

# Forensic technology considerations when responding to cyber matters

NZISF – March 2022



**Incident  
Response**

FORENSIC & CYBER

# Expert Witness

High Court Rules 2016 - Schedule 4  
Code of conduct for expert witnesses

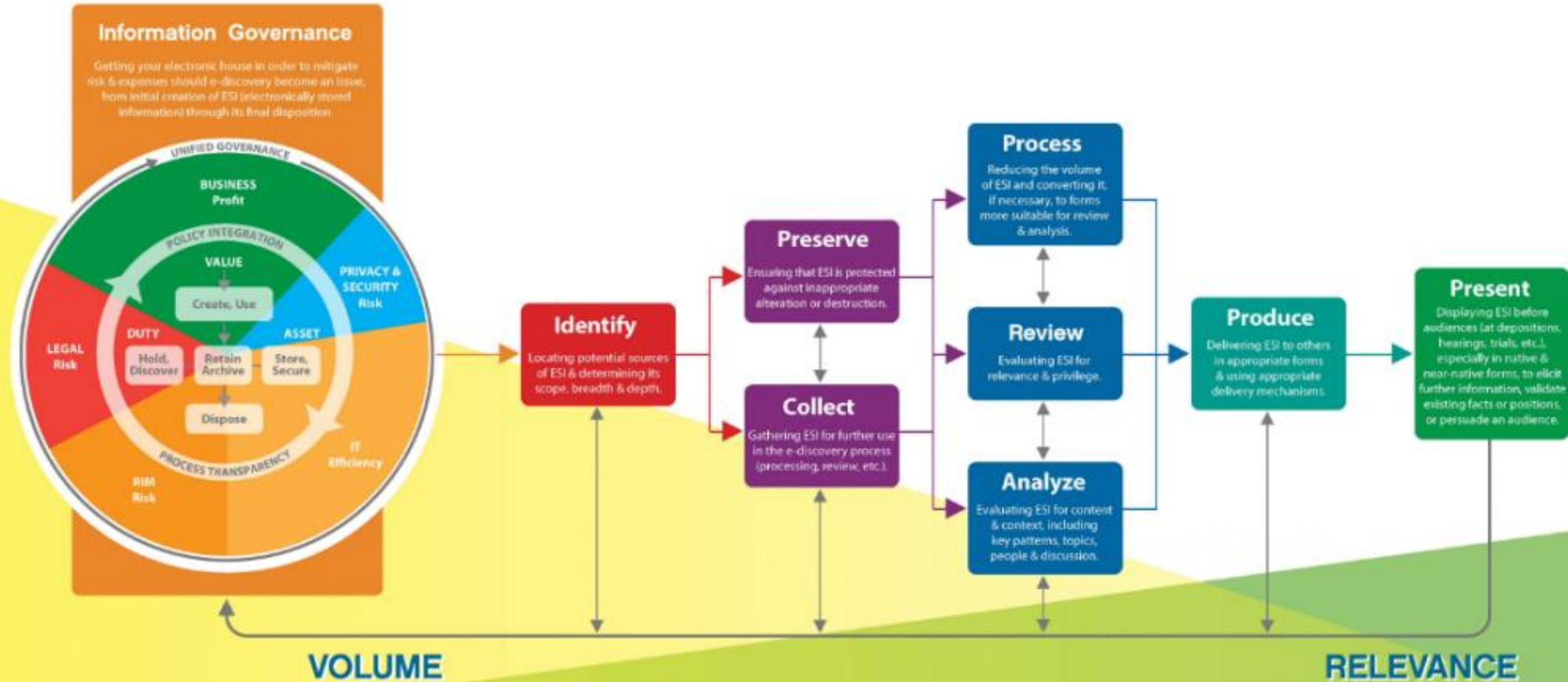
ANZFSS Code of Professional Practice

IACIS Code of Ethics and Professional Conduct

Private Security Personnel and Private Investigators Act 2010

# Electronic Discovery Reference Model

Standards, Guidelines, and Practical Resources for Legal Professionals and E-Discovery Practitioners



