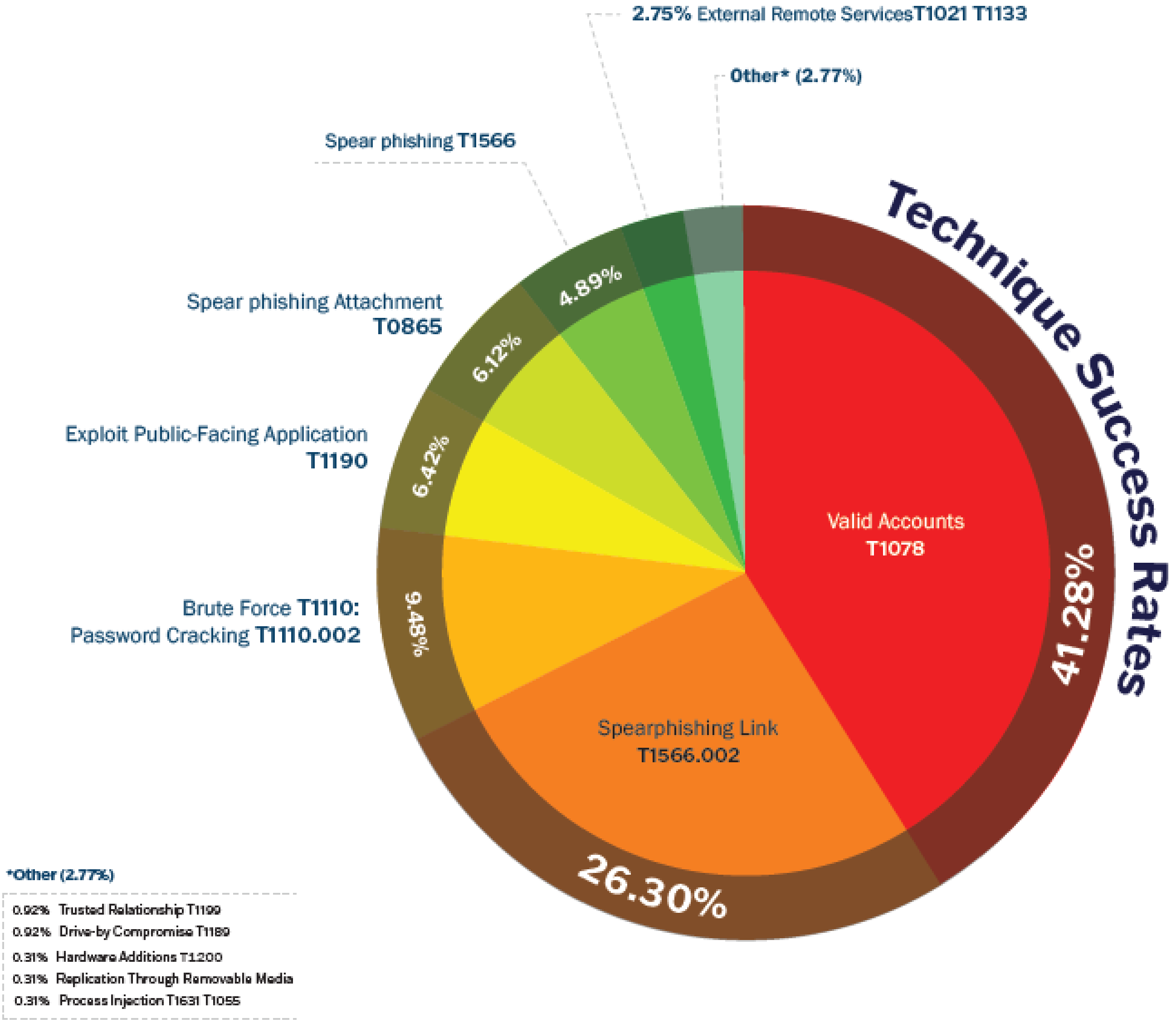
FY23 RVA Results

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.

