



# The Cybersecurity Challenge: Defending Against Modern Threats

**Kiwi Advisor Network  
February 2025**

# Today's Presentation – in 60 Seconds

- Key technology risk issues
- Regulatory Landscape
- Cyber and incident response procedures
- Next steps and how we can help you



# 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

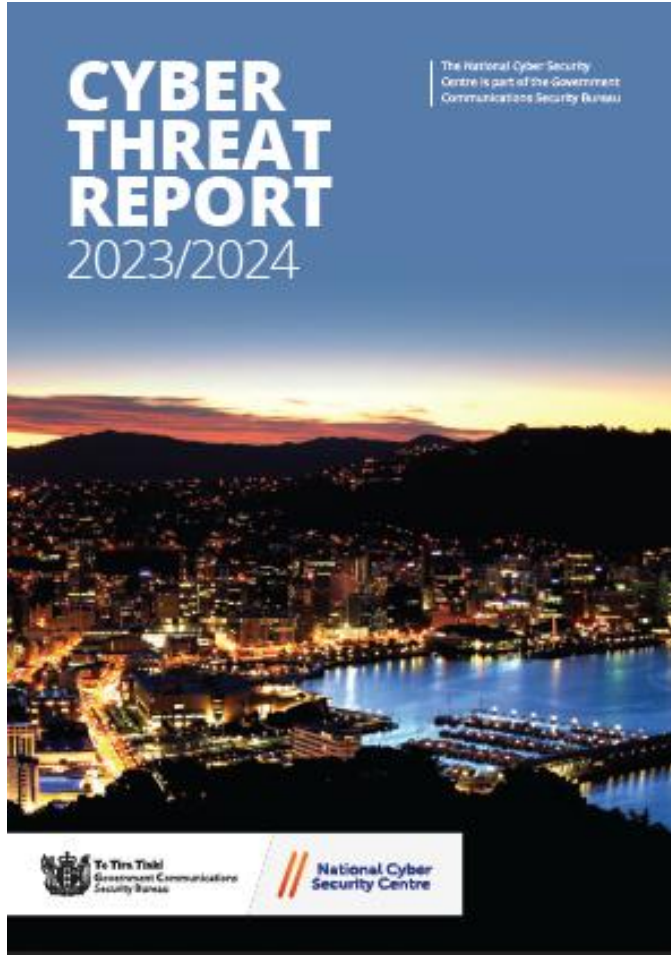
Data loss occurs due to natural events and accidents like fires and floods.



