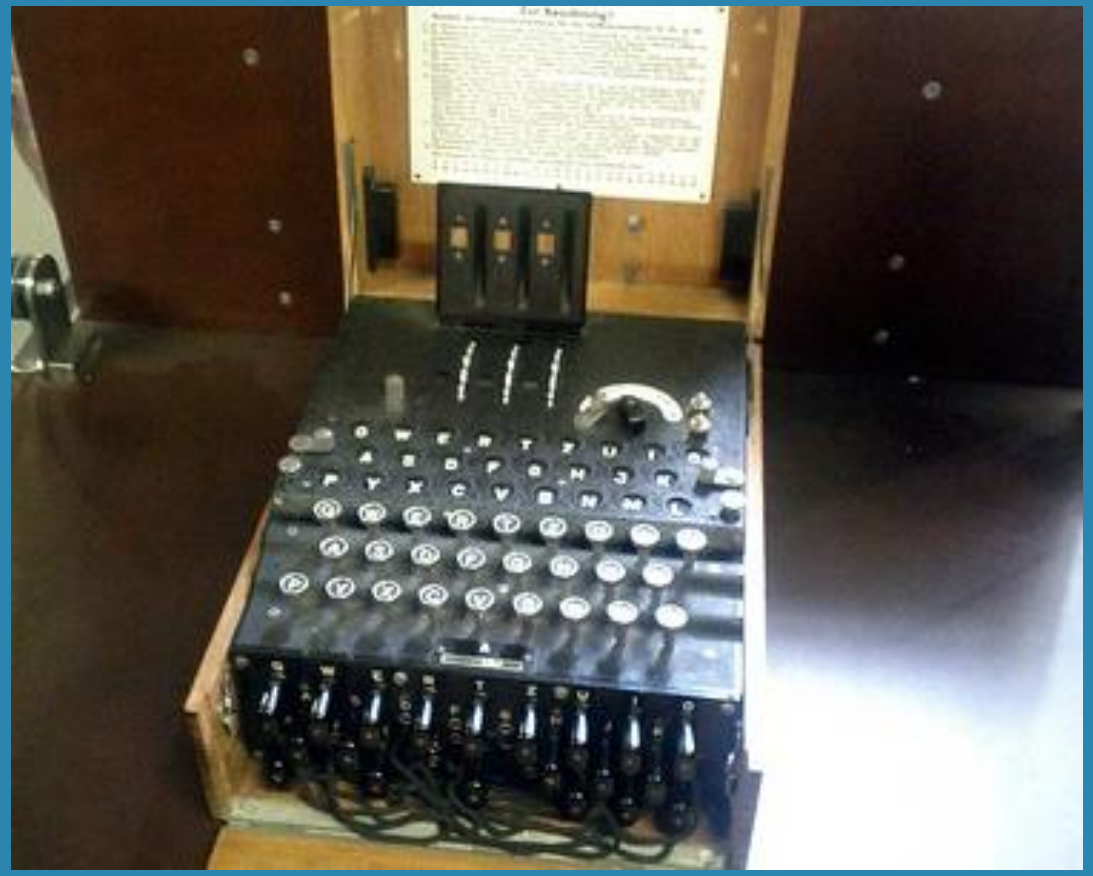


Cyber Update 2021

CAANZ

Focus on Management

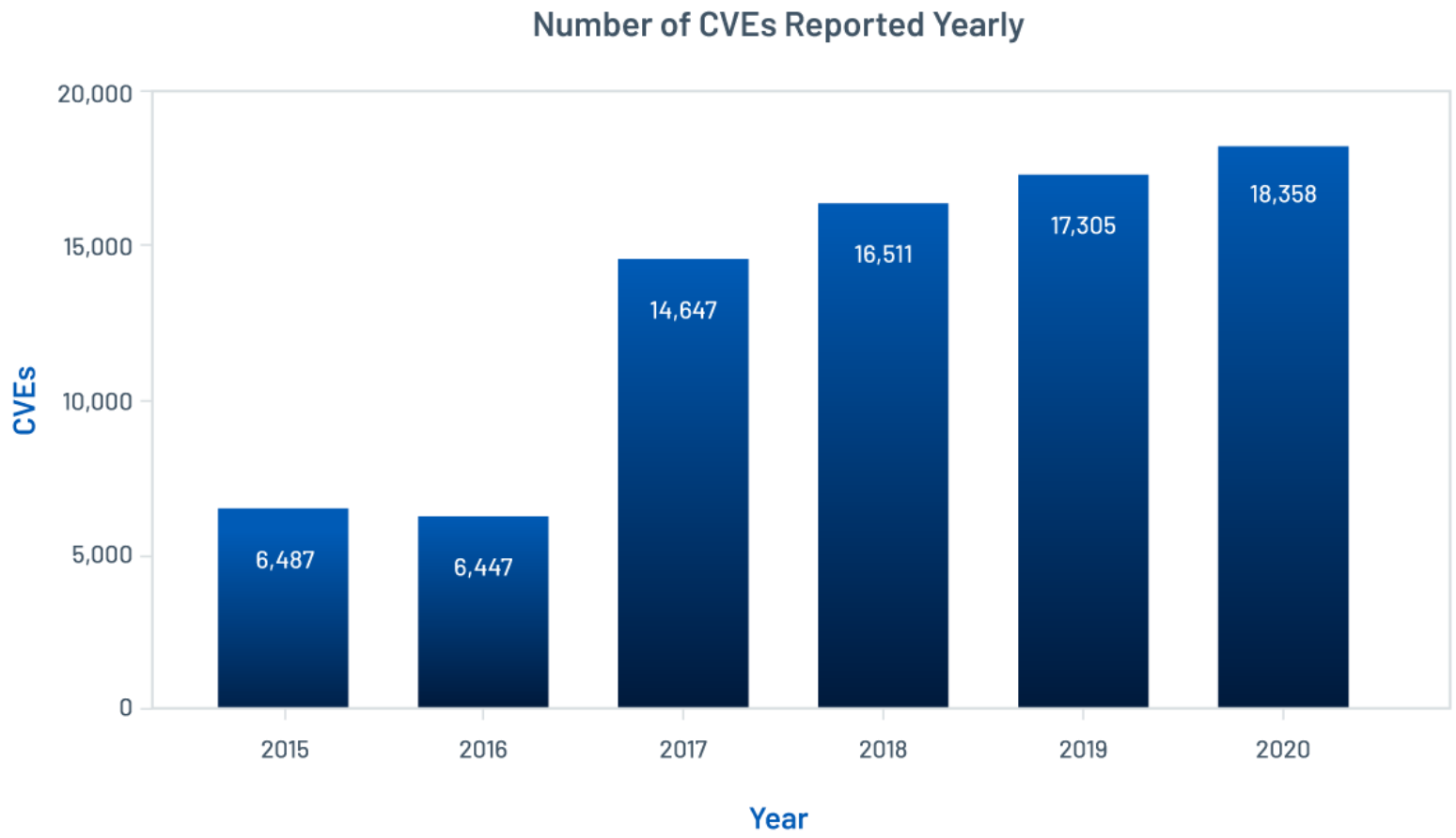
July 2021

Incident Response
FORENSIC & CYBER

Agenda

1. Cyber Incident Response - A brief overview
2. Recent case studies
3. Incident prevention and Response
4. Open forum

Landscape - Vulnerabilities



Source - https://www.tenable.com/blog/tldr-the-tenable-research-2020-threat-landscape-retrospective