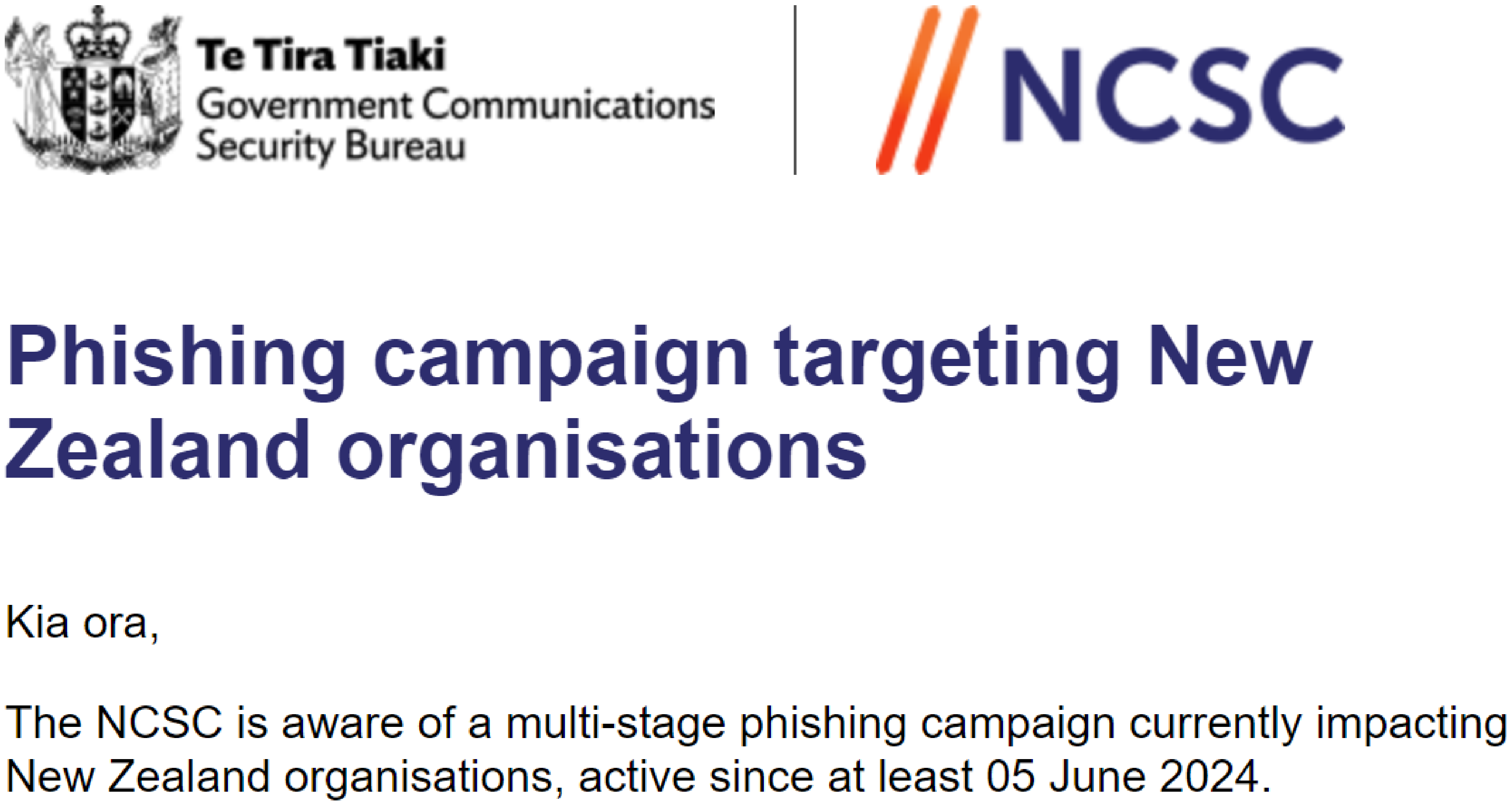
- Cracking password hashes (89% Administrator accounts)
- Default or stolen administrator accounts
- Former employee accounts that have not been removed
- Initial access brokers that sell exploits and valid credentials



*Other (2.77%)

0.92%	Trusted Relationship T1199
0.92%	Drive-by Compromise T1189
0.31%	Hardware Additions T1200
0.31%	Replication Through Removable Media
0.31%	Process Injection T1631 T1055

