Cyber Resilience: Accepting That It’s 'When' Not 'If'

Legalwise

February 2021

Incident Response

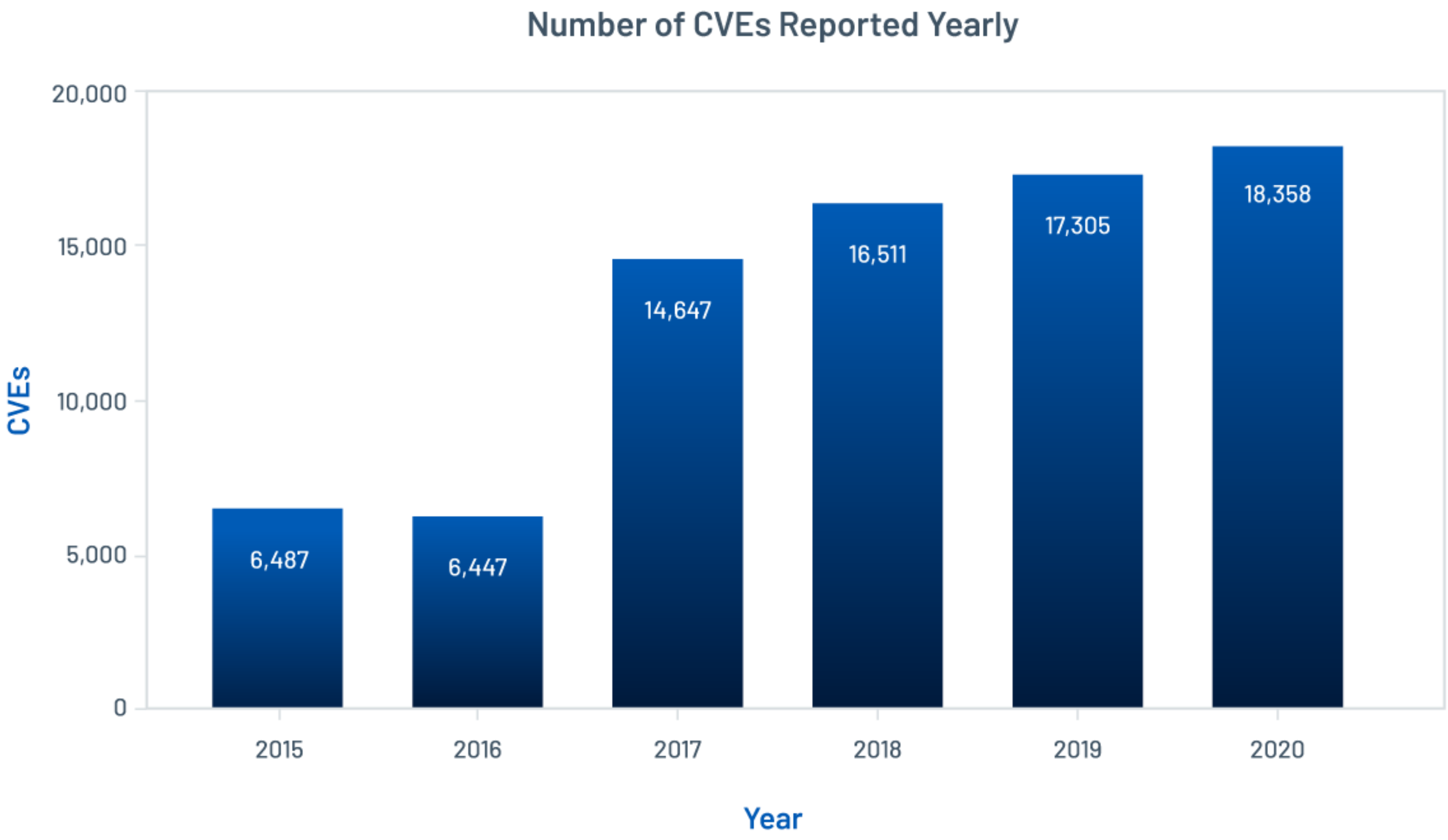
FORENSIC & CYBER

Agenda

1. Cyber Landscape
2. Framework
3. Controls
4. Training

Cyber Landscape

Landscape - Vulnerabilities



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

Landscape - CERT NZ