Landscape - CERT NZ

Table 2: Types of loss

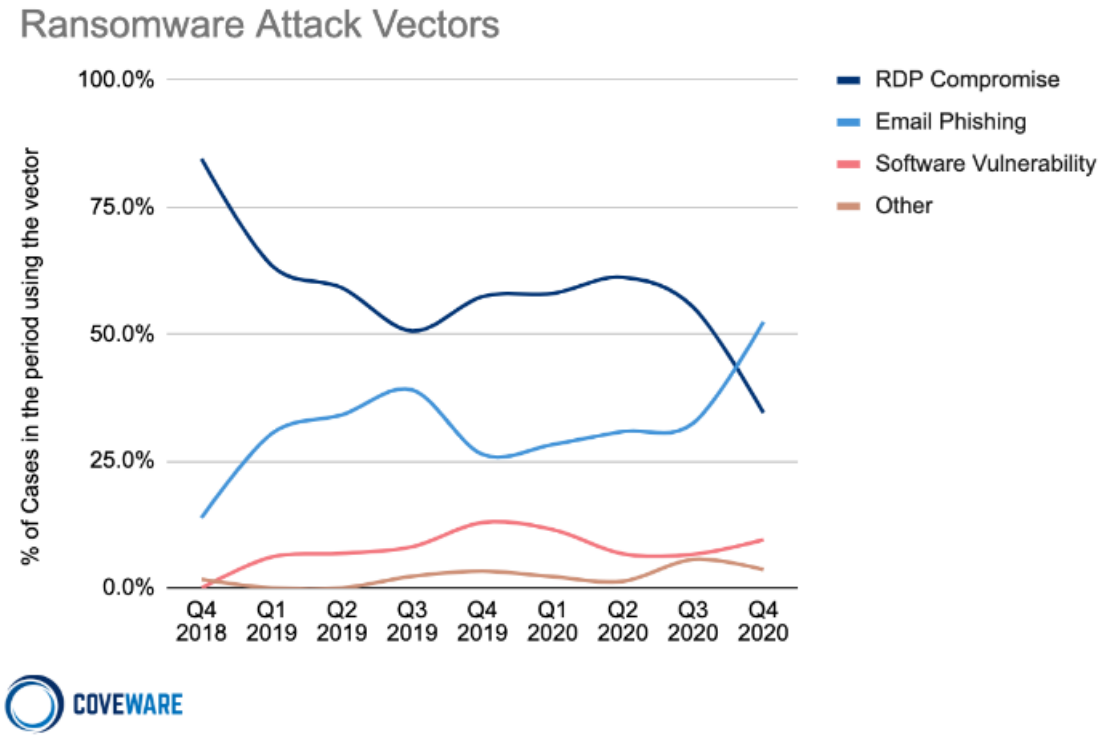
11%	**Financial loss** This not only includes money lost as a direct result of the incident, but also includes the cost of recovery, like the cost of contracting IT security services or investing in new security systems following an incident (Q1 and Q2 2020: 16%).	**0%**	**Reputational loss** Damage to the reputation of an individual or organisation as a result of the incident (Q1 and Q2 2020: 1%).
2%	**Data loss** Loss or unauthorised copying of data, business records, personal records and intellectual property (Q1 and Q2 2020: 3%).	**0%**	**Technical damage** Impacts on services like email, phone systems or websites, resulting in disruption to a business or organisation (Q1 and Q2 2020: 0%).
1%	**Operational impacts** The time, staff and resources spent on recovering from an incident, taking people away from normal business operations (Q1 and Q2 2020: 1%).	**1%**	**Other** Includes types of loss not covered in the other categories (Q1 and Q2 2020:: 1%).

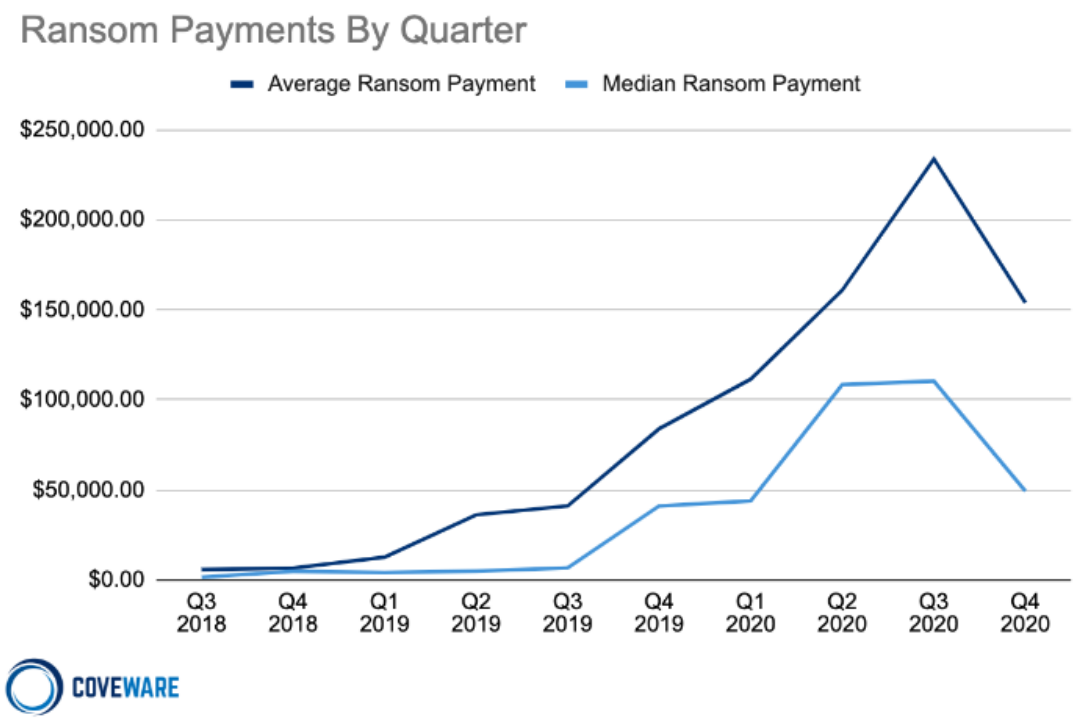
Source - https://www.cert.govt.nz/assets/Uploads/Quarterly-report/2020-q3/cert-nz-q3-2020-data-landscape.pdf