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



Te Tira Tiaki
Government Communications
Security Bureau

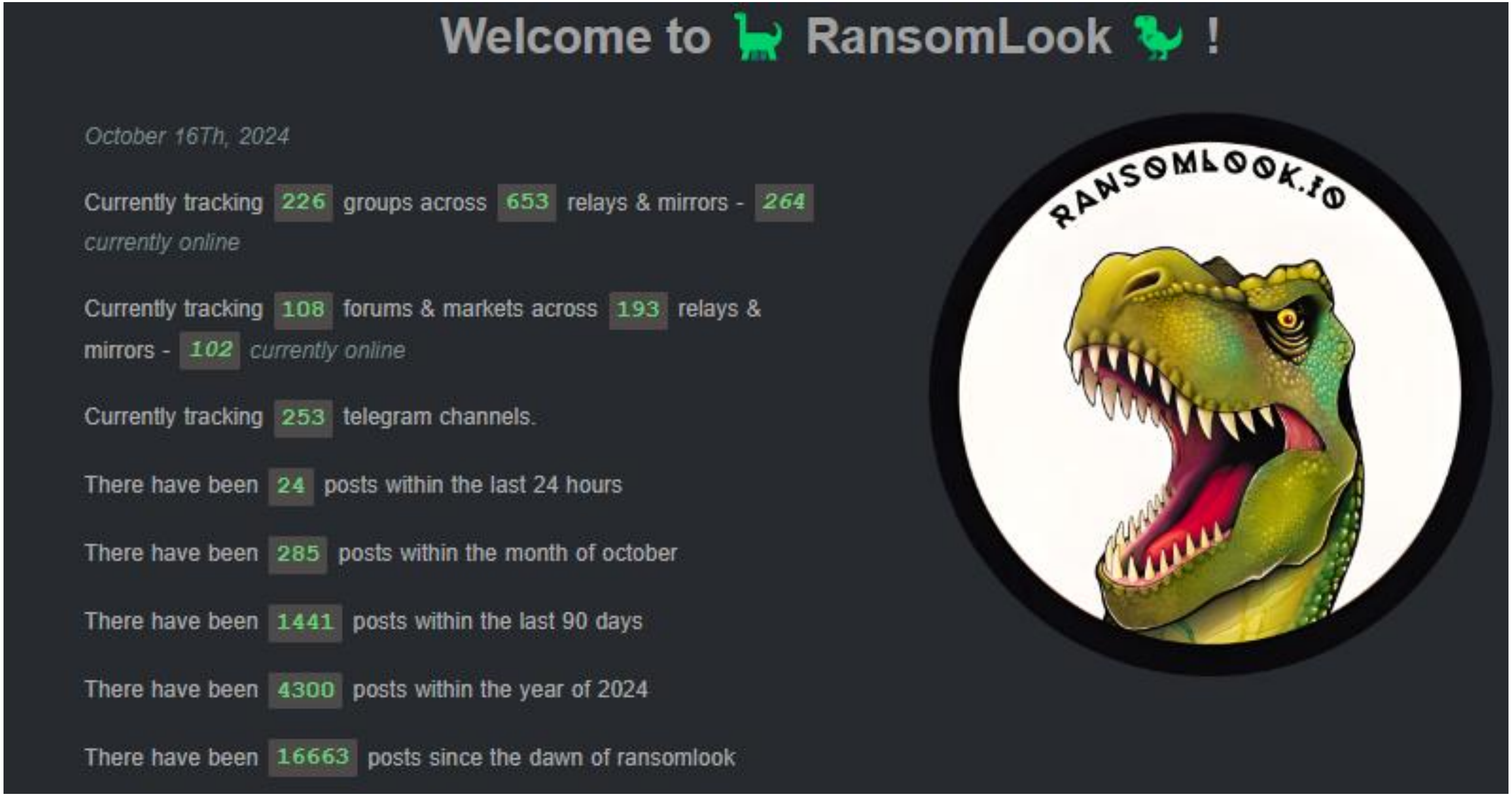
NCSC

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.

State of Ransomware



Welcome to 🦕 RansomLook 🦖 !

October 16Th, 2024

Currently tracking 226 groups across 653 relays & mirrors - *264* *currently online*

Currently tracking 108 forums & markets across 193 relays & mirrors - *102* *currently online*

Currently tracking 253 telegram channels.

