Cyber Security Threat Update

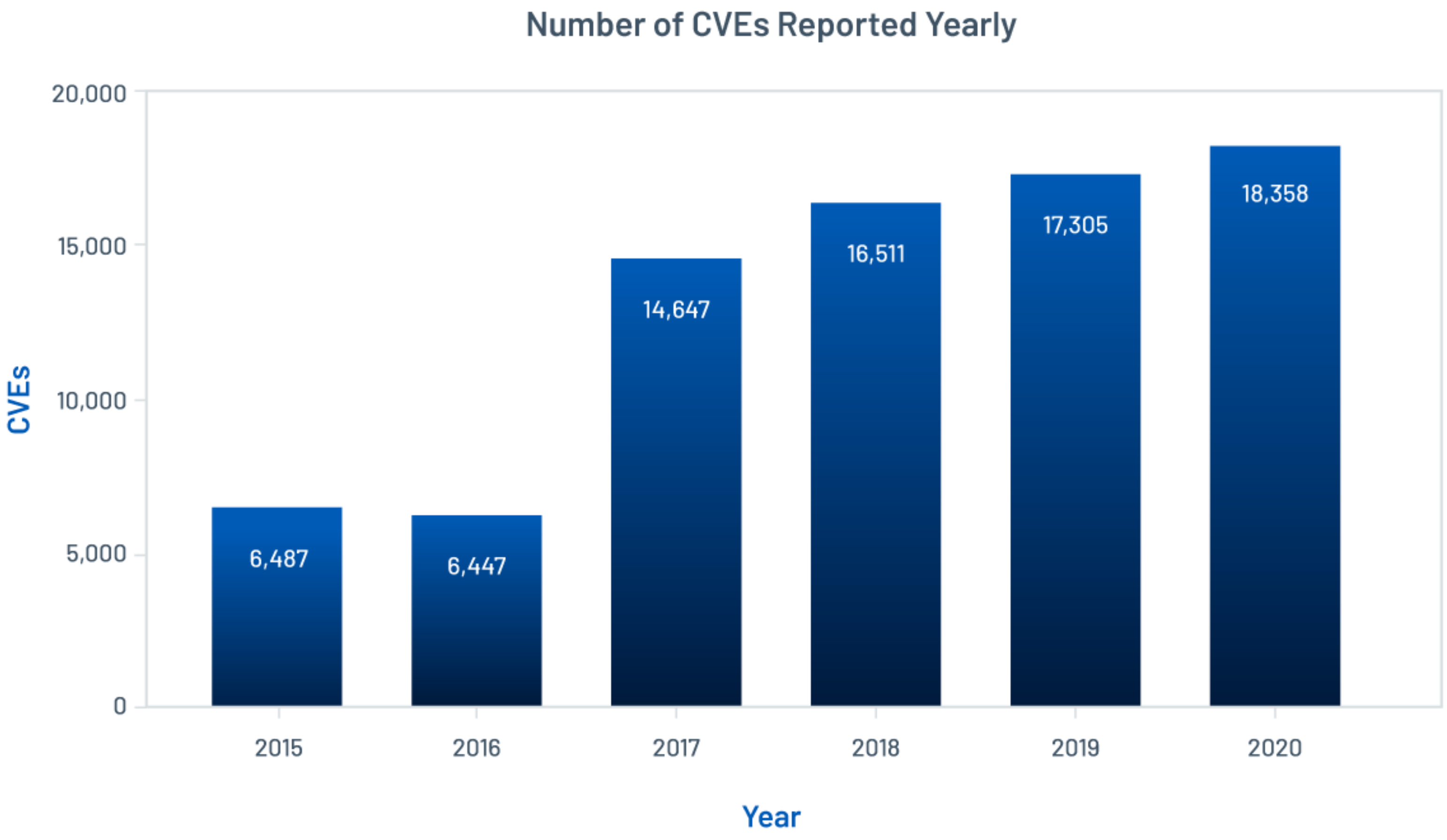
International Association of Privacy Professionals