Landscape - Data Breach

Source - https://www.ibm.com/security/digital-assets/cost-data-breach-report

Landscape - Ransomware





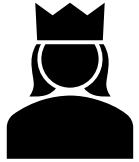
Source - https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020

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:

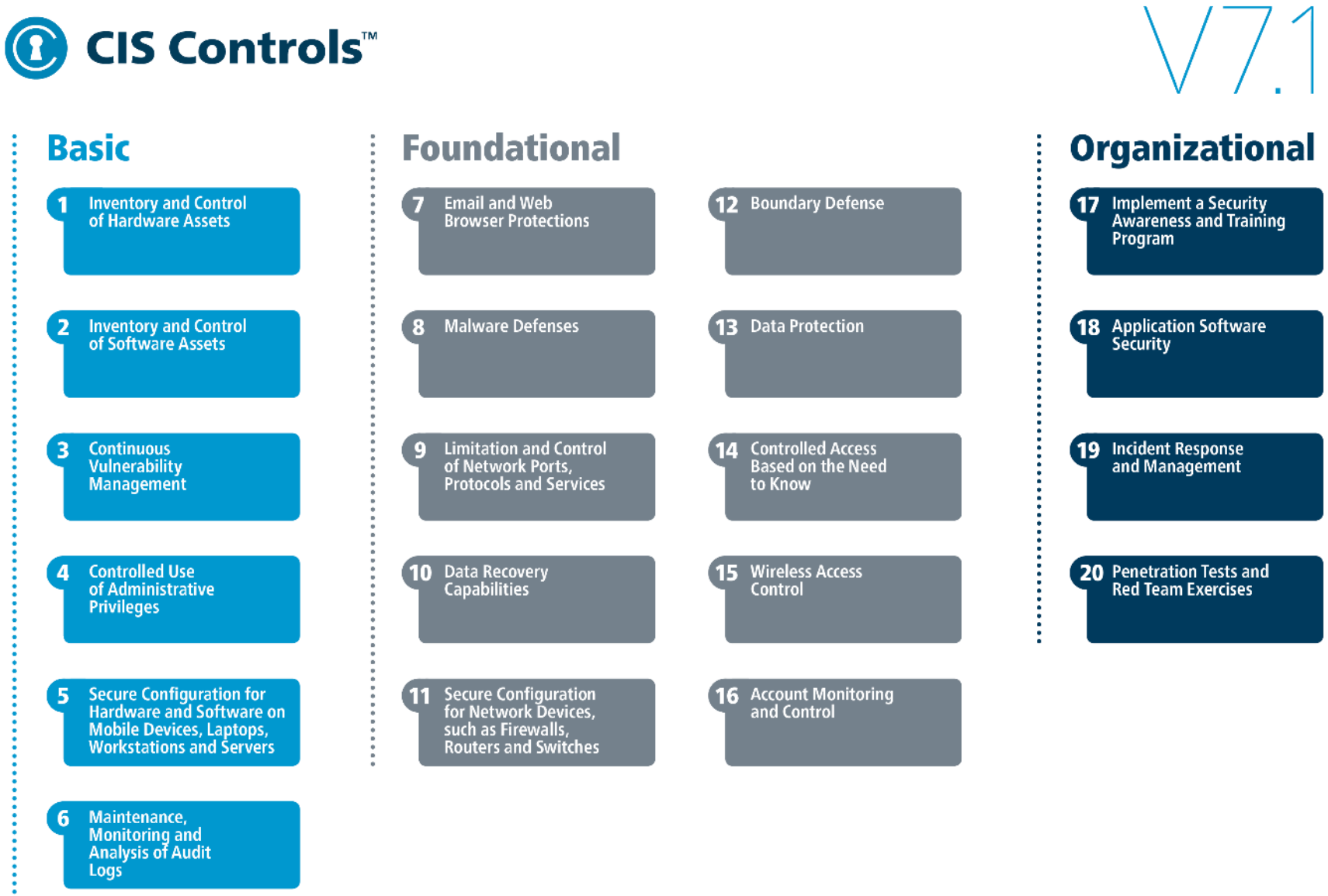
(f) any other relevant matters.

Case Studies

Incident prevention and Response

NIST CSF Framework

CIS Controls



Training

Open Forum

Thank you

Campbell McKenzie

0800 WITNESS or 021 779 310

campbell@incidentresponse.co.nz

incidentresponse.co.nz

whistleblowers.co.nz

Incident Response
FORENSIC & CYBER