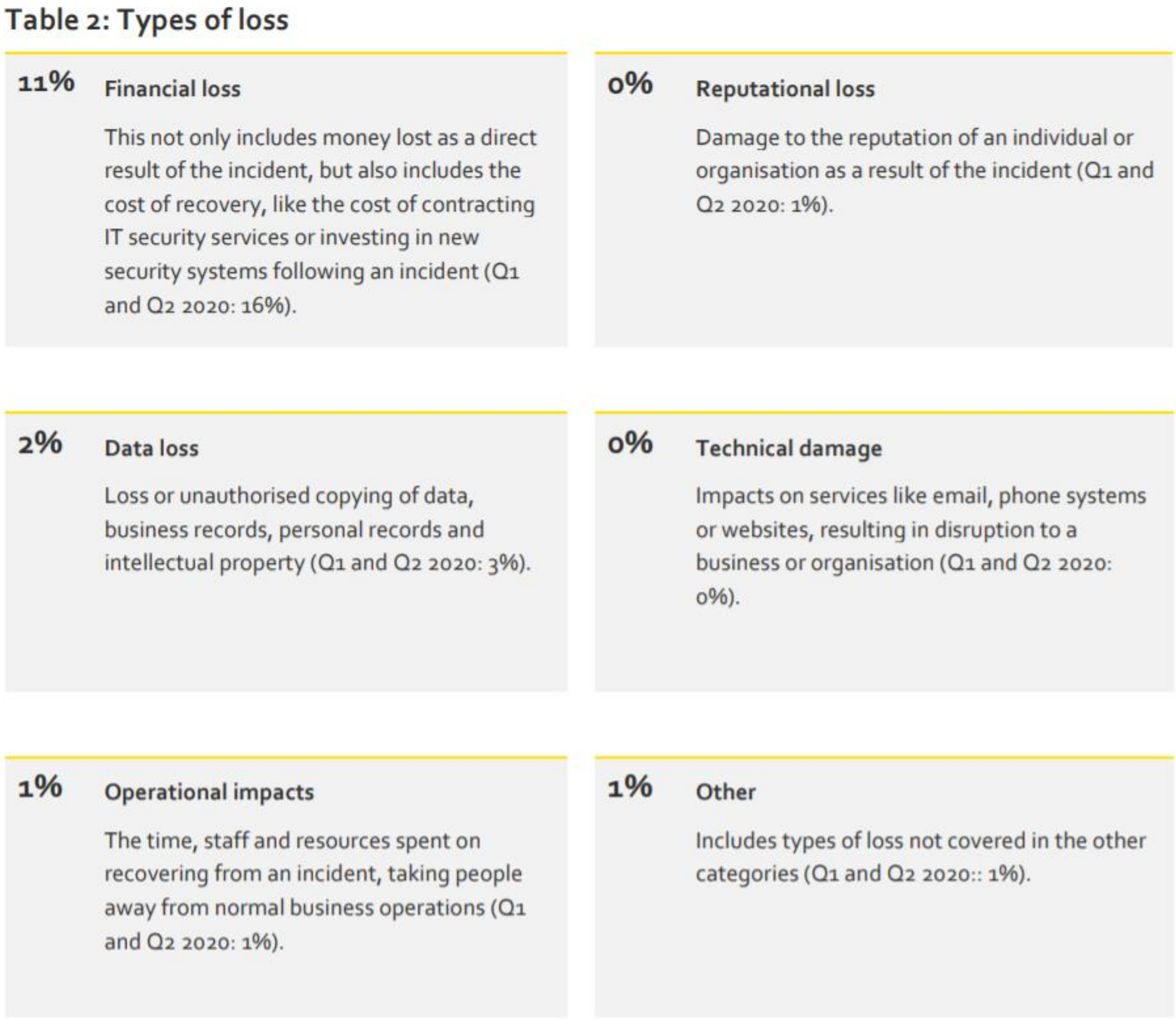
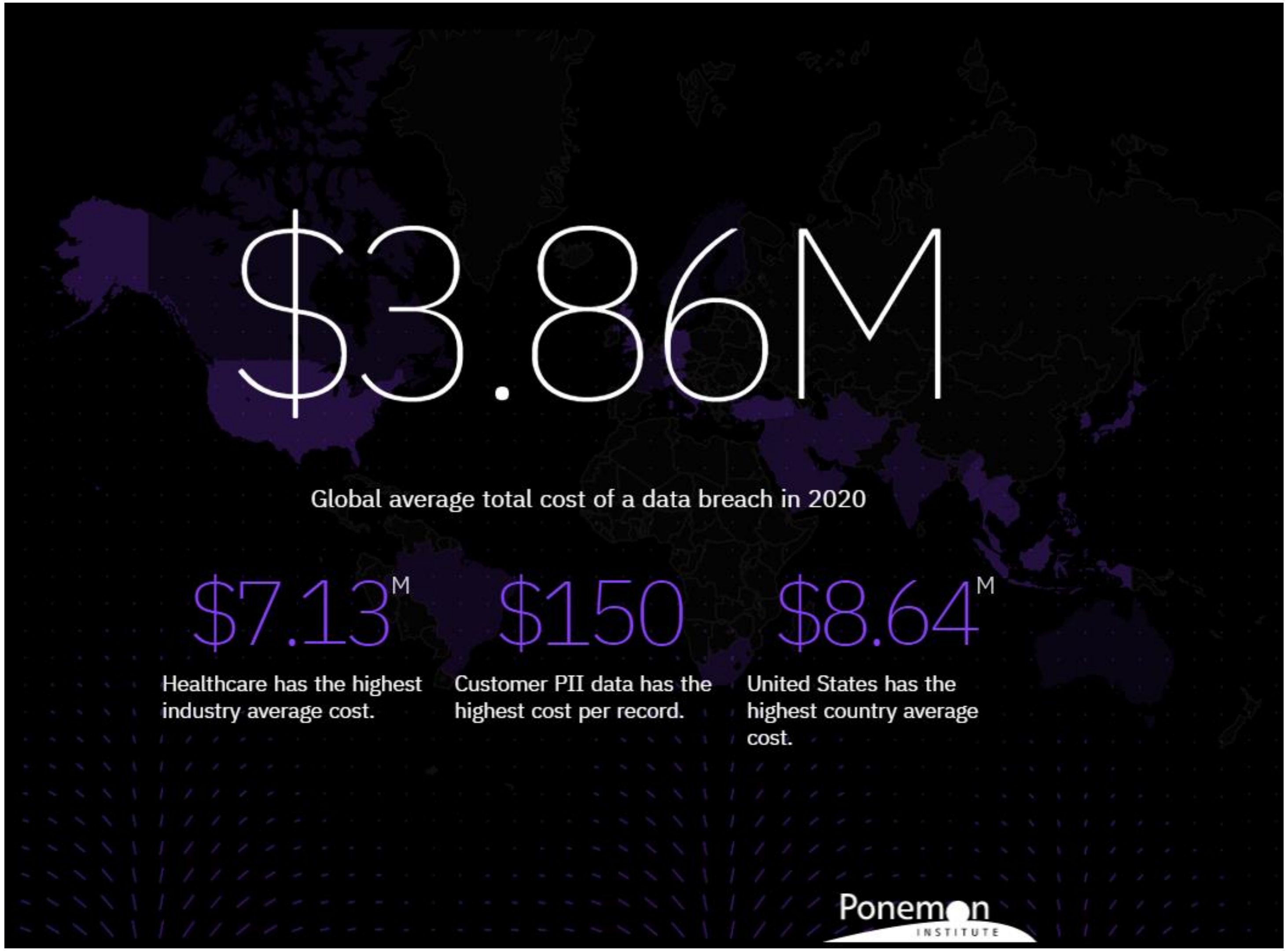


Table 2: Types of loss

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



$3.86M

Global average total cost of a data breach in 2020

$7.13M

Healthcare has the highest industry average cost.

$150

Customer PII data has the highest cost per record.