Incident Response
FORENSIC & CYBER

Agenda

1. Cyber Threat Landscape
2. Emerging Cyber Threats
3. NIST Cyber and Privacy Frameworks
4. Cyber Threat Mitigations

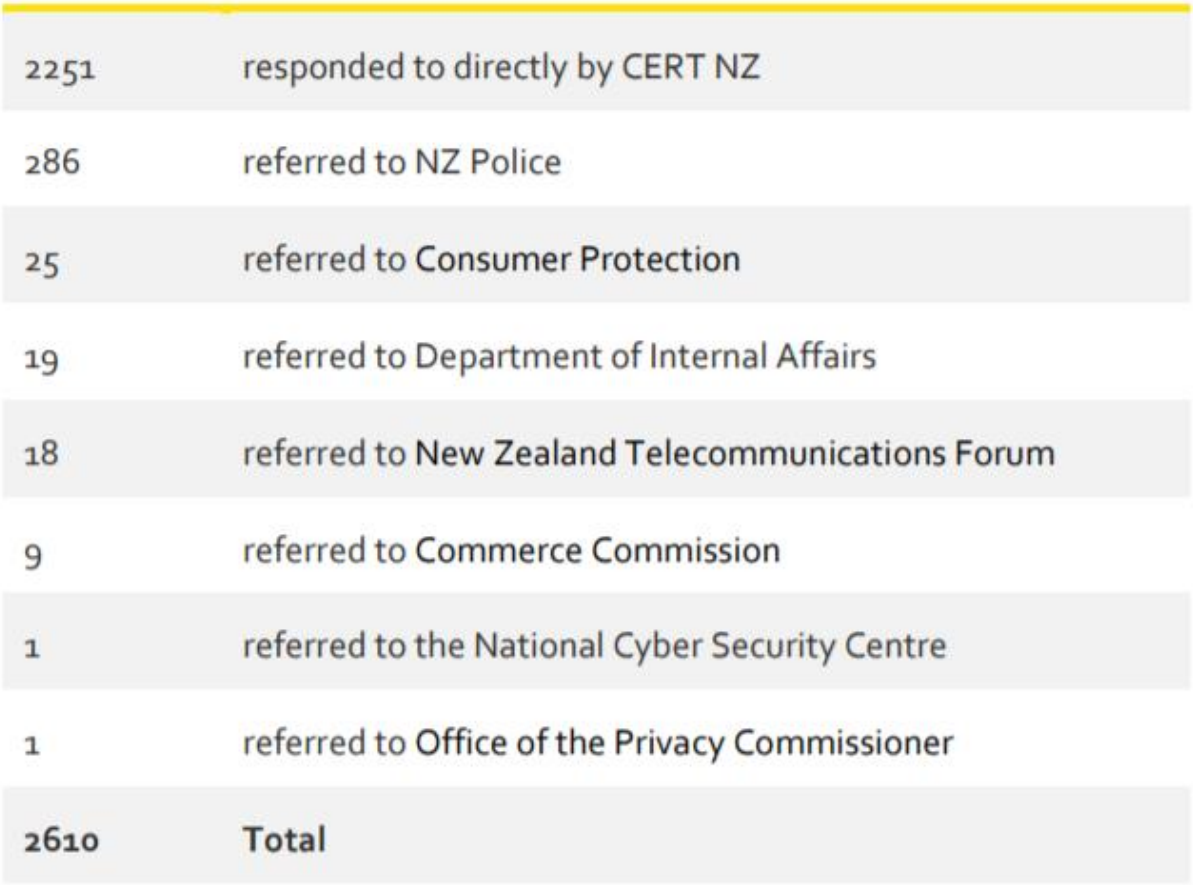
Landscape - Vulnerabilities



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

Landscape - CERT NZ

Table 1: Incident partner referrals



2251	responded to directly by CERT NZ
286	referred to NZ Police
25	referred to Consumer Protection
19	referred to Department of Internal Affairs
18	referred to New Zealand Telecommunications Forum
9	referred to Commerce Commission
1	referred to the National Cyber Security Centre
1	referred to Office of the Privacy Commissioner
2610	**Total**

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

Landscape - CERT NZ

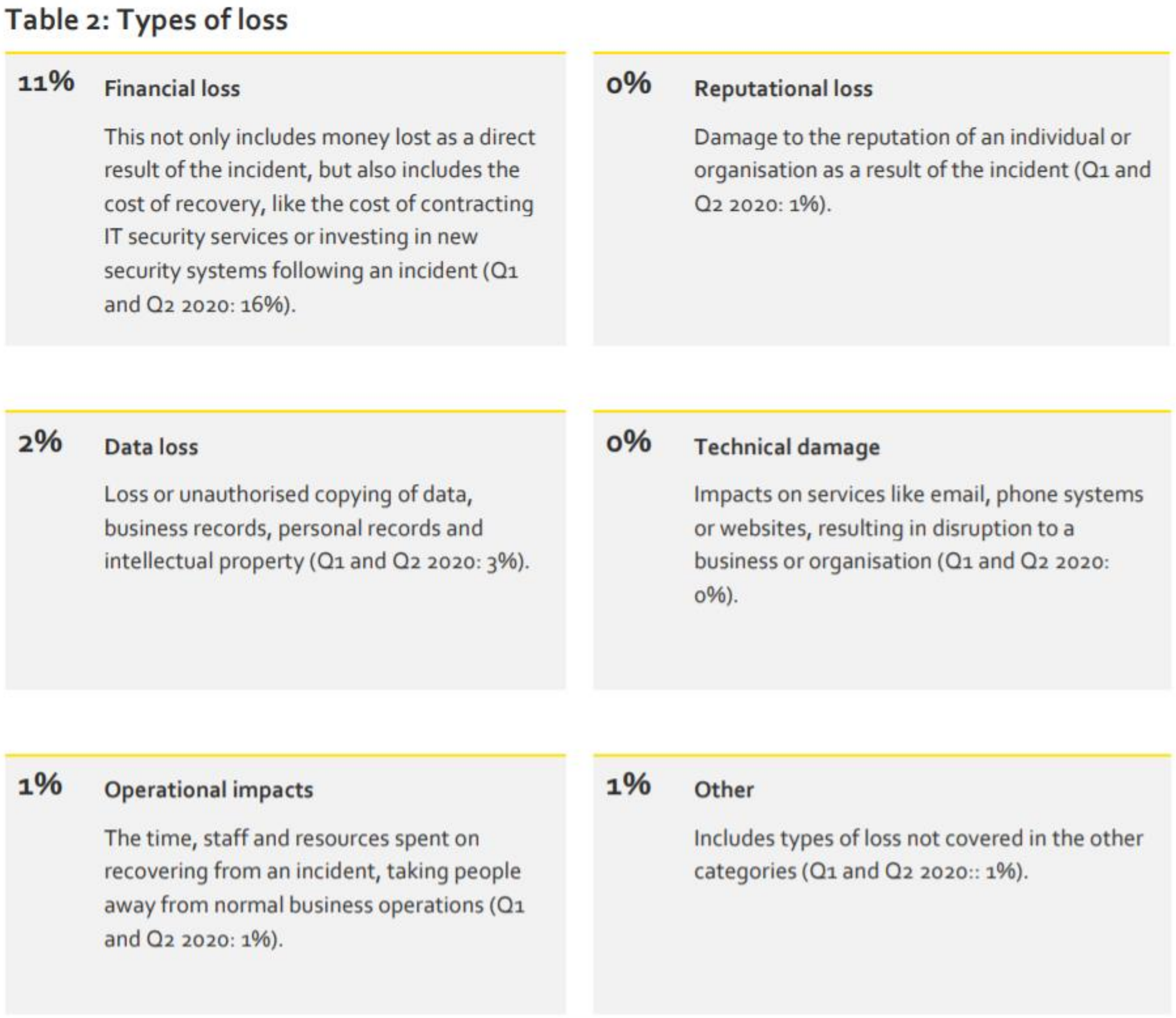


Table 2: Types of loss

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%).