**So what's  
changed?**

**The Forensic Examiner is now an Incident Responder**



# Lockheed Martin - The Cyber Kill Chain®





# #1 RECONNAISSANCE



WEAPONS  
DIRECTOR 2

W 40

791

BOUNDARIES  
ANDORS # ADIZ

COORDINATES  
RADAR SITES

POWER SUP

RAD FIXES

EX DATA

ACCT F-105



#2 WEAPONISATION



# #3 DELIVERY

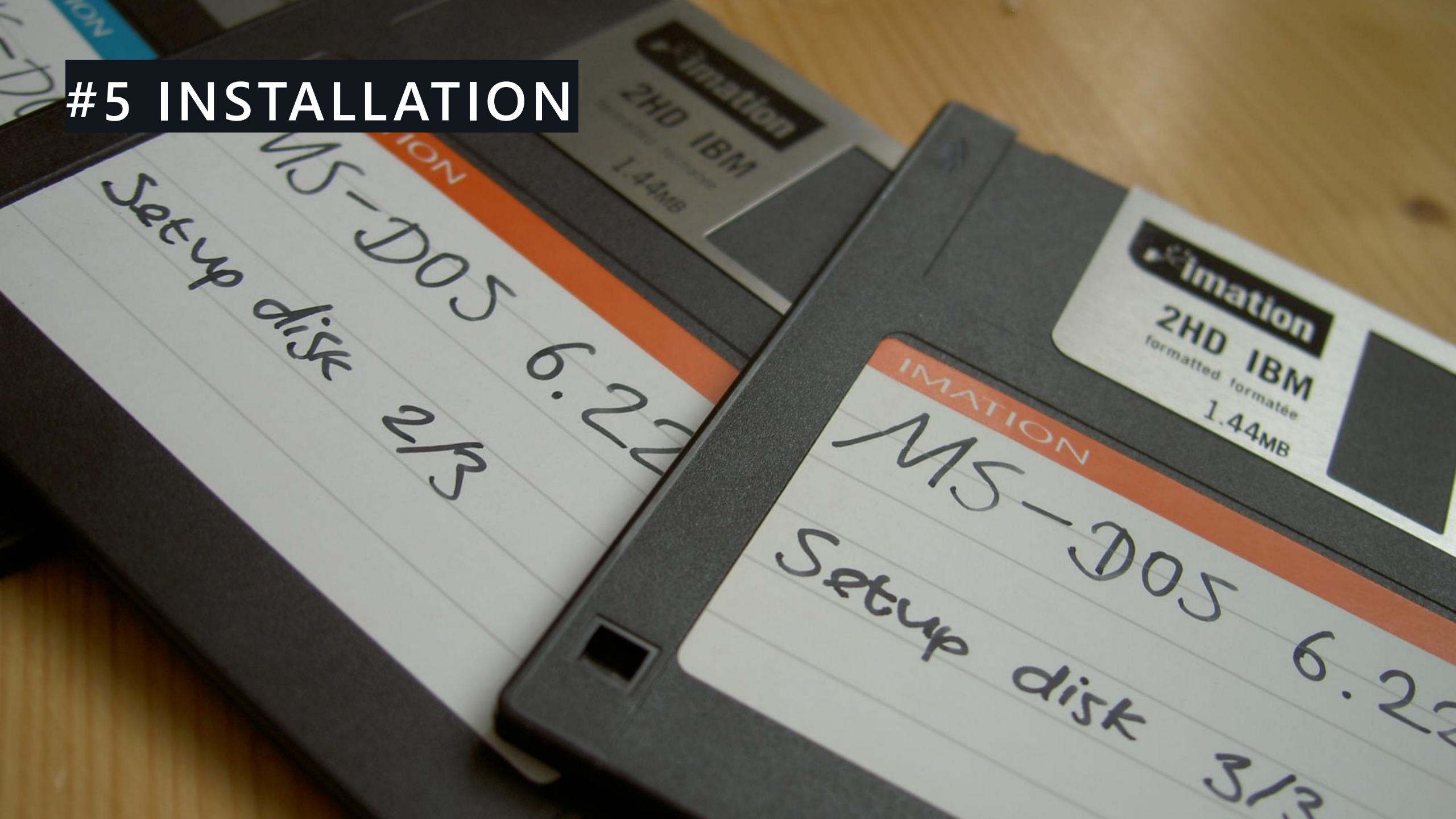
Email