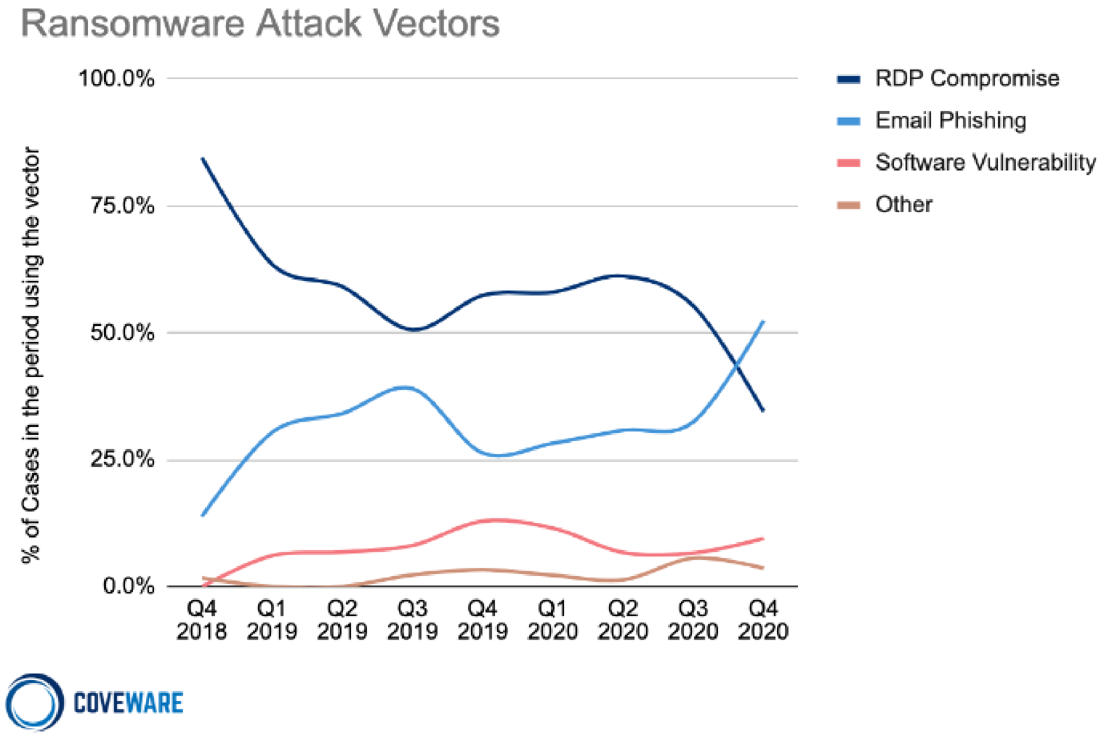
$8.64M

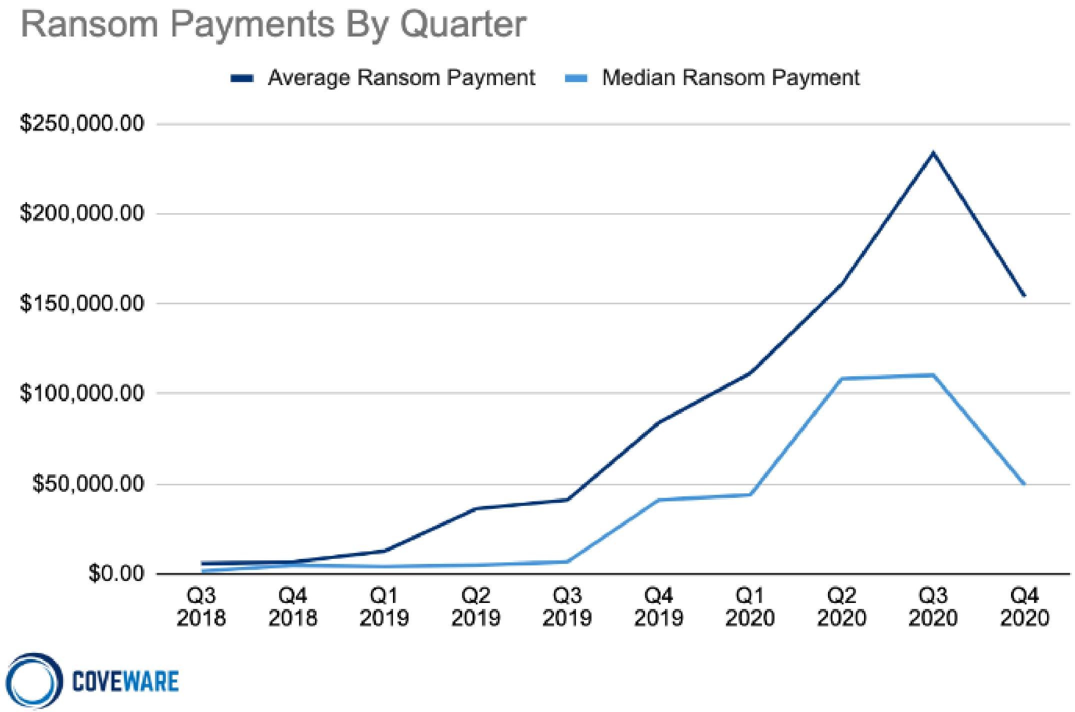
United States has the highest country average cost.