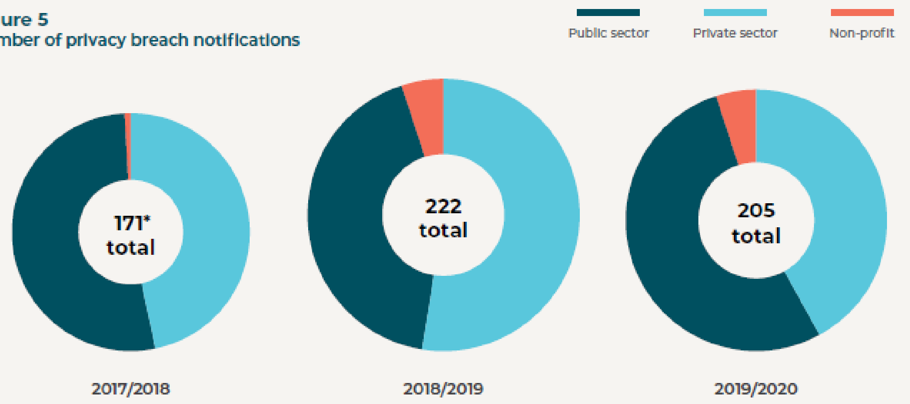
1% **Other**

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

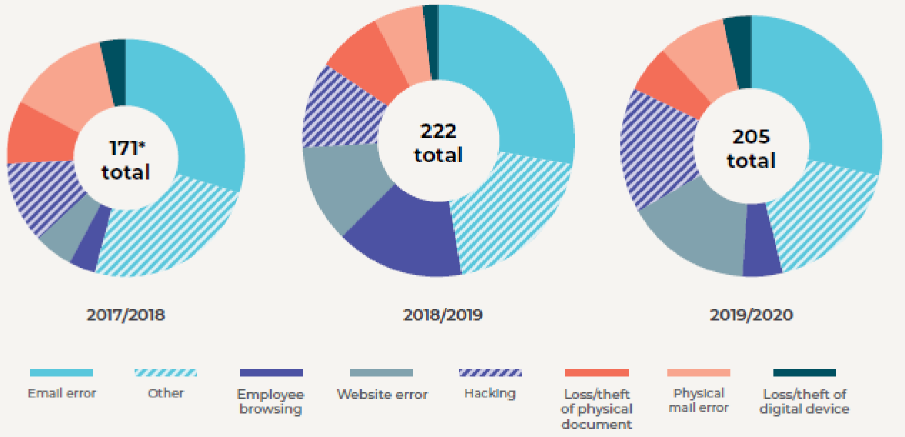
Landscape - OPC

Figure 5
Number of privacy breach notifications



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

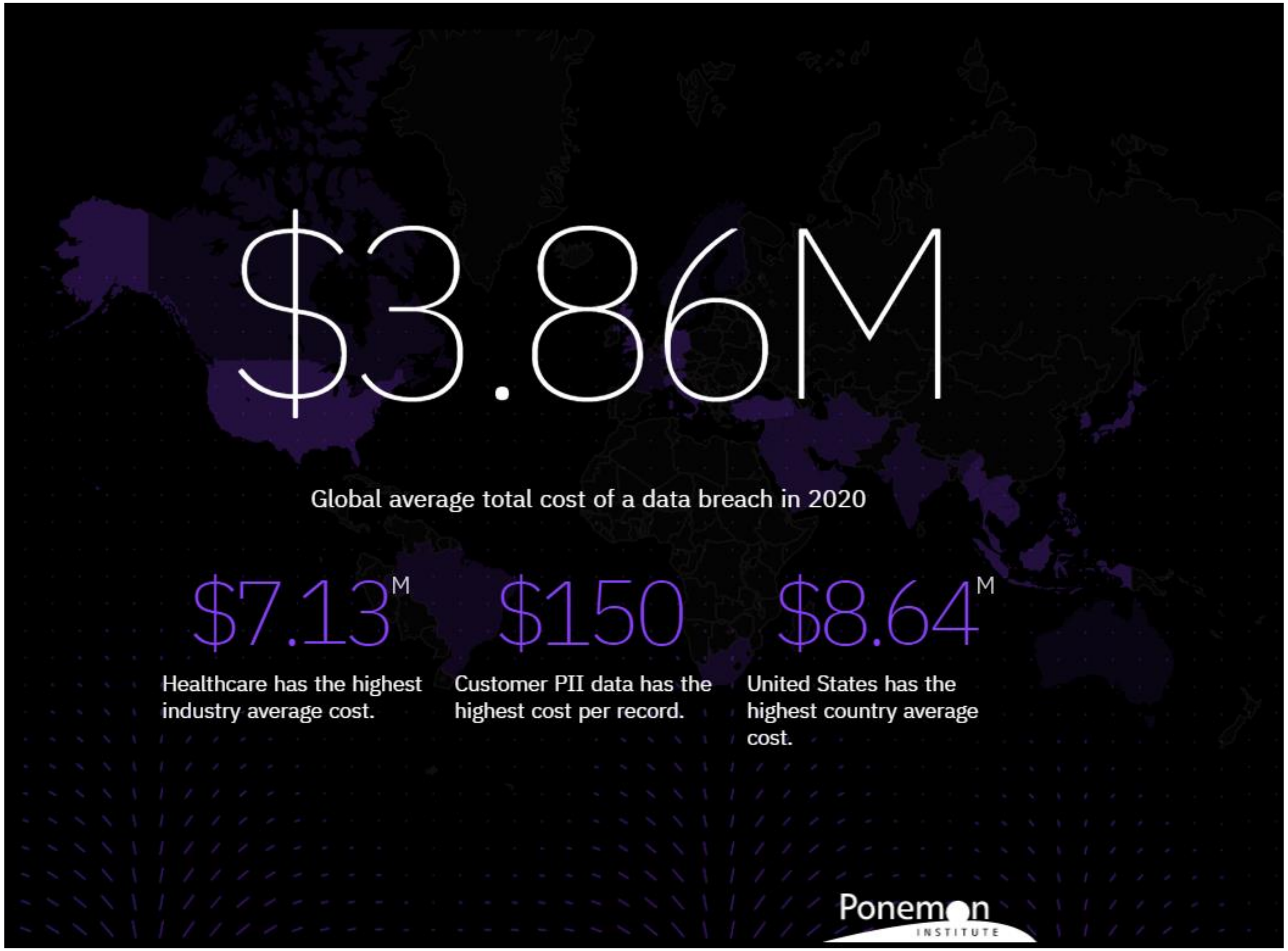
Figure 6