## 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

# Cyber Snapshot

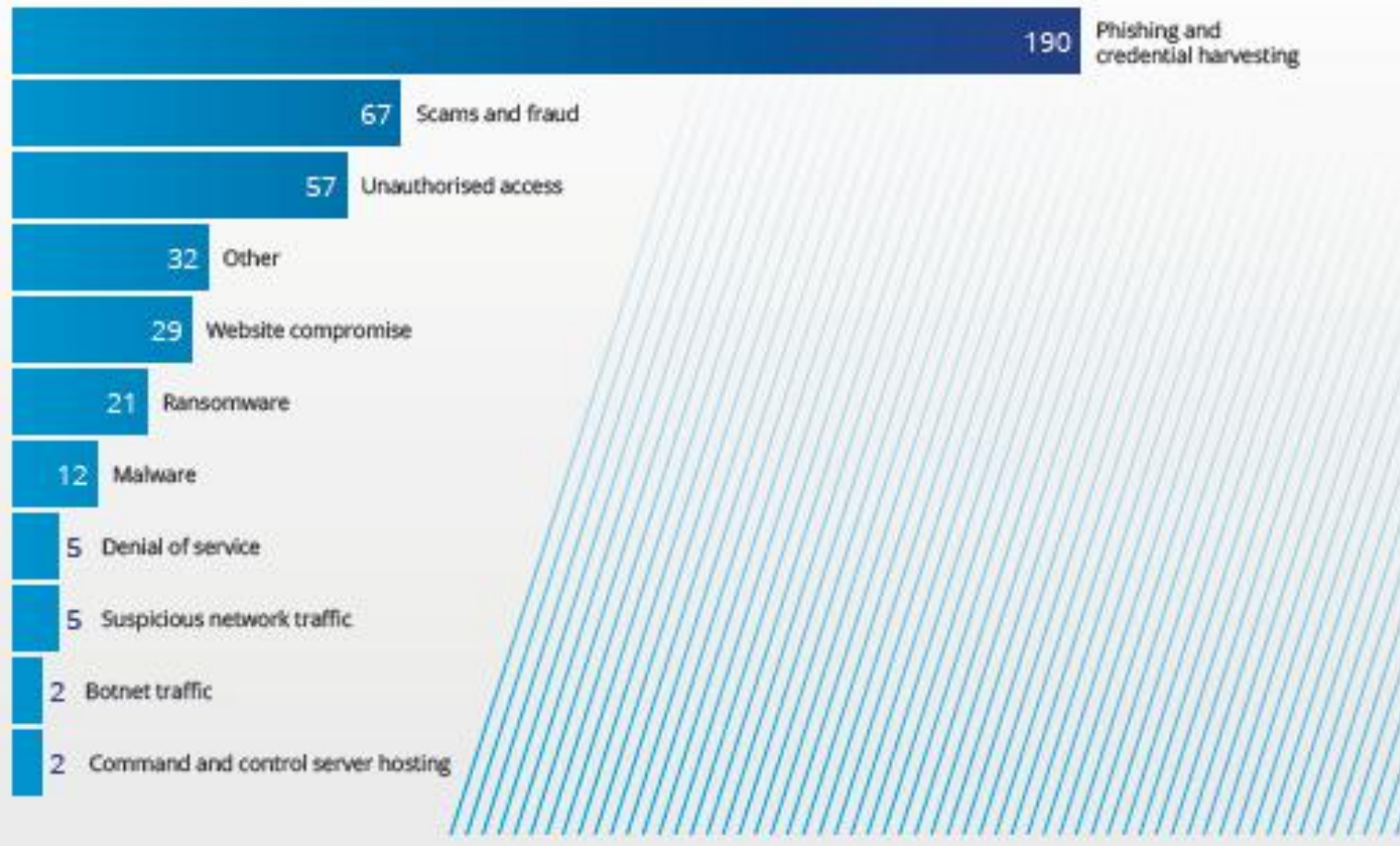


The NCSC in a typical month:

- 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.