There have been 24 posts within the last 24 hours

There have been 285 posts within the month of october

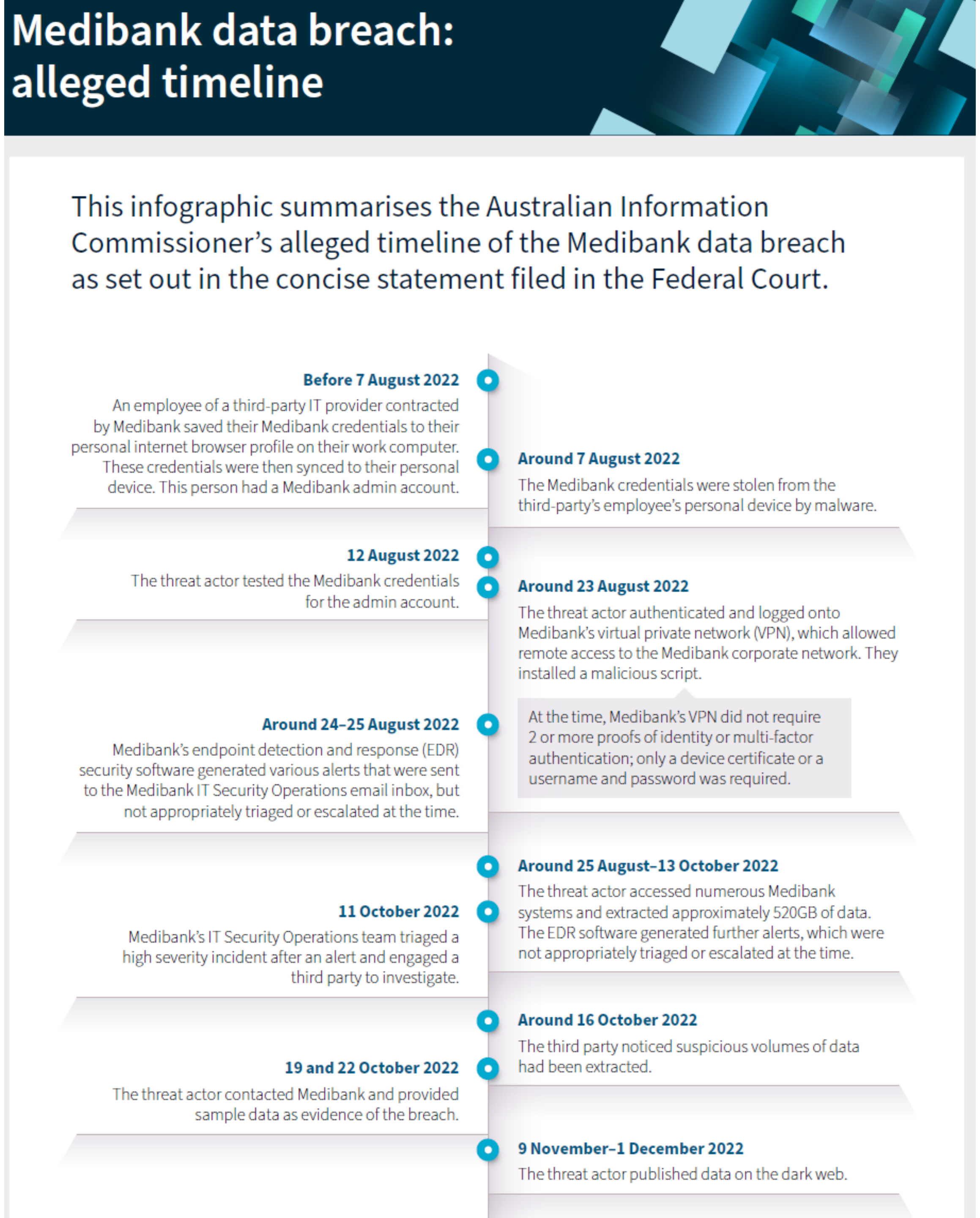
There have been 1441 posts within the last 90 days

There have been 4300 posts within the year of 2024

There have been 16663 posts since the dawn of ransomlook

https://www.ransomlook.io

Regulatory Landscape



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.