Common types of breaches



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

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

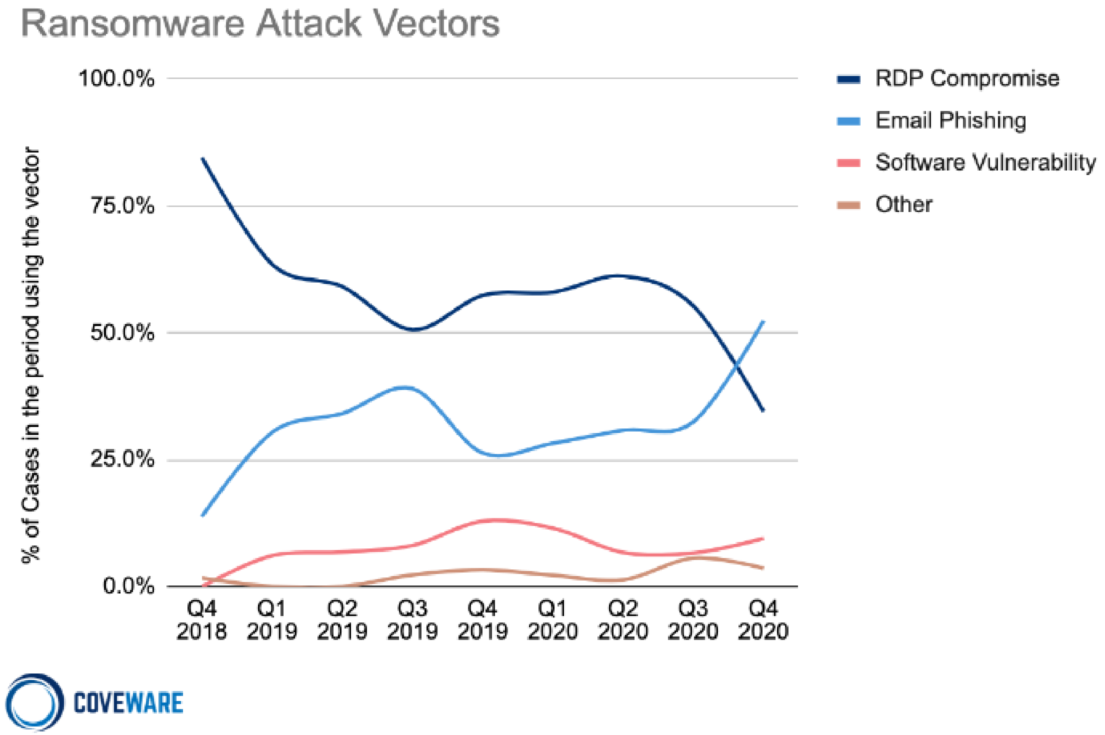
Customer PII data has the highest cost per record.

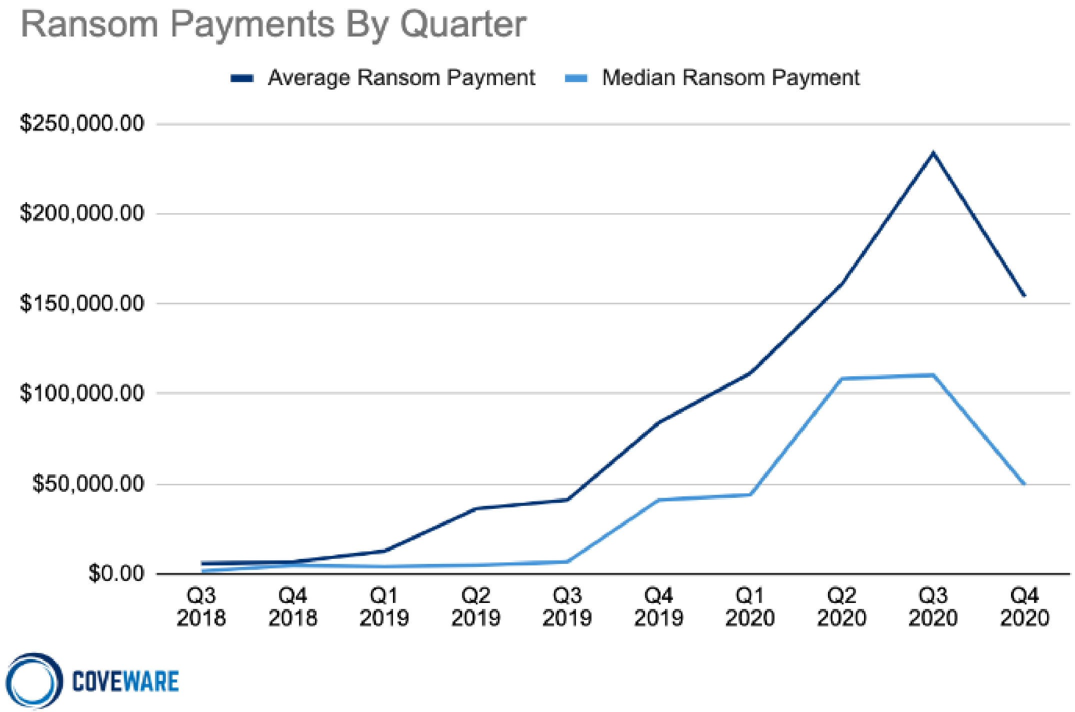
$8.64M

United States has the highest country average cost.