# Cyber Snapshot

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



# CISA Risk and Vulnerability Assessment

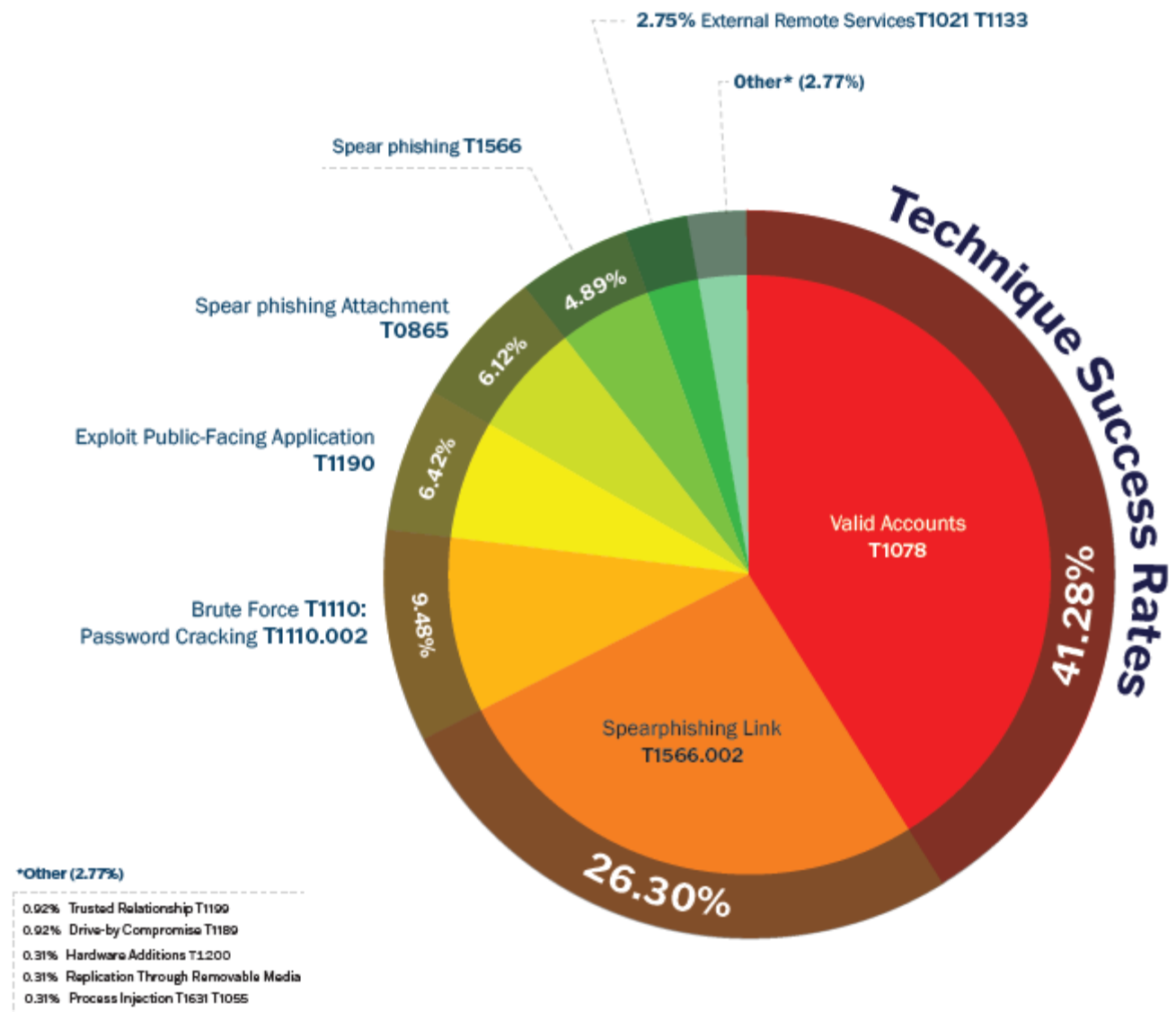
## FY23 RVA Results

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.

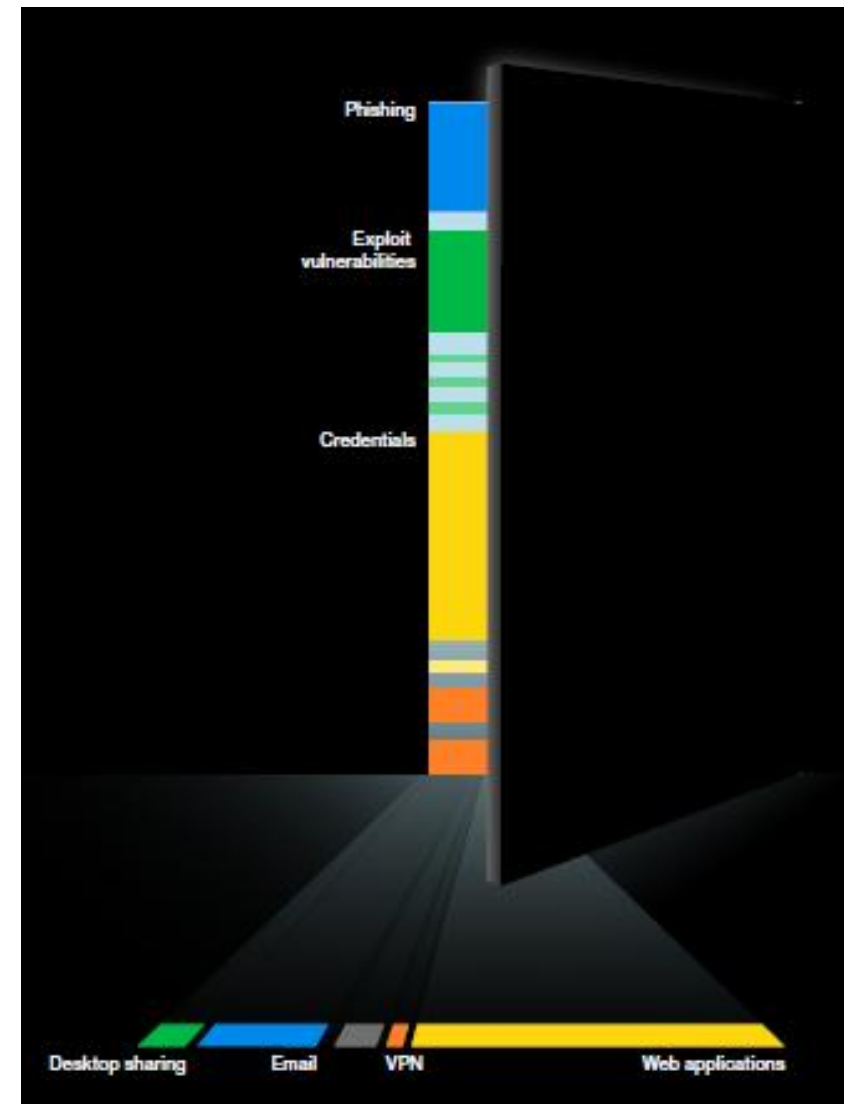
- Cracking password hashes (89% Administrator accounts)
- Default or stolen administrator accounts
- Former employee accounts that have not been removed
- Initial access brokers that sell exploits and valid credentials