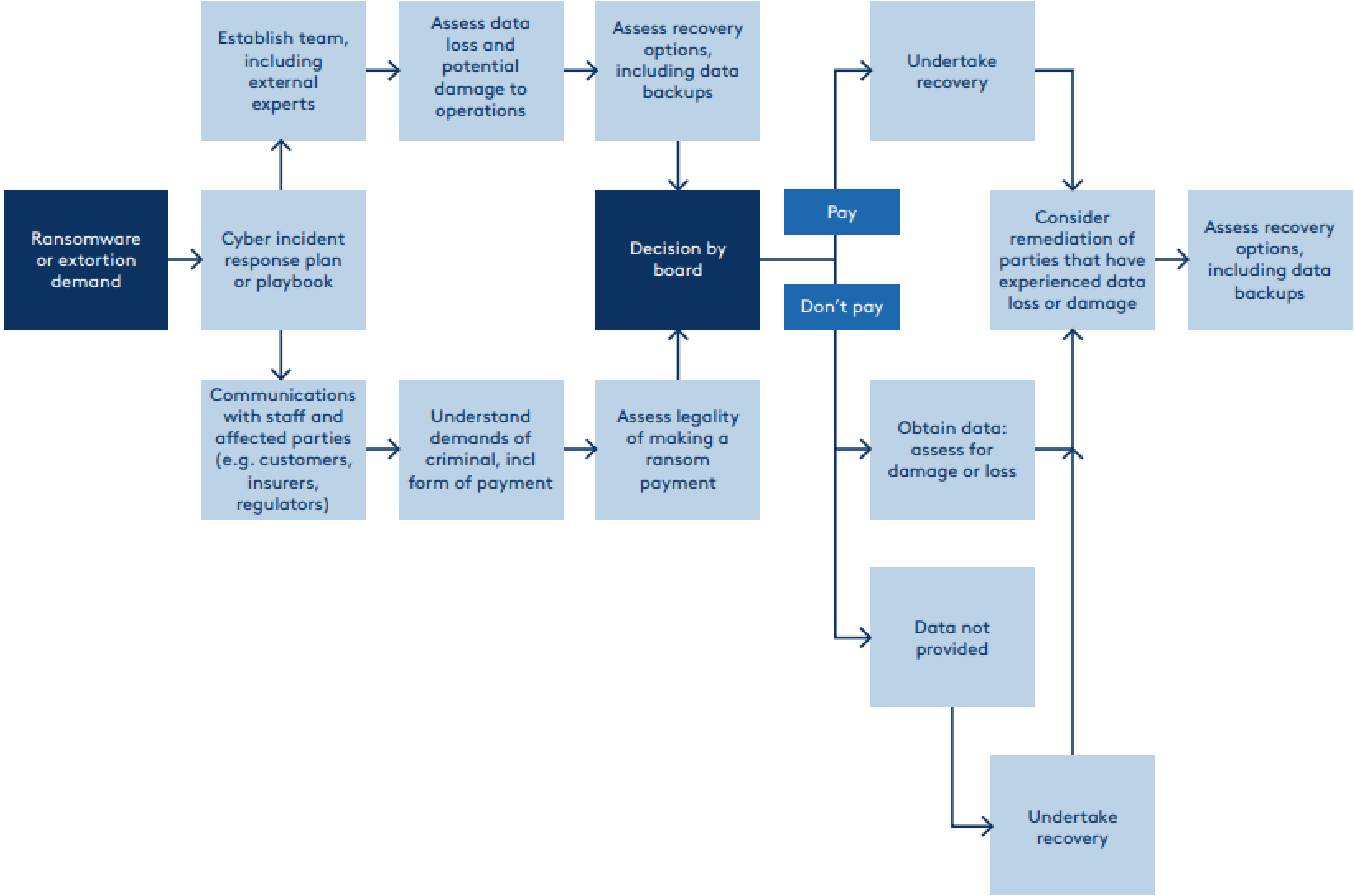
19 and 22 October 2022

The threat actor contacted Medibank and provided sample data as evidence of the breach.

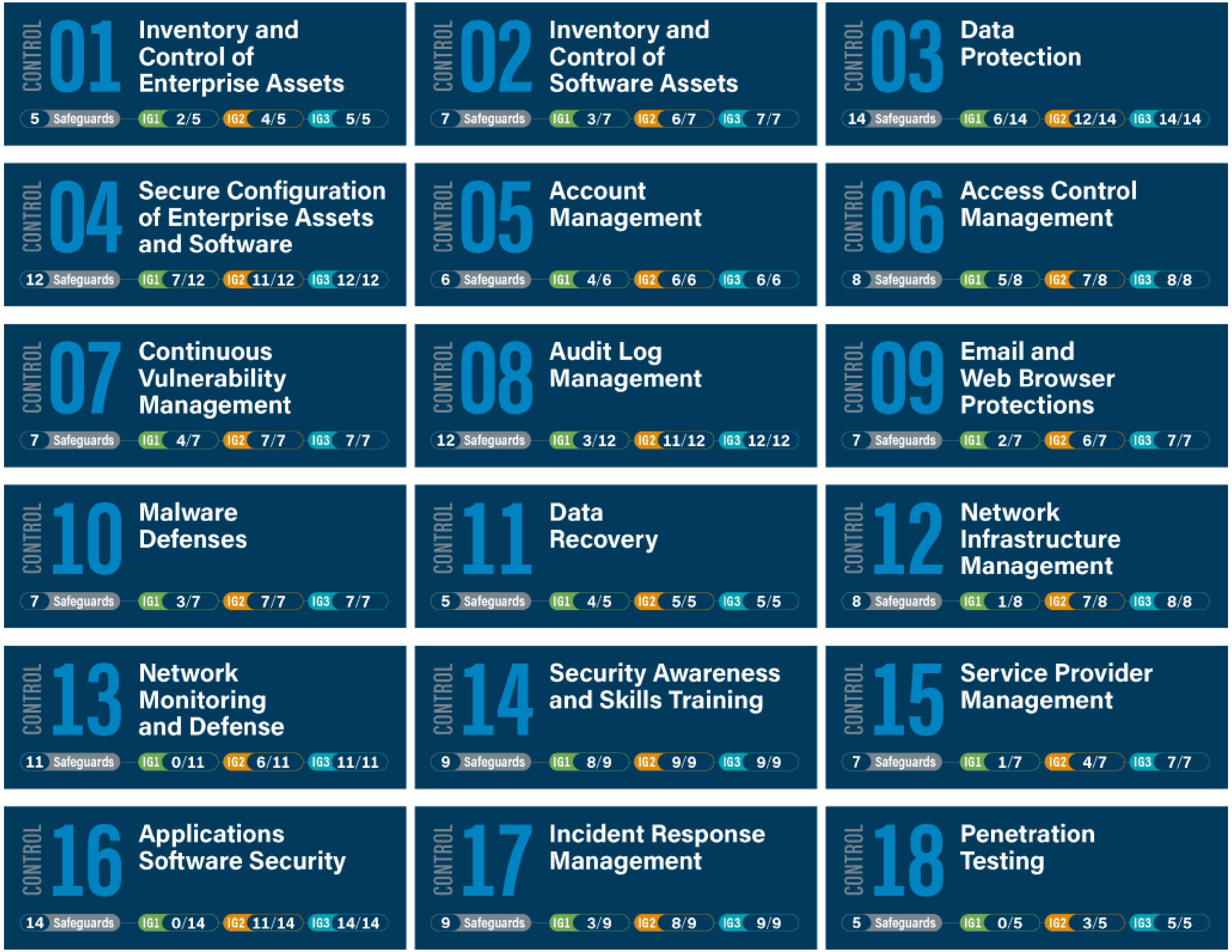
9 November–1 December 2022

The threat actor published data on the dark web.