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

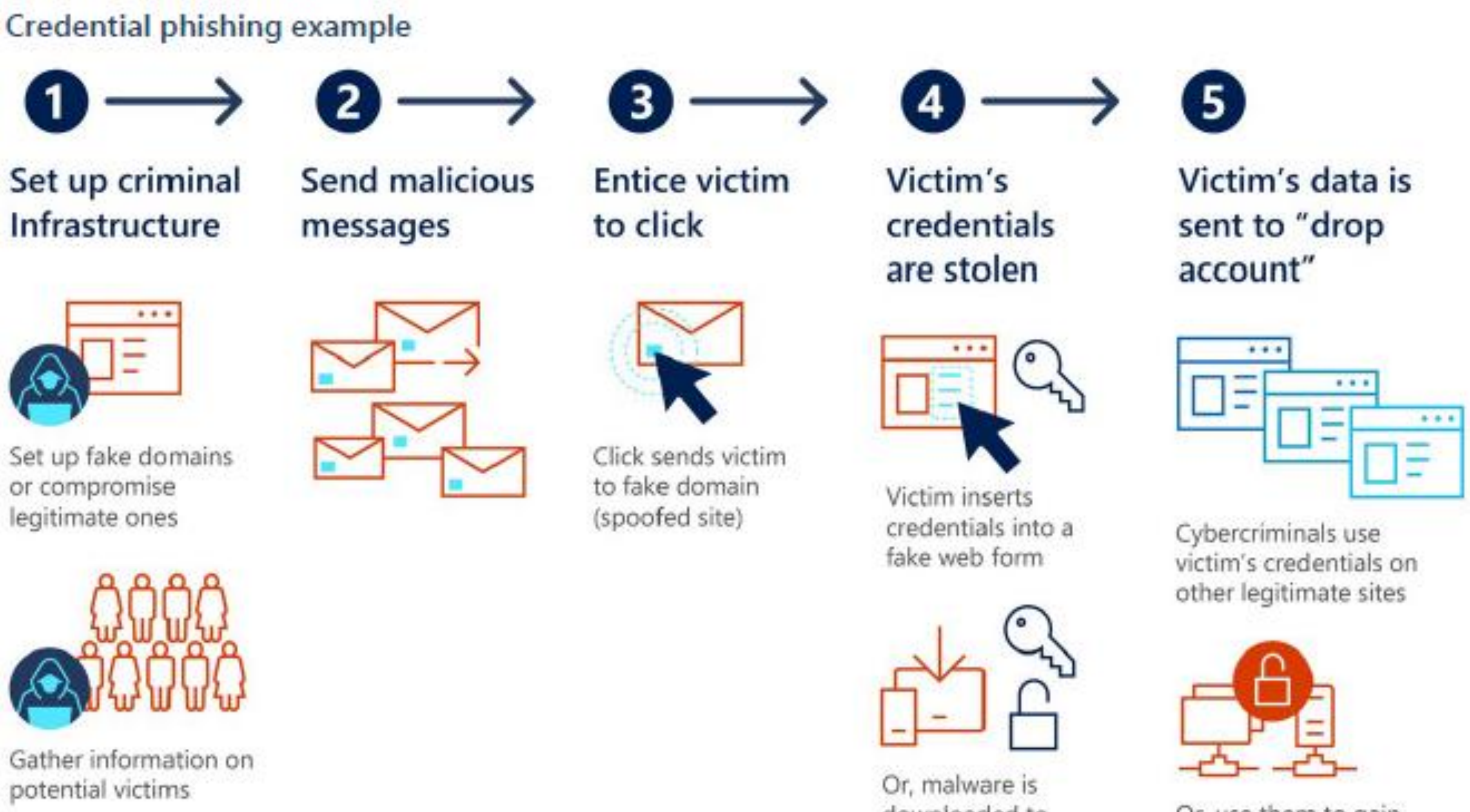
Landscape - Ransomware





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

Emerging – Business Email Compromise

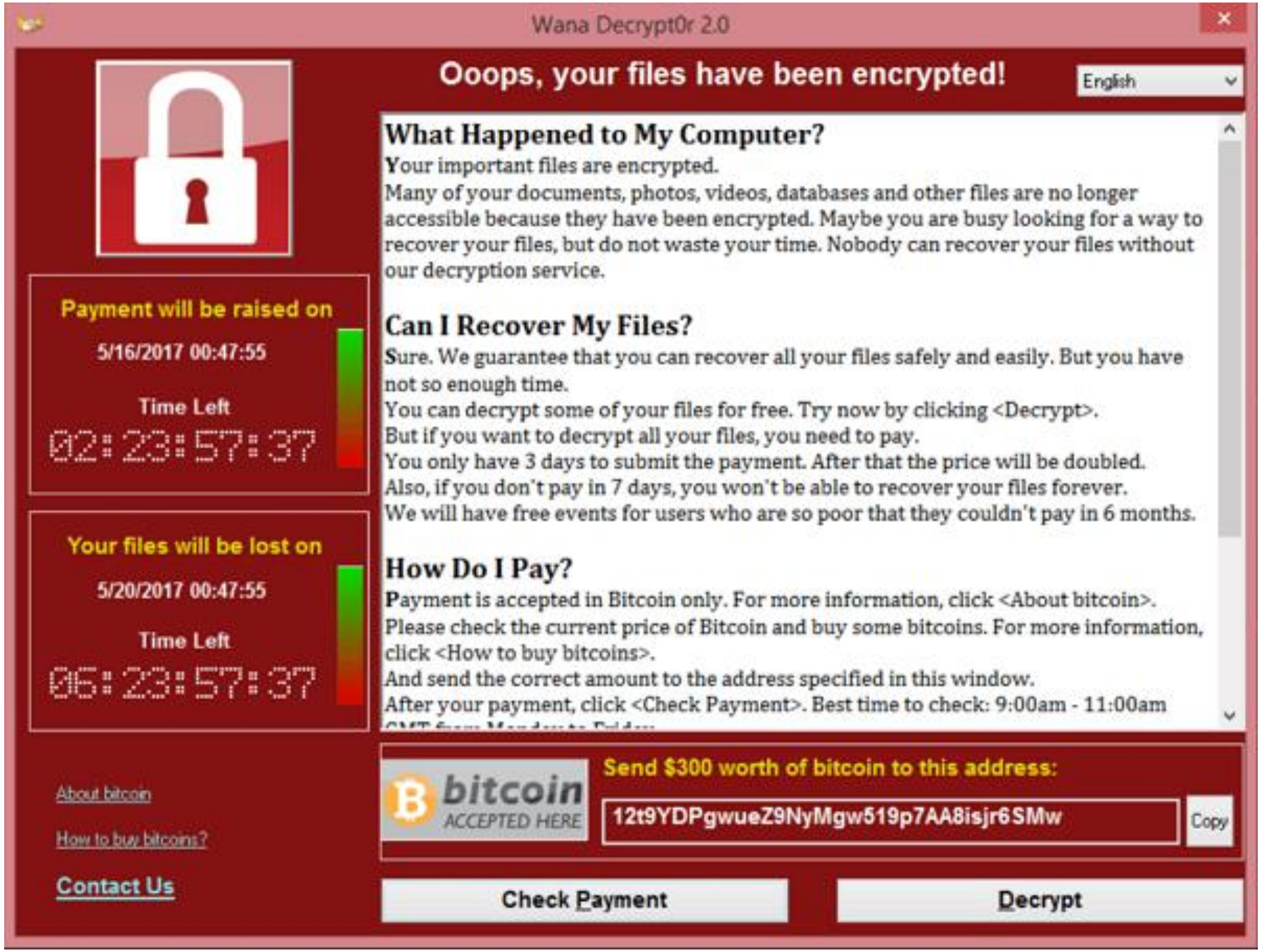


Credential phishing example

1. Set up criminal Infrastructure
   - Set up fake domains or compromise legitimate ones
   - Gather information on potential victims
2. Send malicious messages
3. Entice victim to click
   - Click sends victim to fake domain (spoofed site)
4. Victim's credentials are stolen
   - Victim inserts credentials into a fake web form
   - Or, malware is downloaded to victim's device to gather credentials
5. Victim's data is sent to "drop account"
   - Cybercriminals use victim's credentials on other legitimate sites
   - Or, use them to gain access to corporate networks and data

Source - Microsoft Digital Defense Report, September 2020

Emerging - Ransomware



Ooops, your files have been encrypted!