# Verizon 2024 Data Breach Investigations Report

- 17<sup>th</sup> 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.

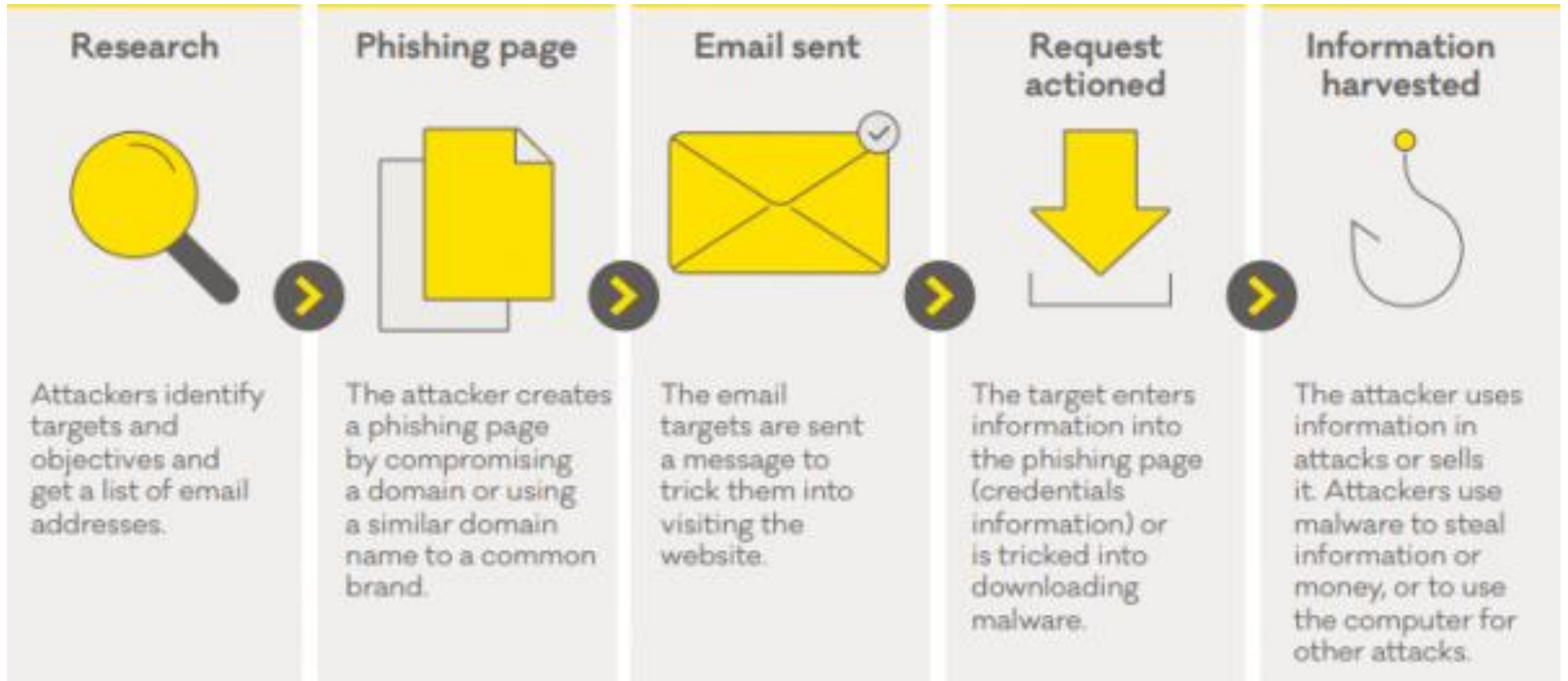


# What Verizon Found – Key Statistics

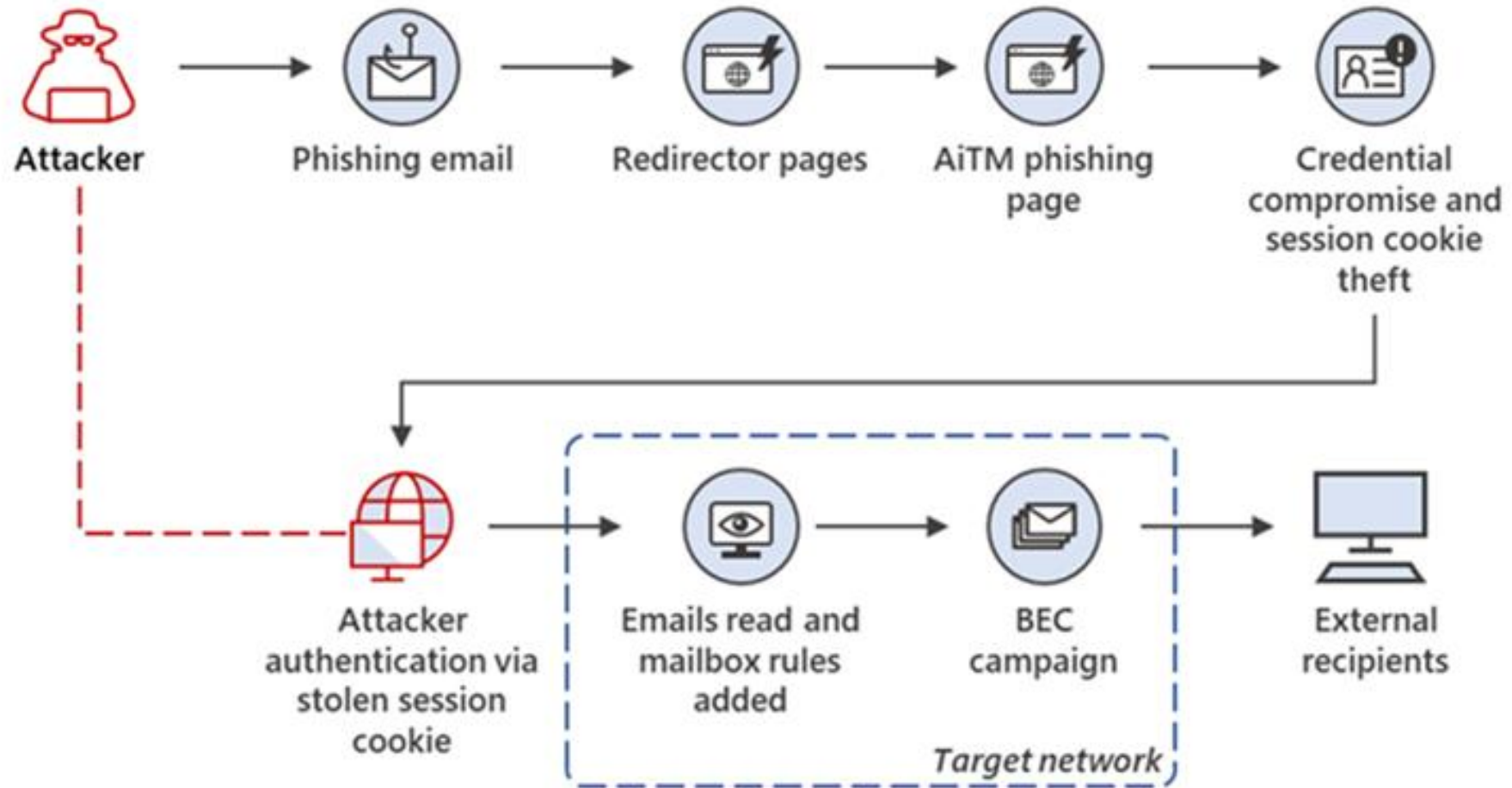
- **68%** of all breaches include the human element  
*Error, stolen credentials or Social Engineering (Privilege Misuse removed)*
- **40%** of all Social Engineering incidents used pretexting  
*Phishing and Pretexting via email make up 73% of social engineering attacks - targeting users with existing 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*