Ransomware Decision Making Process - AICD

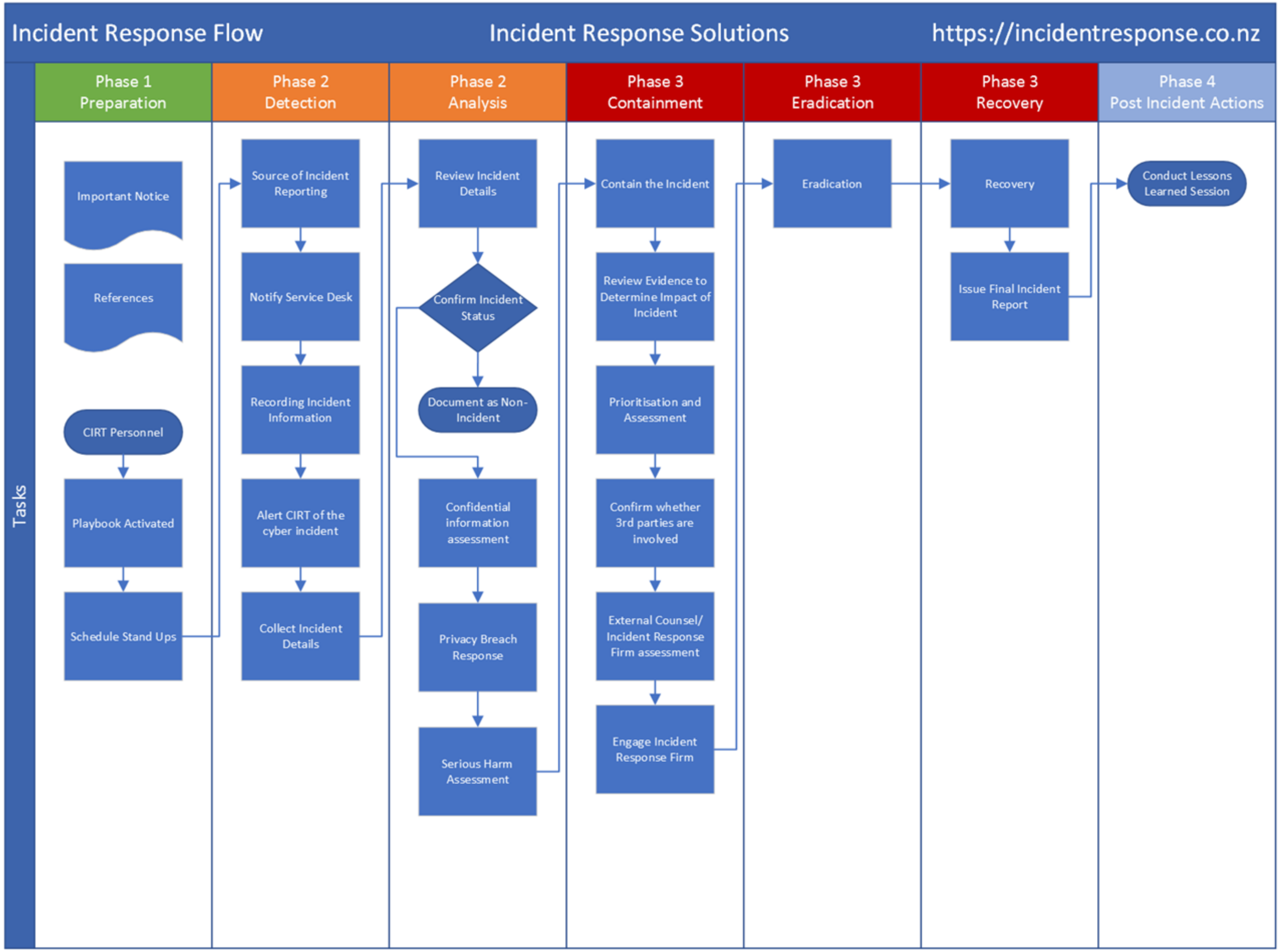

Ransomware or extortion demand
Cyber incident response plan or playbook
Establish team, including external experts
Assess data loss and potential damage to operations
Assess recovery options, including data backups
Communications with staff and affected parties (e.g. customers, insurers, regulators)
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