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

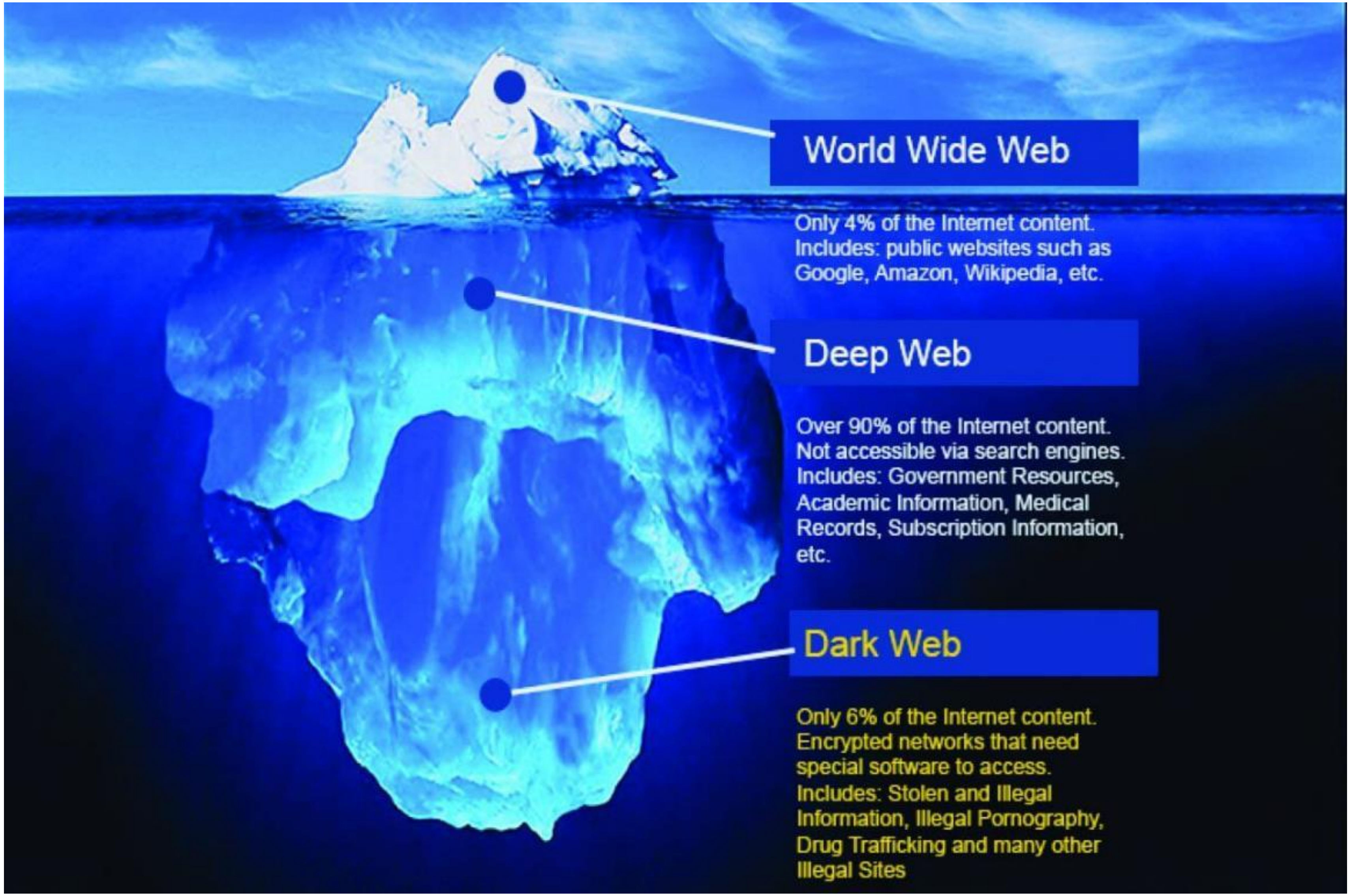
And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Emerging - Dark Web



World Wide Web

Only 4% of the Internet content. Includes: public websites such as Google, Amazon, Wikipedia, etc.

Deep Web

Over 90% of the Internet content. Not accessible via search engines. Includes: Government Resources, Academic Information, Medical Records, Subscription Information, etc.