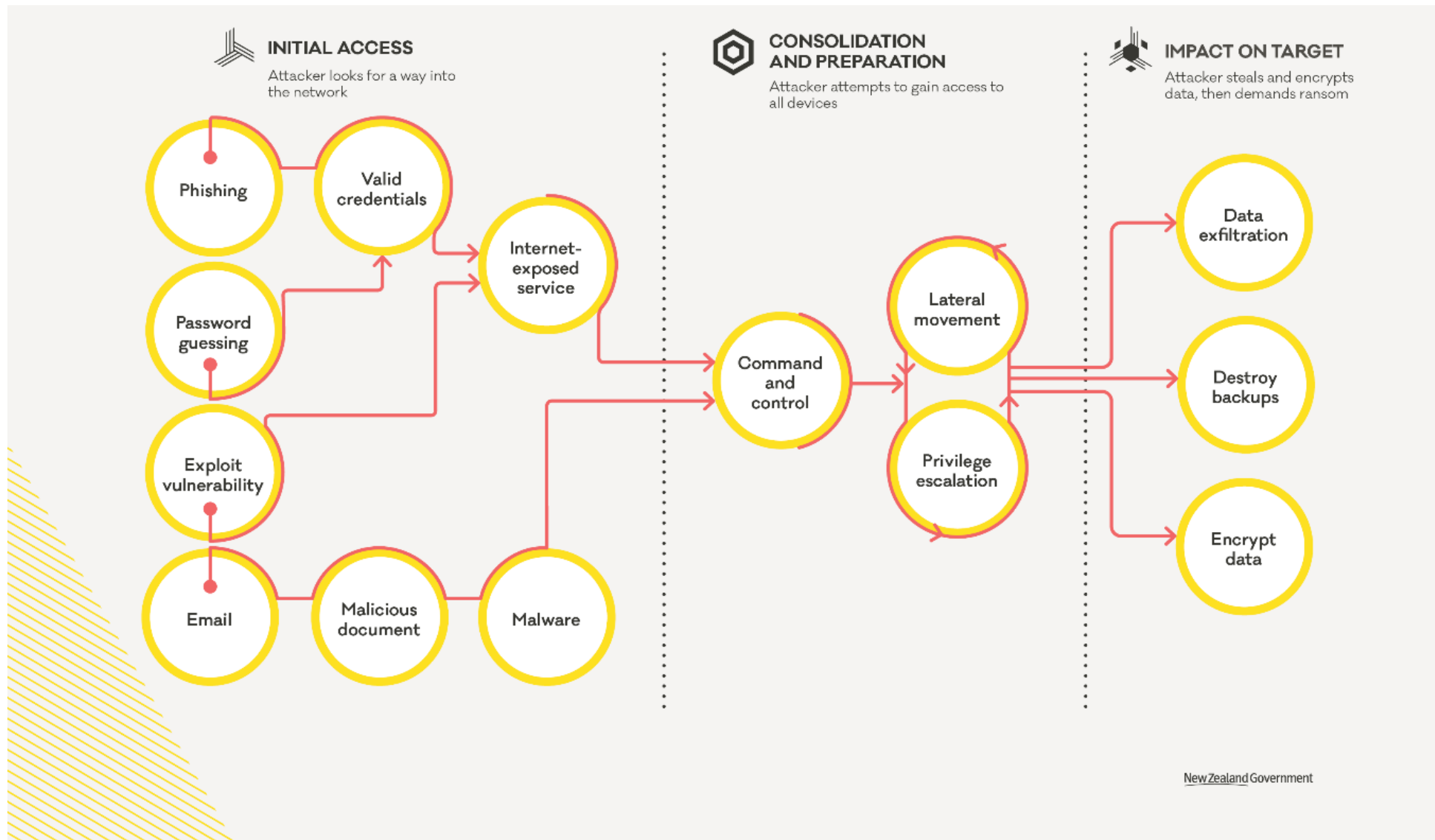
# Traditional Business Email Compromise – Pre MFA