**#4 EXPLOIT**

## #5 INSTALLATION







#6 C2C

# #7 ACTIONS ON OBJECTIVES



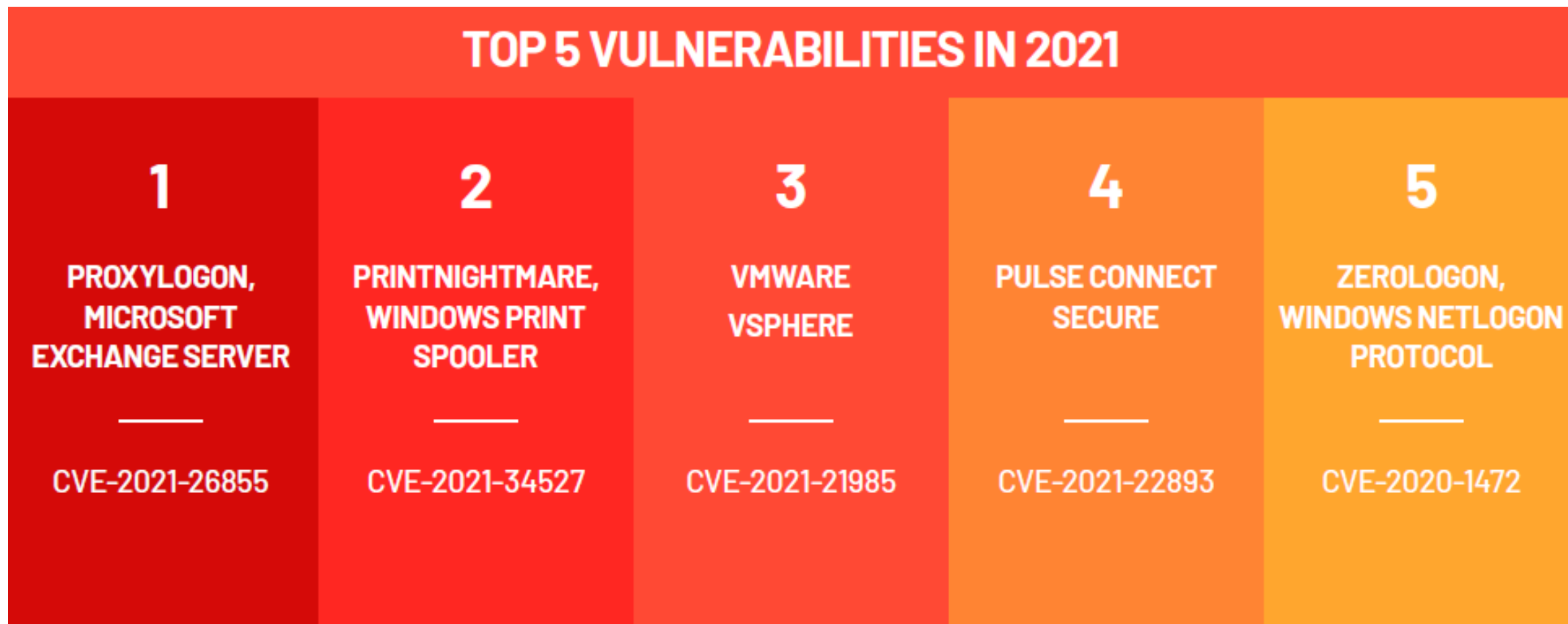




# From the field...

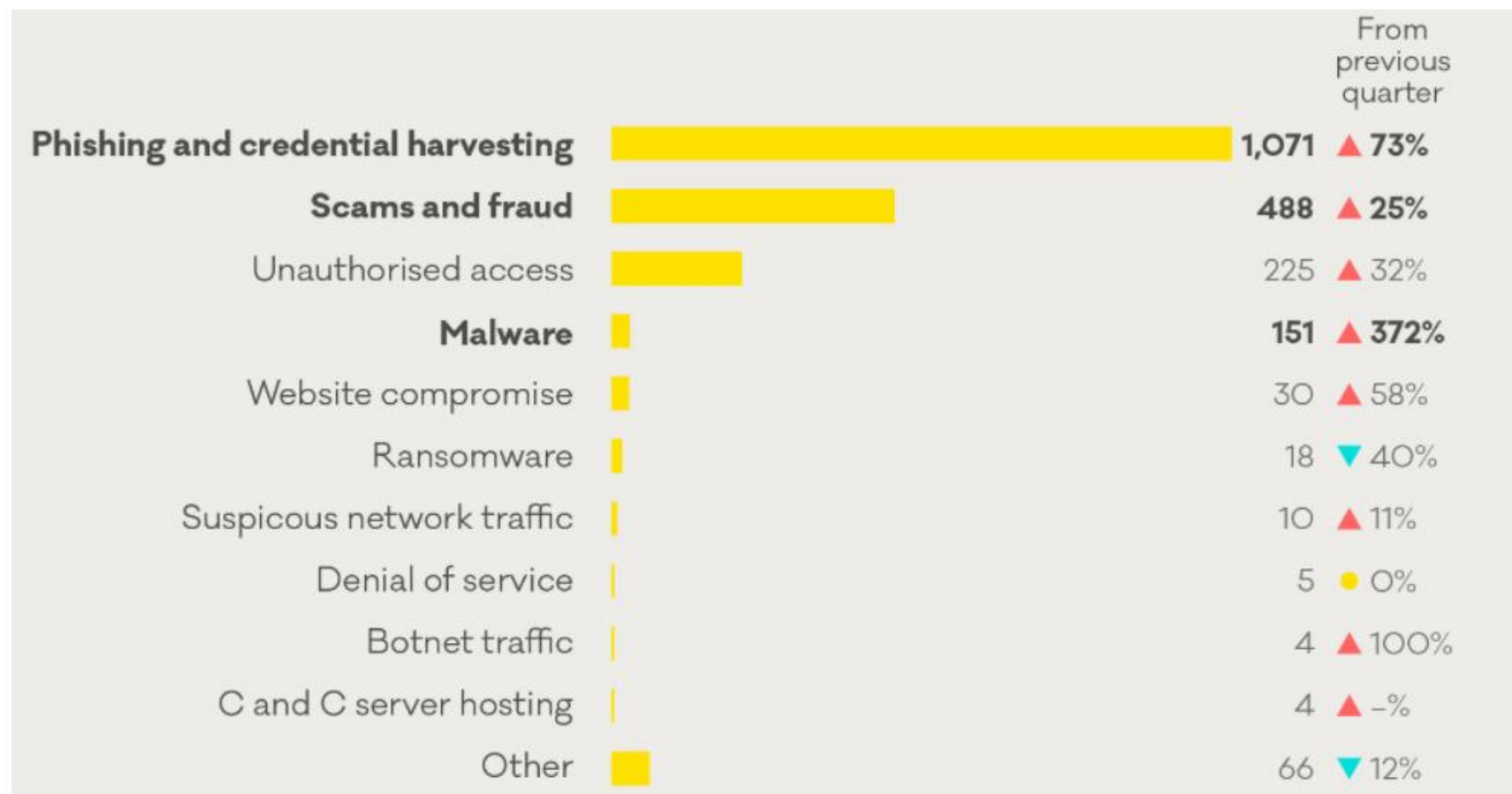


# Landscape - Vulnerabilities

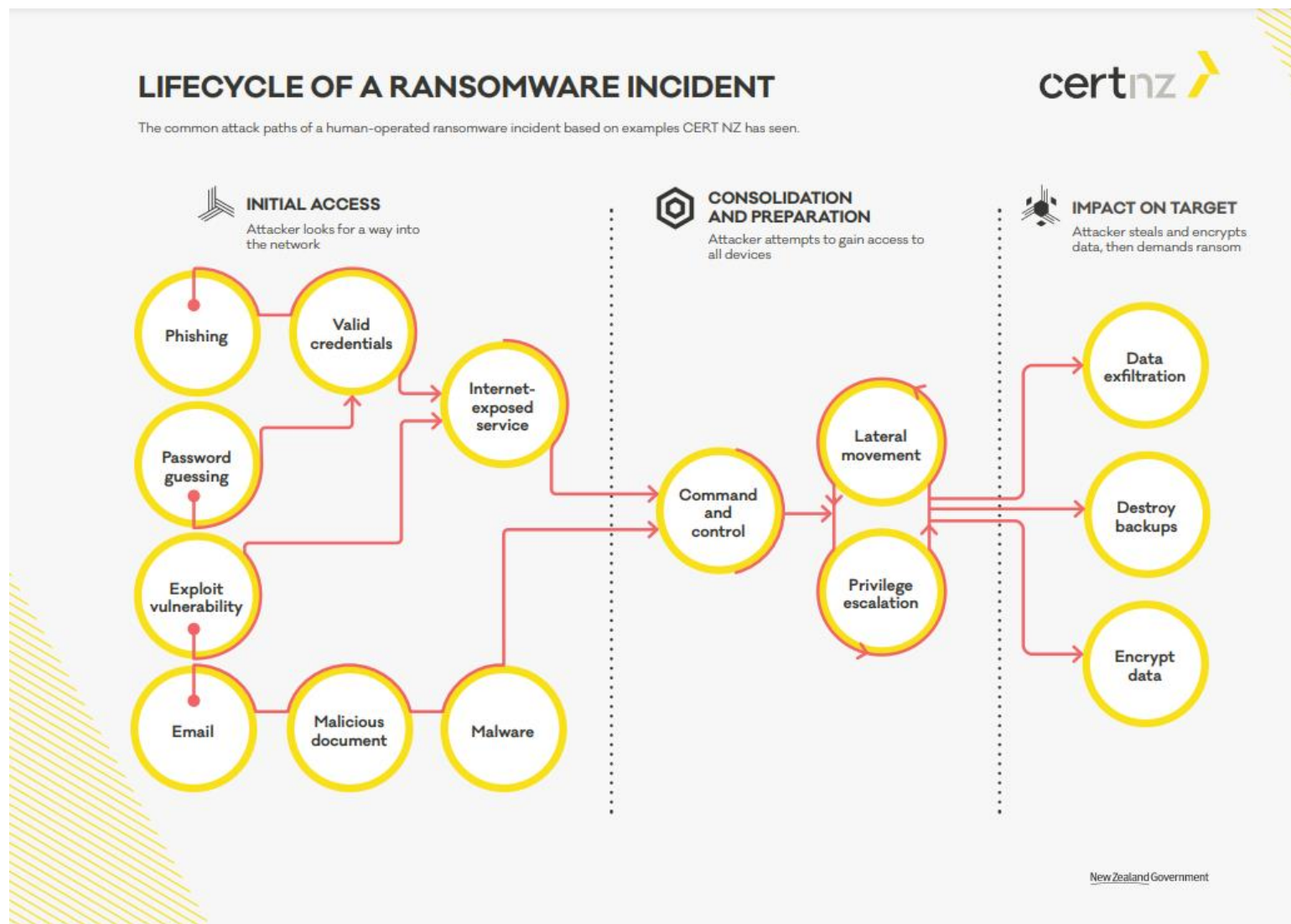




# Landscape – Types of Attacks in NZ

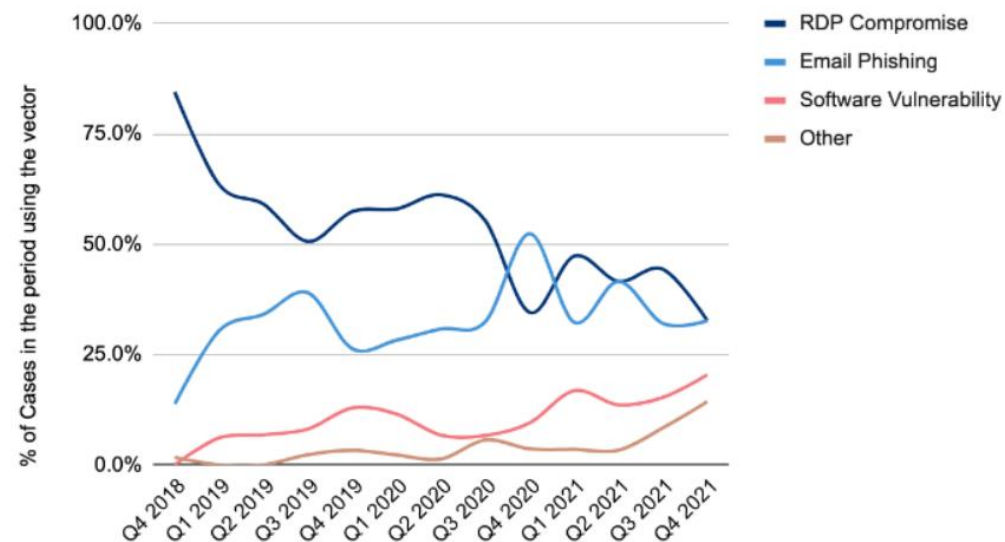


# CERT NZ - Ransomware

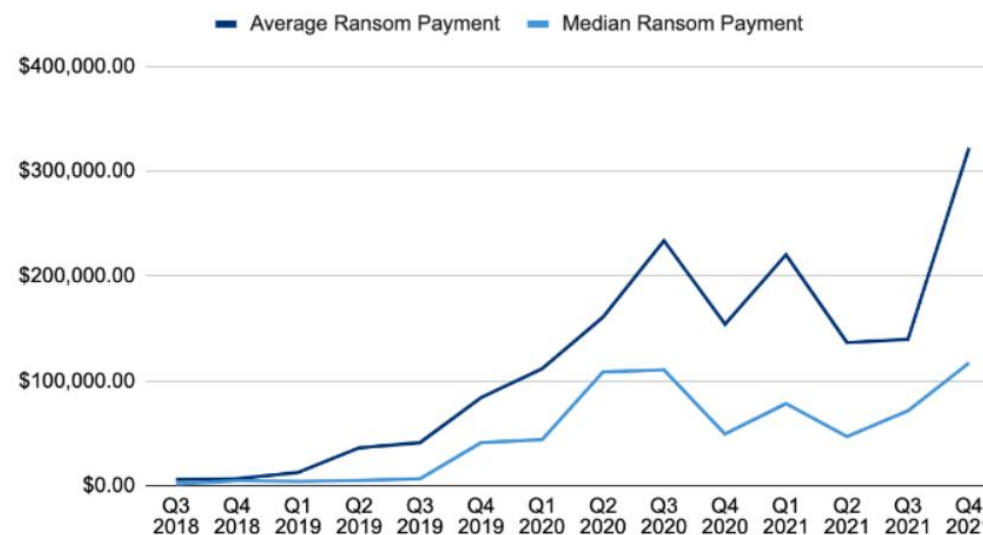