Cyber Risk Mitigation Strategies



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

Solution - Control Room (Plans and Playbooks)



Incident Response Flow

Incident Response Solutions

https://incidentresponse.co.nz

Tasks

Phase 1 Preparation

Important Notice

References

CIRT Personnel

Playbook Activated

Schedule Stand Ups

Phase 2 Detection

Source of Incident Reporting

Notify Service Desk

Recording Incident Information

Alert CIRT of the cyber incident

Collect Incident Details

Phase 2 Analysis

Review Incident Details

Confirm Incident Status

Document as Non-Incident

Confidential information assessment

Privacy Breach Response

Serious Harm Assessment

Phase 3 Containment

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

Phase 3 Eradication

Eradication

Phase 3 Recovery

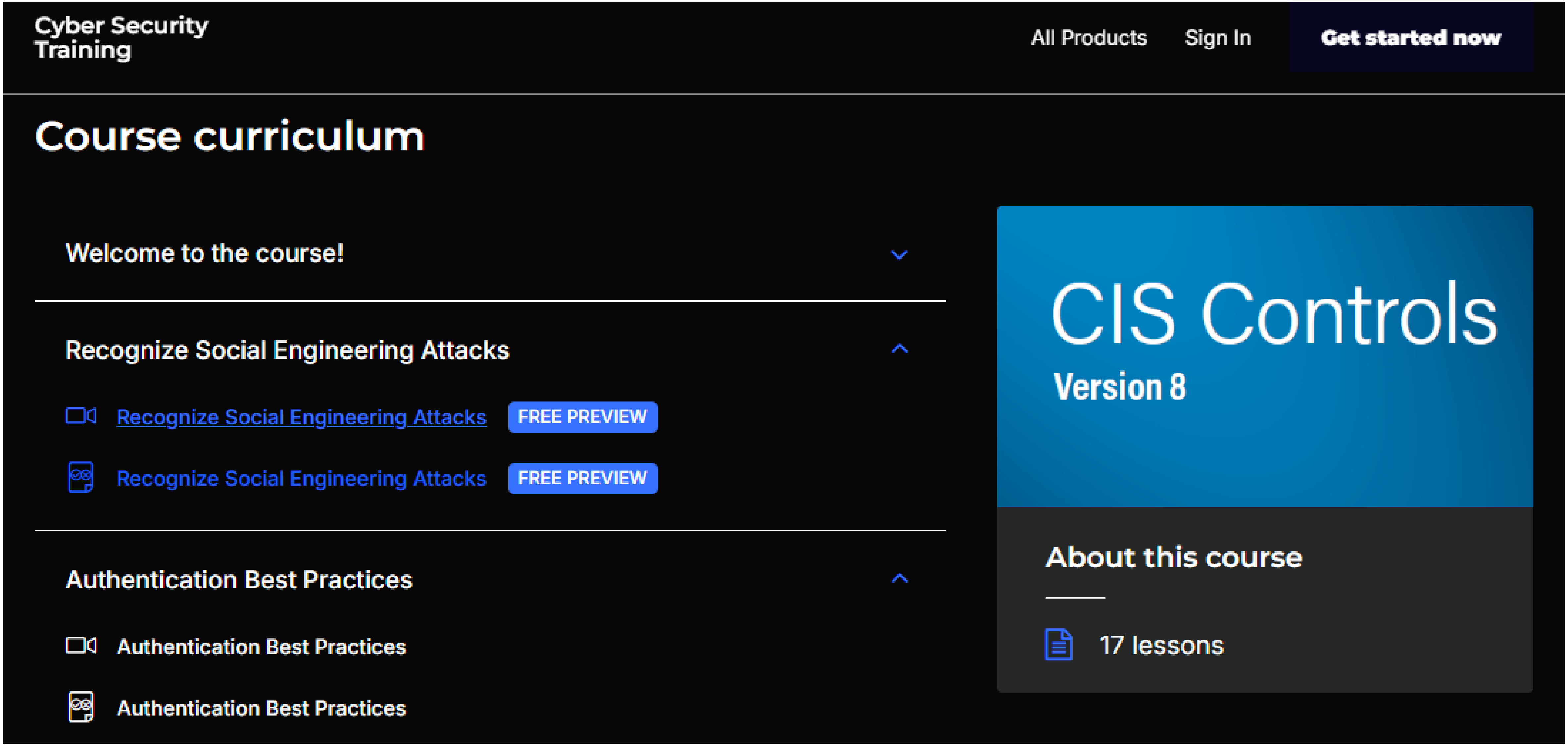
Recovery

Issue Final Incident Report

Phase 4 Post Incident Actions

Conduct Lessons Learned Session

Solution – Cyber Security Awareness Training (LMS)



Cyber Security Training

All Products Sign In **Get started now**

Course curriculum

Welcome to the course!