Ponemon
INSTITUTE

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

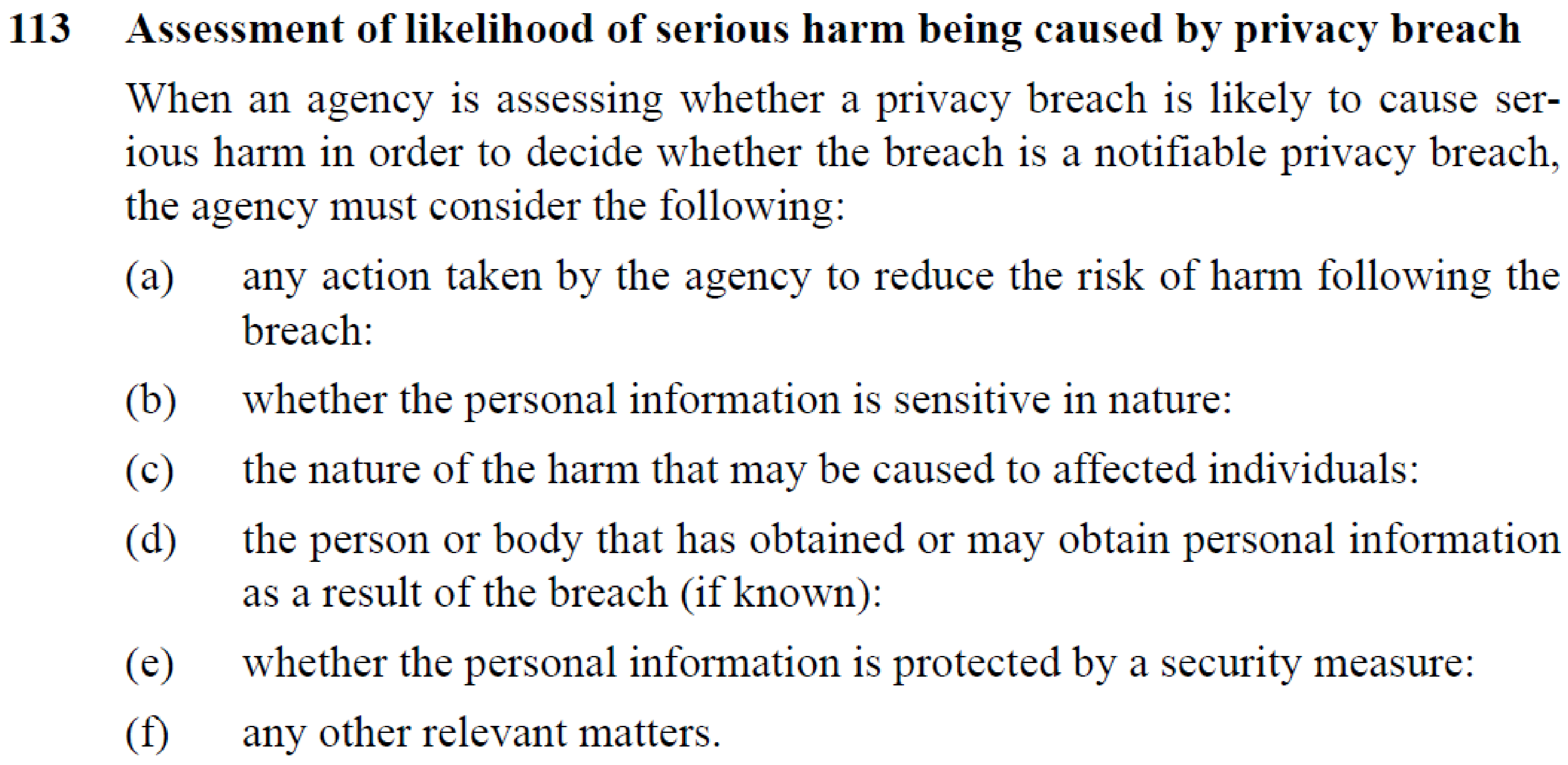
- The Privacy Act replaces 27 year old legislation and implements a number of the changes adopted in comparable jurisdictions, such as the EU, Australia, and various US states.
- These significant reforms will change the way organisations in New Zealand manage privacy issues and data security.

- ***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.

Landscape - OPC

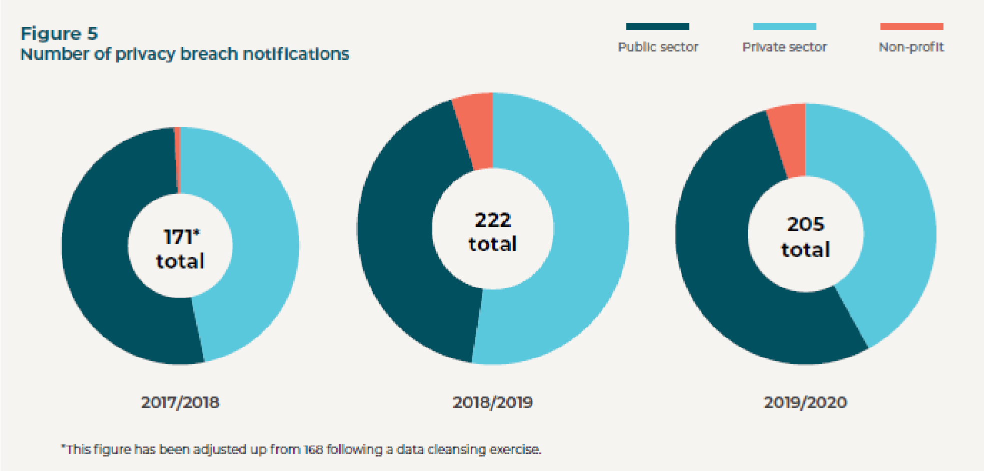


Figure 5
Number of privacy breach notifications

*This figure has been adjusted up from 168 following a data cleansing exercise.