# Landscape - Ransomware

## Ransomware Attack Vectors



## Ransom Payments By Quarter







# Impact of the Privacy Act Reform



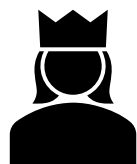
# Privacy Act 2020

- The Privacy Act replaces 27 year old legislation and implements a number of the changes adopted in comparable jurisdictions, such as the EU, Australia, and various US states.
- These significant reforms will change the way organisations in New Zealand manage privacy issues and data security.

• ***Mandatory notifications for privacy breaches***



***Increased powers for the Privacy Commissioner***



• ***Controls on disclosure of information overseas***



• ***Criminal offences***



• ***Extra-territorial scope***



# Serious Harm

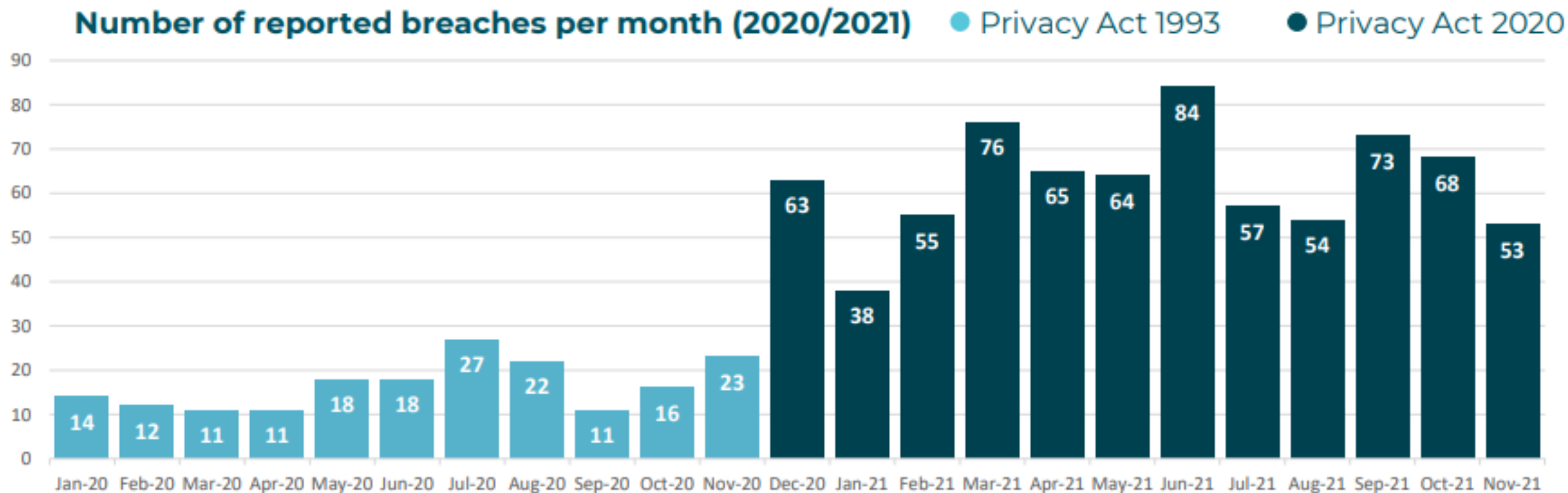
## **113 Assessment of likelihood of serious harm being caused by privacy breach**

When an agency is assessing whether a privacy breach is likely to cause serious harm in order to decide whether the breach is a notifiable privacy breach, the agency must consider the following:

- (a) any action taken by the agency to reduce the risk of harm following the breach:
- (b) whether the personal information is sensitive in nature:
- (c) the nature of the harm that may be caused to affected individuals:
- (d) the person or body that has obtained or may obtain personal information as a result of the breach (if known):
- (e) whether the personal information is protected by a security measure:
- (f) any other relevant matters.