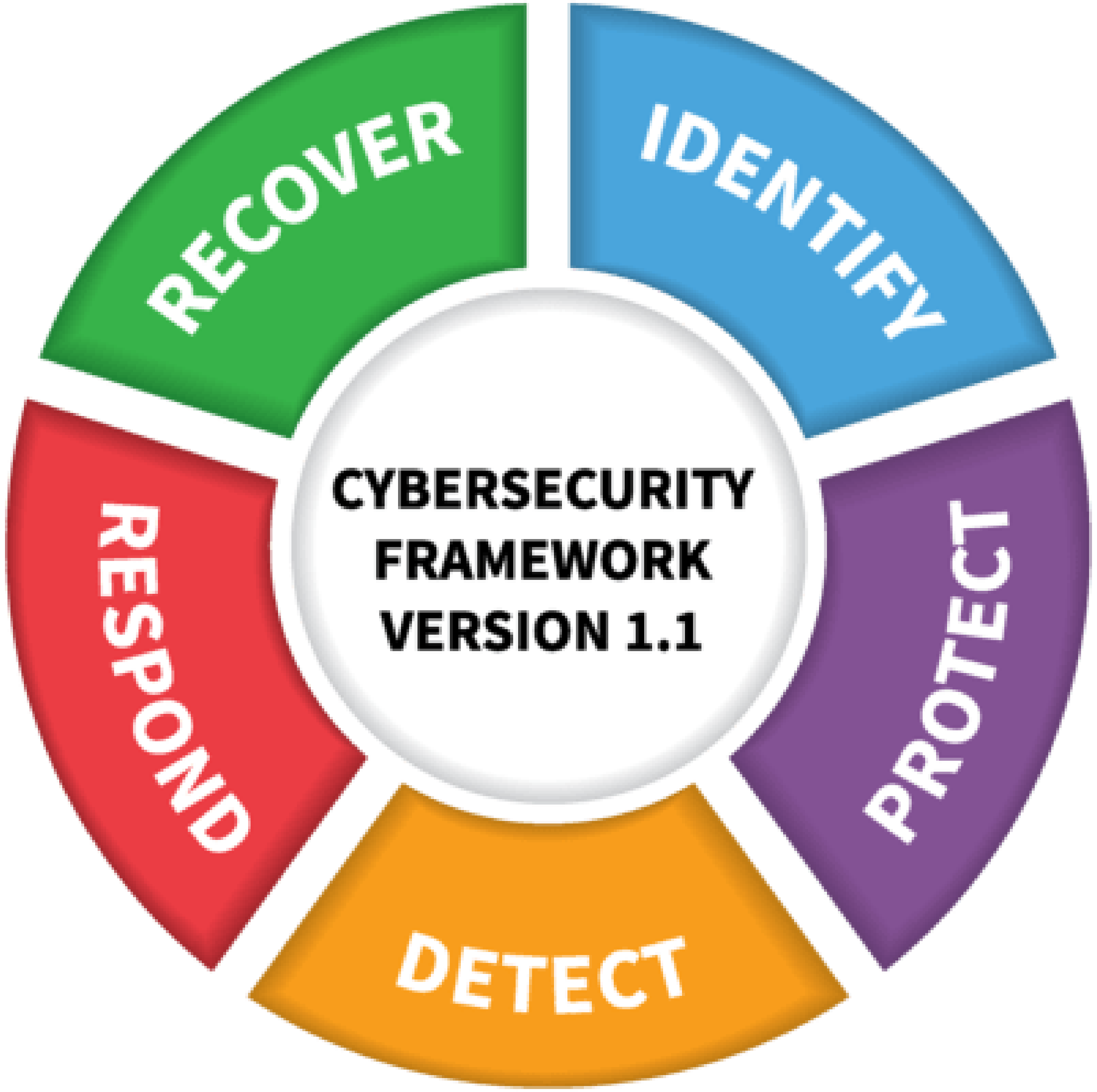
Dark Web

Only 6% of the Internet content. Encrypted networks that need special software to access. Includes: Stolen and Illegal Information, Illegal Pornography, Drug Trafficking and many other Illegal Sites