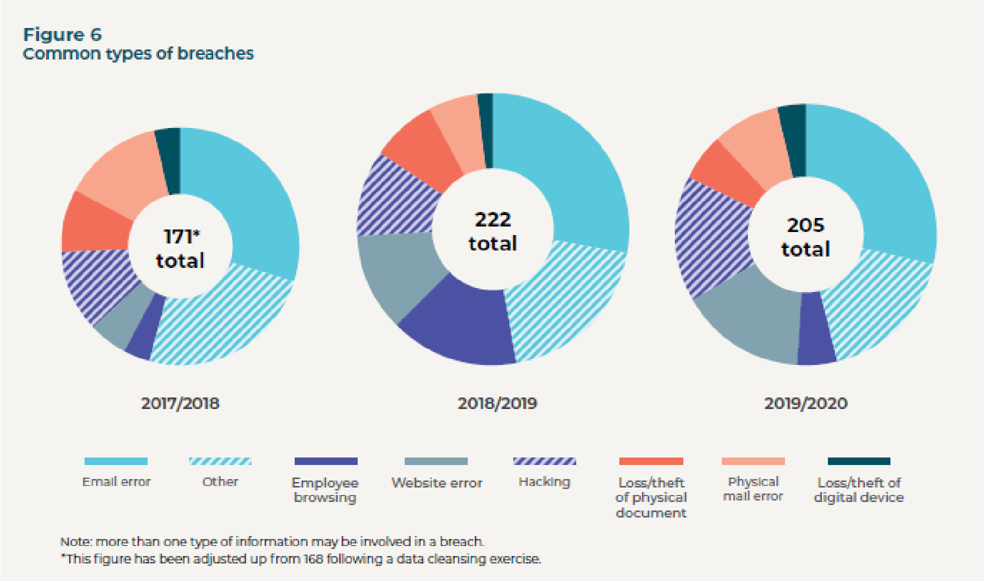


Figure 6
Common types of breaches

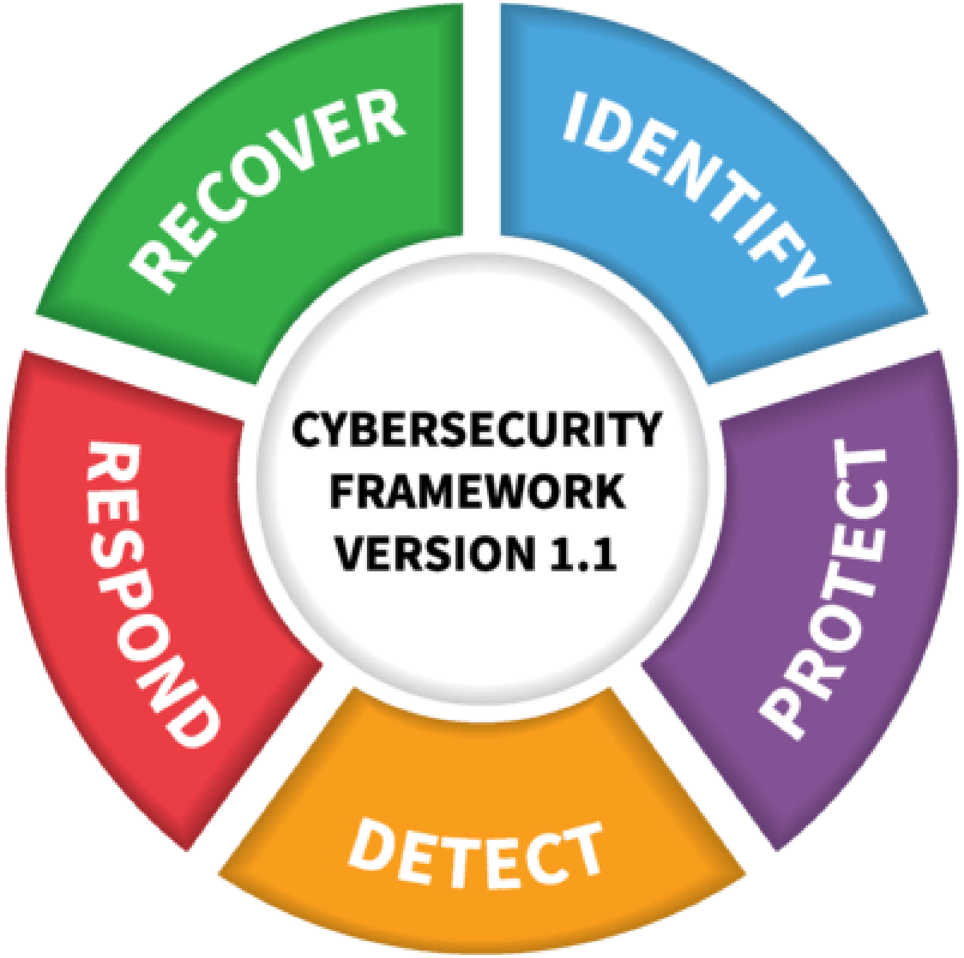
Note: more than one type of information may be involved in a breach.
*This figure has been adjusted up from 168 following a data cleansing exercise.

Source - https://www.privacy.org.nz/assets/Privacy-Commissioner-Annual-Report-20.pdf

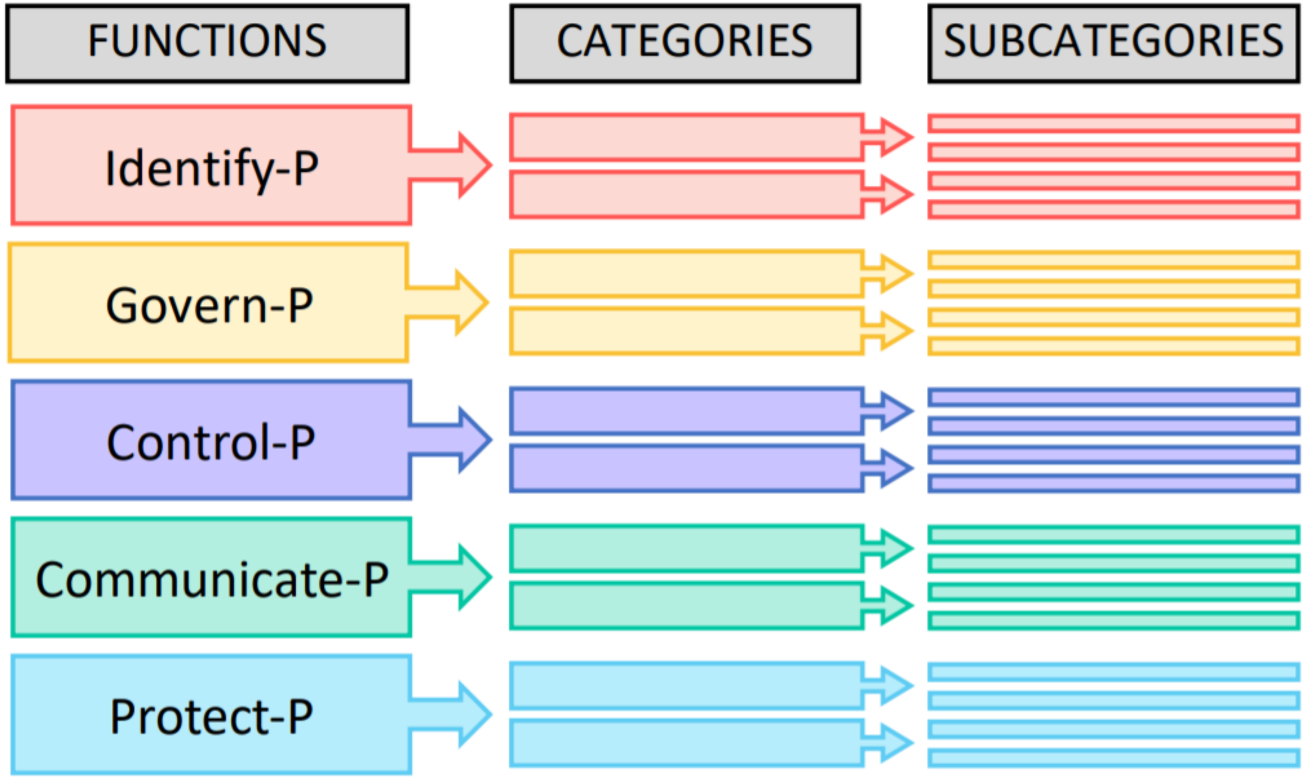
Cyber Framework

National Institute of Standards and Technology (NIST)