# OPC - Mandatory privacy breach reporting



# OPC - Mandatory privacy breach reporting



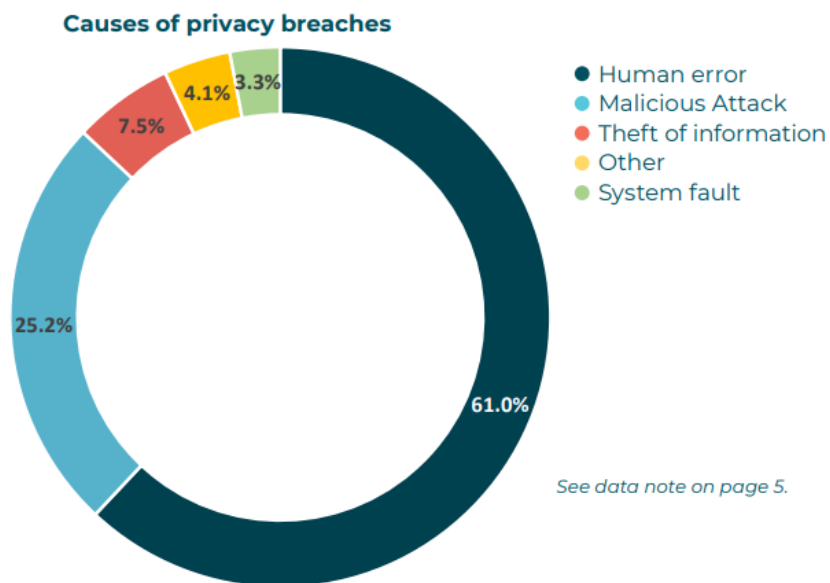
**33%** of all reported breaches met the serious harm threshold.

- Serious
- Not serious



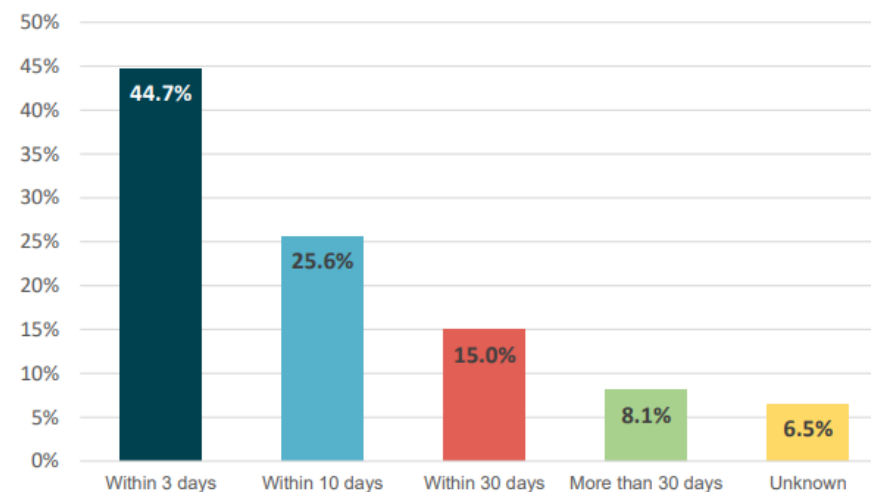
**61%** of affected individuals had been notified by the time the Office was informed of the privacy breach

- Had been notified
- Had not been notified



See data note on page 5.

Timeliness of breach reporting to OPC







Thank you

**Campbell McKenzie**

0800 WITNESS

021 779 310

[campbell@incidentresponse.co.nz](mailto:campbell@incidentresponse.co.nz)

[incidentresponse.co.nz](http://incidentresponse.co.nz)

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