# Evolving Business Email Compromise – Post MFA



# Lifecycle of a Ransomware Incident



# Current Ransomware Activity

Welcome to 🦖 RansomLook 🦖 !

February 18Th, 2025

Currently tracking **282** groups across **1483** relays & mirrors - **614** currently online

Got **513** DLS, **763** FS, **188** Chats and **19** Admin/Affiliates pages.

Currently tracking **117** forums & markets across **204** relays & mirrors - **111** currently online

Currently tracking **284** telegram channels.

There have been **35** posts within the last 24 hours

There have been **497** posts within the month of february

There have been **2112** posts within the last 90 days

There have been **1193** posts within the year of 2025

There have been **19600** posts since the dawn of ransomlook



# Cyber Governance – NZ v Australia

- *“We're seeing a trend overseas of new legislation being developed to address increasingly sophisticated and frequent cyber threats.”*
- *“It remains to be seen whether our Government will choose to increase investment in cyber security regulation, echoing the approaches of the UK and Australia.”*

<https://www.russellmcveagh.com/insights-news/digital-download-looking-to-2025-and-beyond-script-version/>



Cyber Security Act 2024

No. 98, 2024

An Act relating to cyber security for Australians, and for other purposes



# Cyber-resilience in FMA-regulated financial services guidance

- On 11 July 2019, the FMA released their report on their review of cyber-resilience in New Zealand financial services.
- “Cyber-risk encompasses all risk of loss, disruption, or damage to a firm caused by failure in its information technology systems – from both internal and external threats.”
- “All market participants should assess cyber-risk as part of their wider risk-assessment and management programme. We also strongly encourage all market participants to use a recognised cybersecurity framework to assist with planning, prioritising and managing their cyber-resilience.”

# The Code of Professional Conduct for Financial Advice Services

- On 7 May 2019, the Minister of Commerce and Consumer Affairs approved the Code of Professional Conduct for Financial Advice Services, which took effect on 15 March 2021.
- The Code requires Financial Advisers to protect client information, including:
  - Taking reasonable steps to prevent loss, unauthorised access, use, modification, or disclosure.
  - Ensuring client information includes all collected or held records, including work papers and financial advice.
  - Retaining information only as long as required, then returning or securely disposing of it.
  - Maintaining physical and electronic security to restrict access to authorised personnel.
  - Applying the standard consistently with Privacy Act obligations where personal information is involved.



# Developing cyber resilience for financial advice providers

- The new financial advice regime came into force on 15 March 2021.
- Entities and individuals granted a full Financial Advice Providers (FAP) licence under the Financial Markets Conduct Act 2013 (FMC Act) will be subject to the standard conditions for full FAP licences.
- Standard condition 5 sets out requirements around business continuity and technology systems, particularly for maintaining information security of technology systems which, if disrupted, would materially affect the financial advice service.

# FMA - Regulatory Impact Statement:





















- 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.