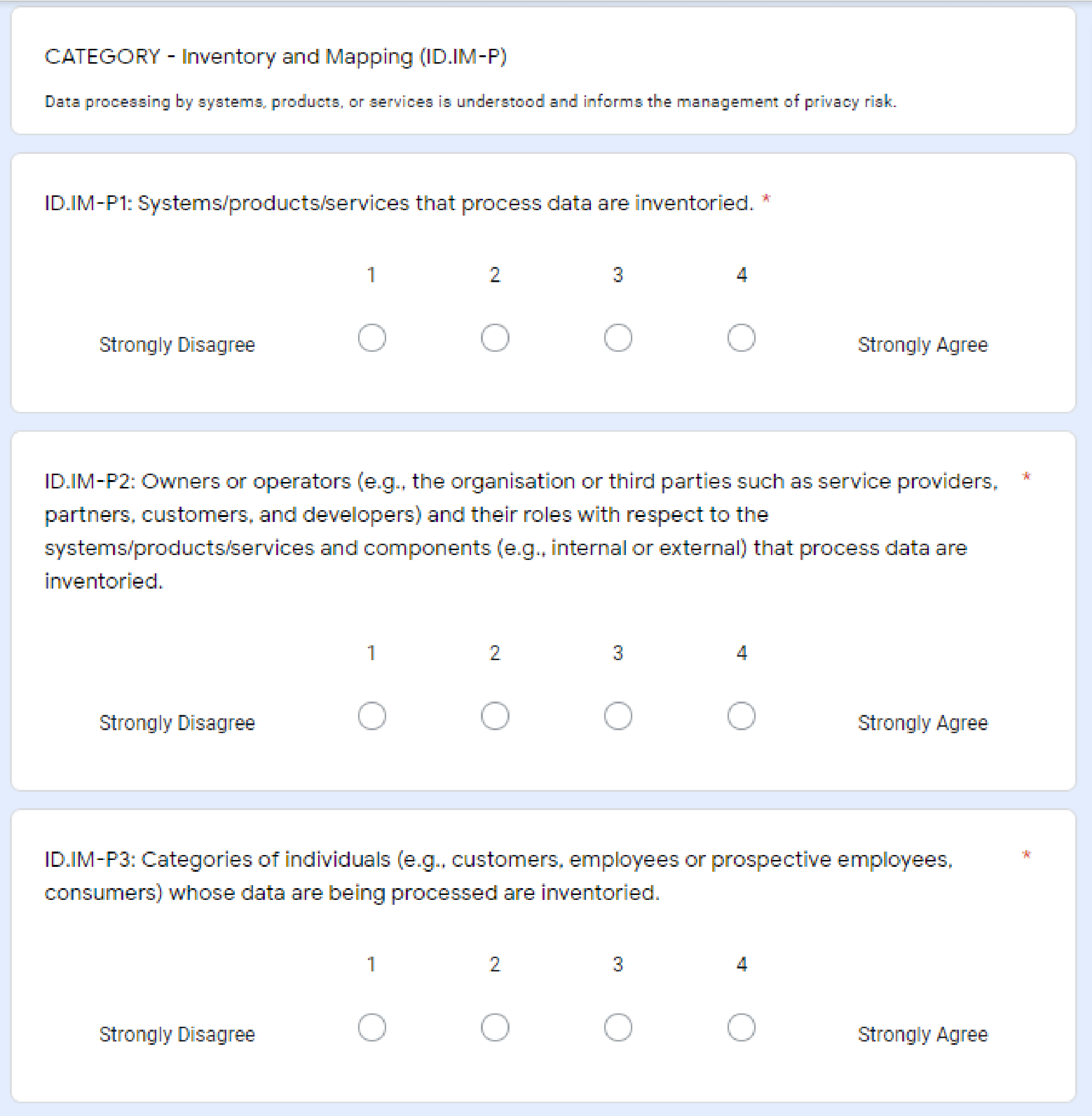
NIST CSF Framework



NIST Privacy Framework



Completing the Framework



CATEGORY - Inventory and Mapping (ID.IM-P)

Data processing by systems, products, or services is understood and informs the management of privacy risk.

ID.IM-P1: Systems/products/services that process data are inventoried. *

	1	2	3	4	
Strongly Disagree	○	○	○	○	Strongly Agree

ID.IM-P2: Owners or operators (e.g., the organisation or third parties such as service providers, partners, customers, and developers) and their roles with respect to the systems/products/services and components (e.g., internal or external) that process data are inventoried. *

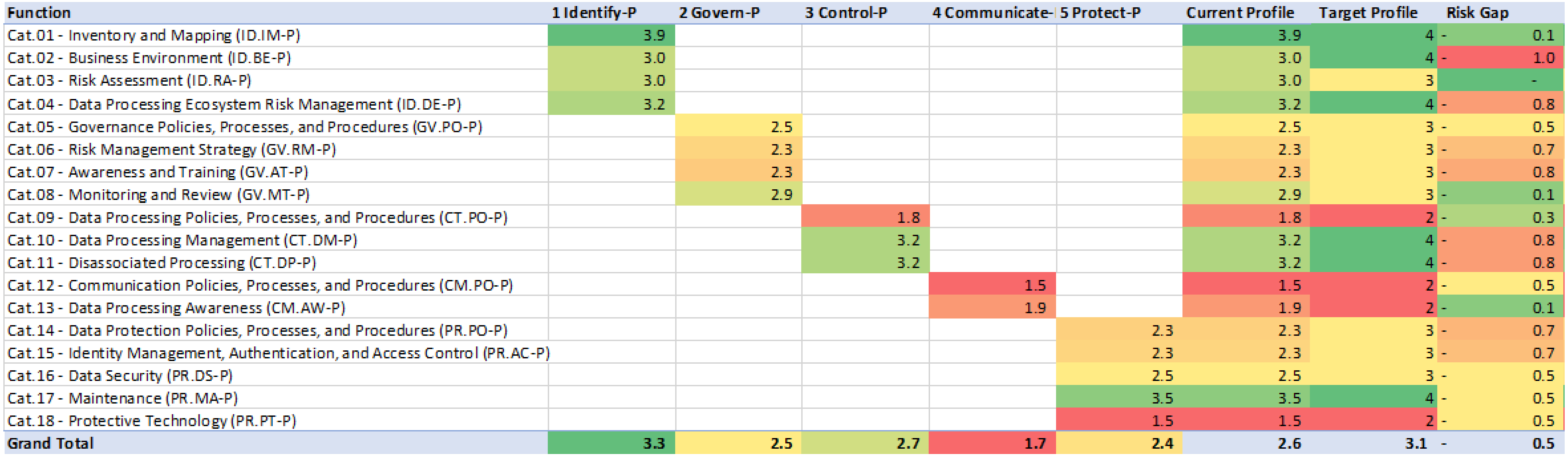
	1	2	3	4	
Strongly Disagree	○	○	○	○	Strongly Agree