Recognize Social Engineering Attacks

- Recognize Social Engineering Attacks FREE PREVIEW
- Recognize Social Engineering Attacks FREE PREVIEW

Authentication Best Practices

- Authentication Best Practices
- Authentication Best Practices

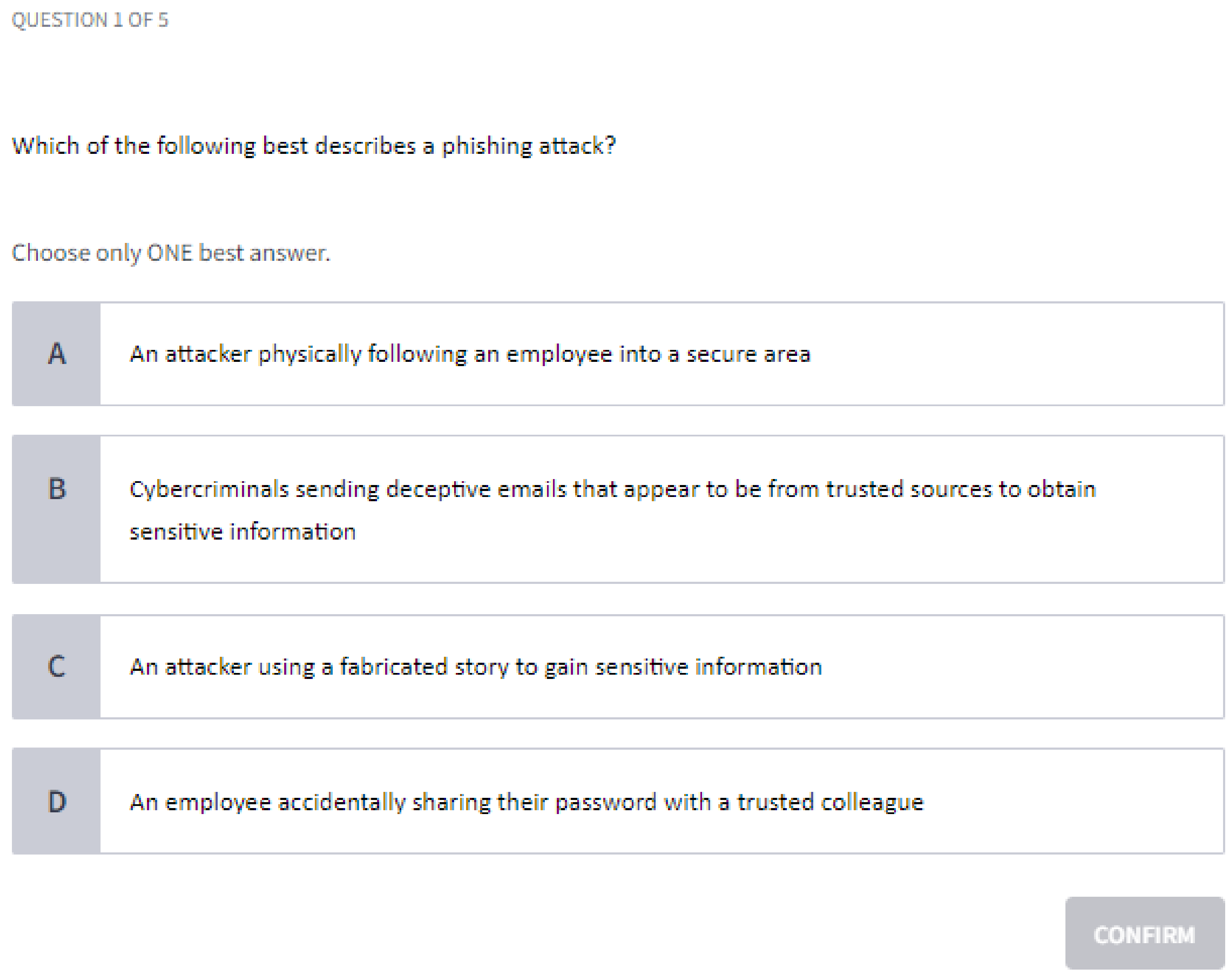
CIS Controls

Version 8

About this course

17 lessons

Solution – Cyber Security Awareness Training (LMS)



QUESTION 1 OF 5

Which of the following best describes a phishing attack?

Choose only ONE best answer.

A An attacker physically following an employee into a secure area

B Cybercriminals sending deceptive emails that appear to be from trusted sources to obtain sensitive information

C An attacker using a fabricated story to gain sensitive information

D An employee accidentally sharing their password with a trusted colleague

Thank you

Campbell McKenzie

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

incidentresponse.co.nz
whistleblowers.co.nz

Incident Response
FORENSIC & CYBER