# Cyber Governance and Risk Management - Controls







# Incident Response – Insurance Panel Provider

## 17 Incident Response Management

17.1	Designate Personnel to Manage Incident Handling			
17.2	Establish and Maintain Contact Information for Reporting Security Incidents			
17.3	Establish and Maintain an Enterprise Process for Reporting Incidents			
17.4	Establish and Maintain an Incident Response Process			
17.5	Assign Key Roles and Responsibilities			
17.6	Define Mechanisms for Communicating During Incident Response			
17.7	Conduct Routine Incident Response Exercises			
17.8	Conduct Post-Incident Reviews			
17.9	Establish and Maintain Security Incident Thresholds			

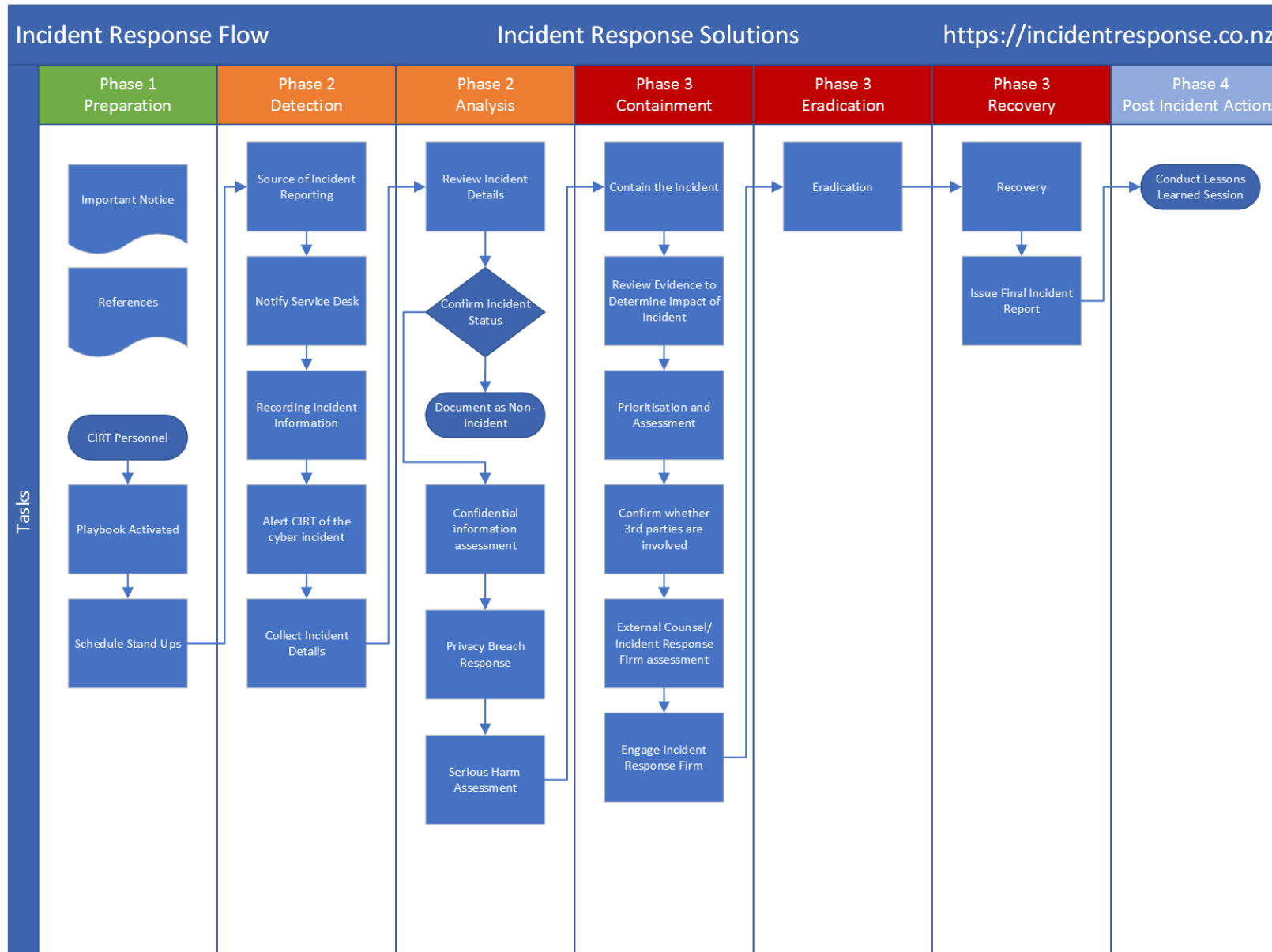
# Security Awareness and Skills Training

## 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			



# IR, DR, BCP Plans and Simulations





# 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*