ID.IM-P3: Categories of individuals (e.g., customers, employees or prospective employees, consumers) whose data are being processed are inventoried. *

	1	2	3	4	
Strongly Disagree	○	○	○	○	Strongly Agree

Completed Framework Example

Sample Report 3: Current Profile v Target Profile + Risk Gap

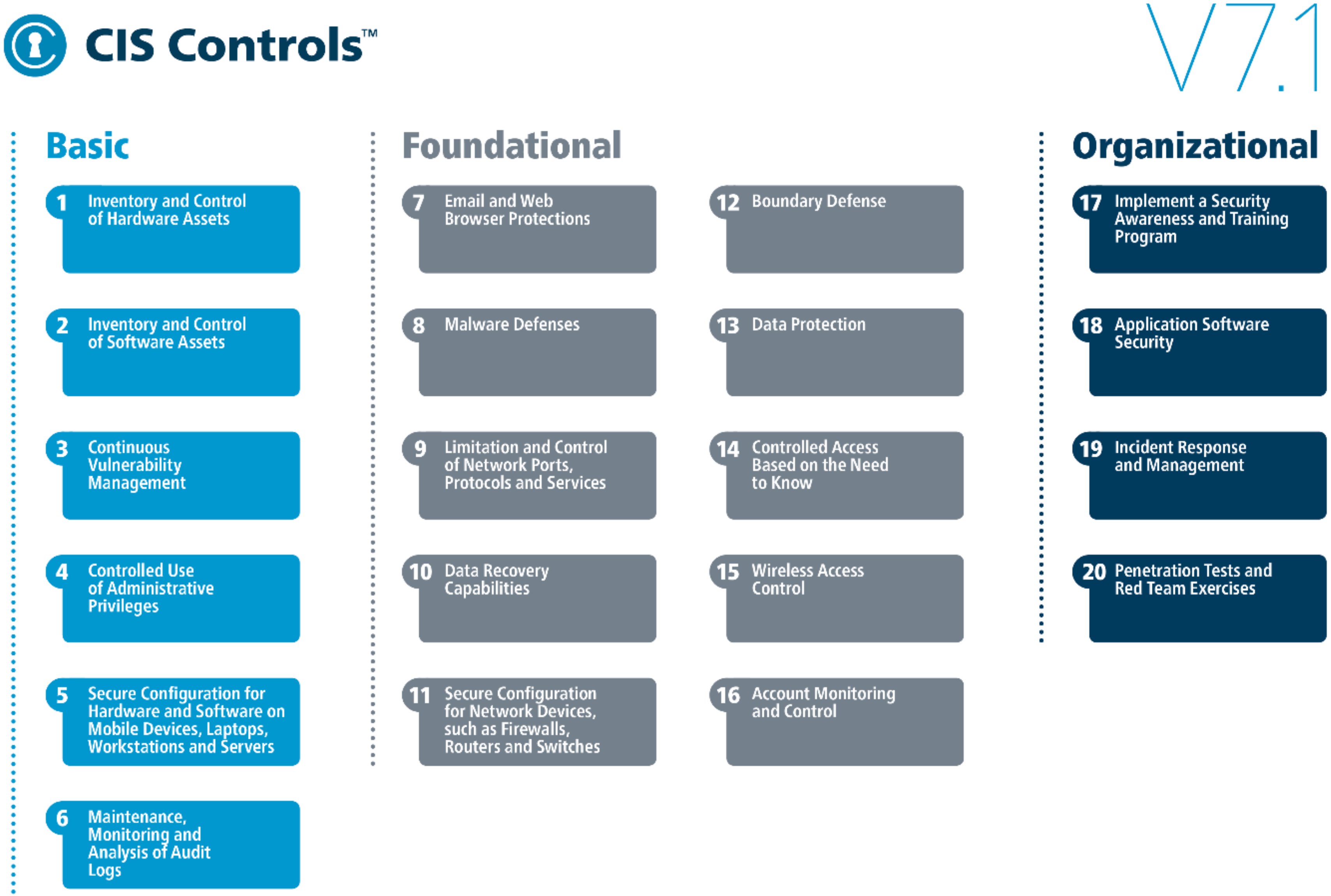


Function	1 Identify-P	2 Govern-P	3 Control-P	4 Communicate-	5 Protect-P	Current Profile	Target Profile	Risk Gap
Cat.01 - Inventory and Mapping (ID.IM-P)	3.9					3.9	4	- 0.1
Cat.02 - Business Environment (ID.BE-P)	3.0					3.0	4	- 1.0
Cat.03 - Risk Assessment (ID.RA-P)	3.0					3.0	3	-
Cat.04 - Data Processing Ecosystem Risk Management (ID.DE-P)	3.2					3.2	4	- 0.8
Cat.05 - Governance Policies, Processes, and Procedures (GV.PO-P)		2.5				2.5	3	- 0.5
Cat.06 - Risk Management Strategy (GV.RM-P)		2.3				2.3	3	- 0.7
Cat.07 - Awareness and Training (GV.AT-P)		2.3				2.3	3	- 0.8
Cat.08 - Monitoring and Review (GV.MT-P)		2.9				2.9	3	- 0.1
Cat.09 - Data Processing Policies, Processes, and Procedures (CT.PO-P)			1.8			1.8	2	- 0.3
Cat.10 - Data Processing Management (CT.DM-P)			3.2			3.2	4	- 0.8
Cat.11 - Disassociated Processing (CT.DP-P)			3.2			3.2	4	- 0.8
Cat.12 - Communication Policies, Processes, and Procedures (CM.PO-P)				1.5		1.5	2	- 0.5
Cat.13 - Data Processing Awareness (CM.AW-P)				1.9		1.9	2	- 0.1
Cat.14 - Data Protection Policies, Processes, and Procedures (PR.PO-P)					2.3	2.3	3	- 0.7
Cat.15 - Identity Management, Authentication, and Access Control (PR.AC-P)					2.3	2.3	3	- 0.7
Cat.16 - Data Security (PR.DS-P)					2.5	2.5	3	- 0.5
Cat.17 - Maintenance (PR.MA-P)					3.5	3.5	4	- 0.5
Cat.18 - Protective Technology (PR.PT-P)					1.5	1.5	2	- 0.5
Grand Total	**3.3**	**2.5**	**2.7**	**1.7**	**2.4**	**2.6**	**3.1**	**- 0.5**

Cyber Controls

Centre for Internet Security (CIS)

CIS Controls



CIS Controls™

V7.1

Basic

1 Inventory and Control of Hardware Assets

2 Inventory and Control of Software Assets

3 Continuous Vulnerability Management

4 Controlled Use of Administrative Privileges

5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7 Email and Web Browser Protections

8 Malware Defenses

9 Limitation and Control of Network Ports, Protocols and Services

10 Data Recovery Capabilities

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

12 Boundary Defense

13 Data Protection

14 Controlled Access Based on the Need to Know

15 Wireless Access Control

16 Account Monitoring and Control

Organizational

17 Implement a Security Awareness and Training Program

18 Application Software Security

19 Incident Response and Management

20 Penetration Tests and Red Team Exercises

Training

Executive and Technical

governance Leadership centre

PRACTICE GUIDE

Cyber-Risk Practice Guide

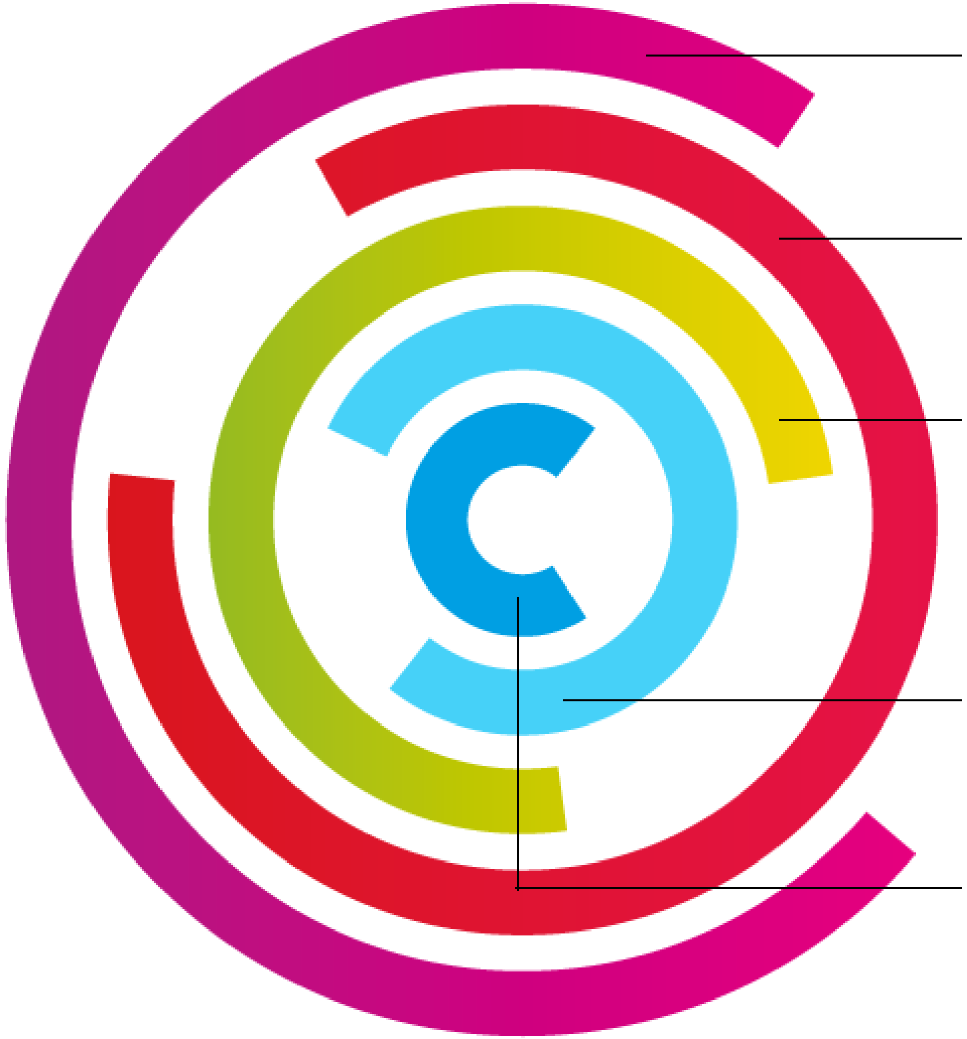
Put cybersecurity on the agenda before it becomes the agenda

Institute of Directors

At the Institute of Directors we're raising
the standard of governance in all areas
of New Zealand business and society.
iod.org.nz

Five core principles

There are five core principles for boards in their oversight of cyber risks.



1 Take a holistic approach

Directors should approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue.

2 Understand the legislative environment

Directors should understand the legal implications of cyber risk as they apply to the company's specific circumstances.

3 Access expertise and put cybersecurity on the board agenda

Boards should have adequate access to cybersecurity expertise. Discussions about cyber-risk management should be given regular and adequate time on the board meeting agenda.

4 Establish a framework

Directors should set the expectation that management will establish an enterprise-wide cyber-risk management framework.

5 Categorise the risks

Board and management discussion of cyber risks should include identification of which risks to avoid, which to accept, and which to mitigate or transfer through insurance, as well as specific plans associated with each approach.

Digital Cyber Risk Training

YOUR TRUSTED PROVIDER

GROUP MANAGEMENT

VIDEO-BASED TRAINING

LIBRARY OF TEMPLATES

STAGGERED PHISHING EMAILS

GRAPHICAL QBR REPORTING

Thank you

Campbell McKenzie

0800 WITNESS or 021 779 310

campbell@incidentresponse.co.nz

incidentresponse.co.nz

whistleblowers.co.nz

Incident Response

FORENSIC & CYBER