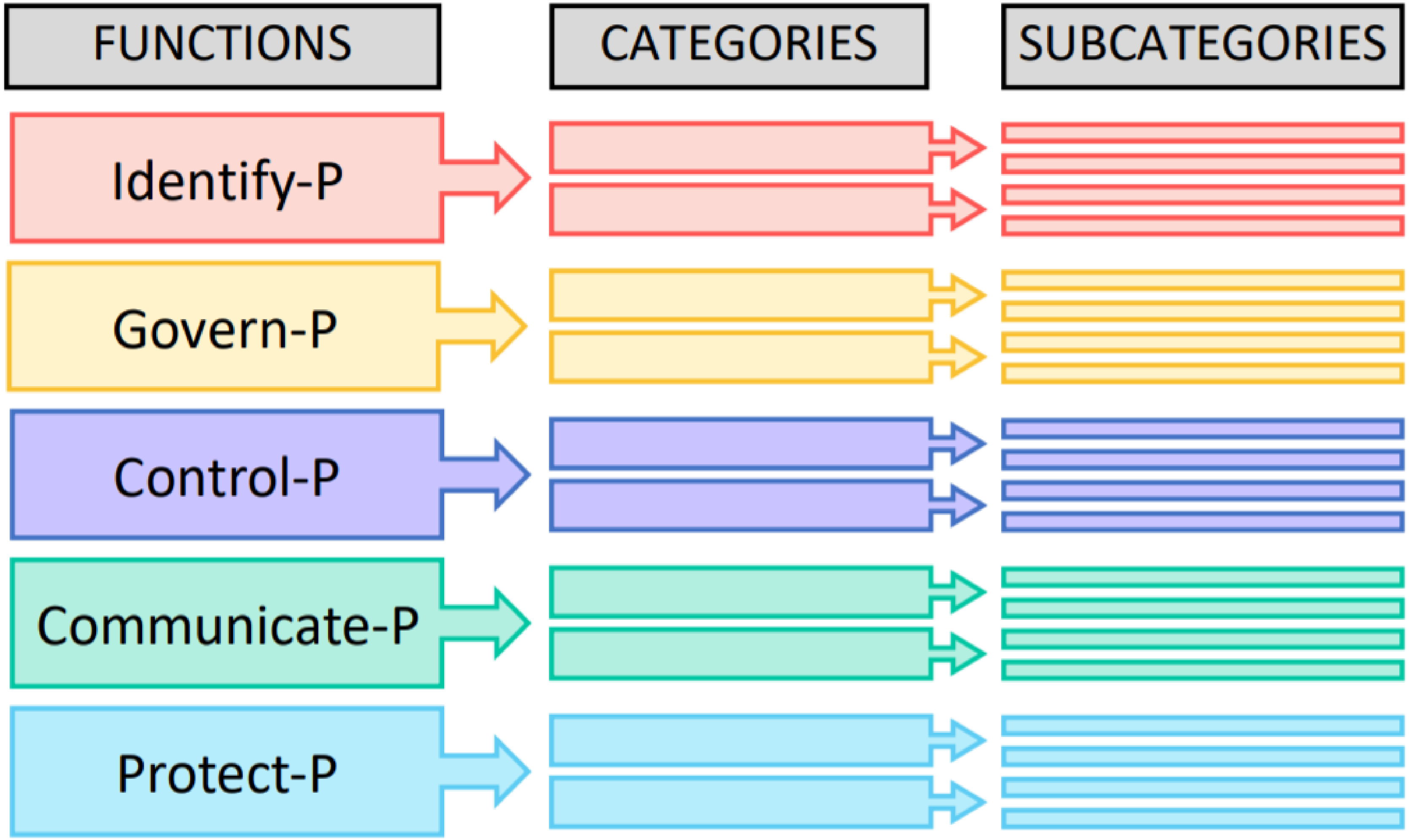
Emerging - Data Leak

Emerging - The Insider Threat

NIST – CSF Framework



NIST – Privacy Framework



FUNCTIONS

CATEGORIES

SUBCATEGORIES

Identify-P

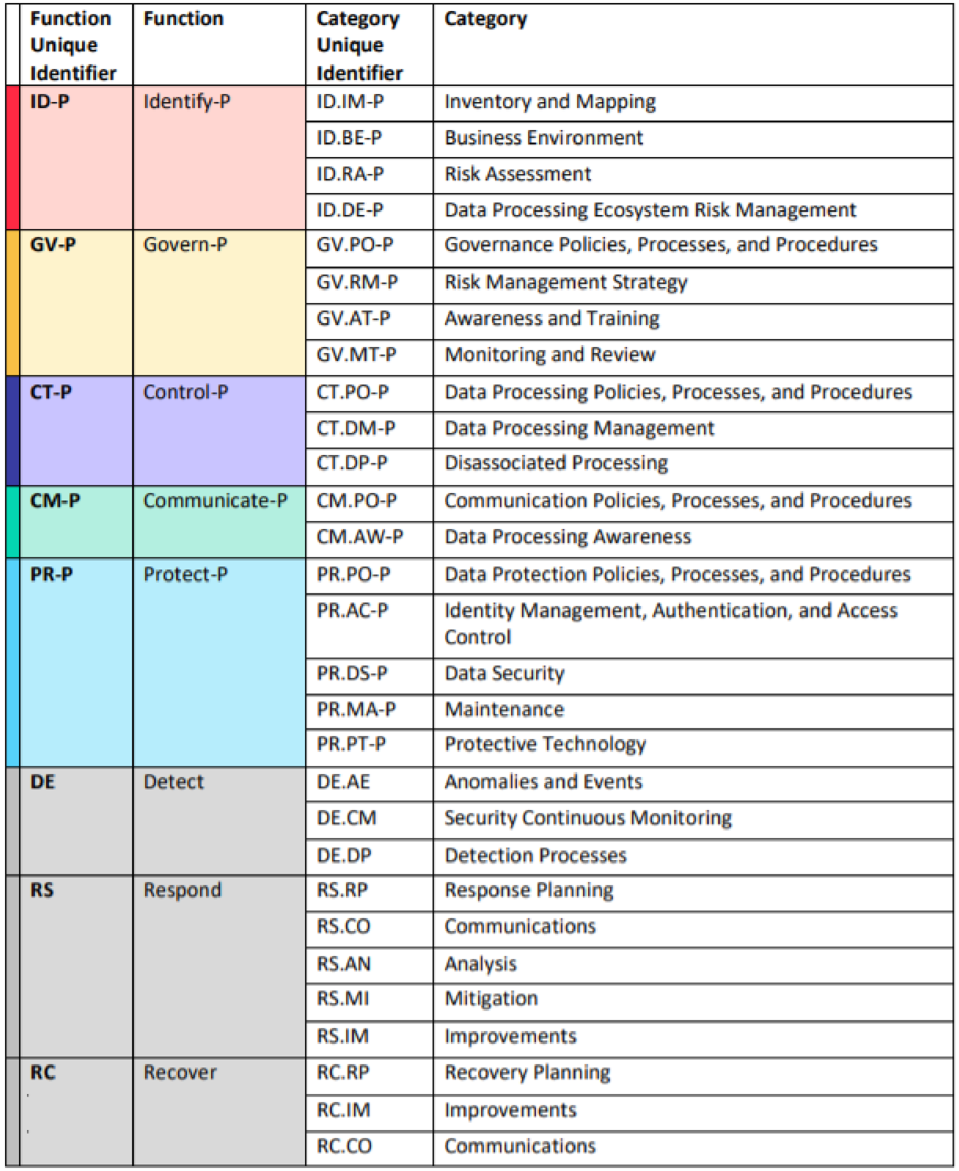
Govern-P

Control-P

Communicate-P

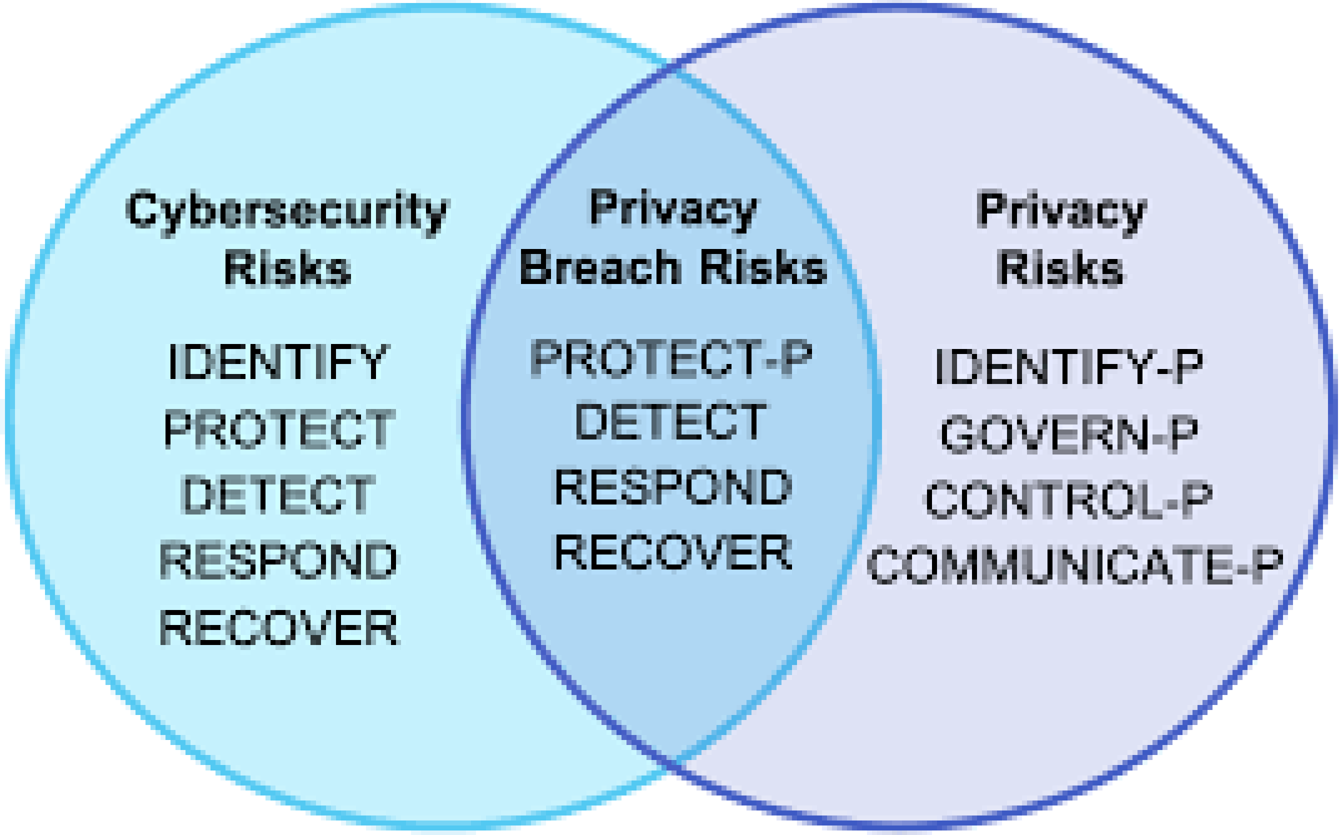
Protect-P

NIST - Privacy Framework Categories

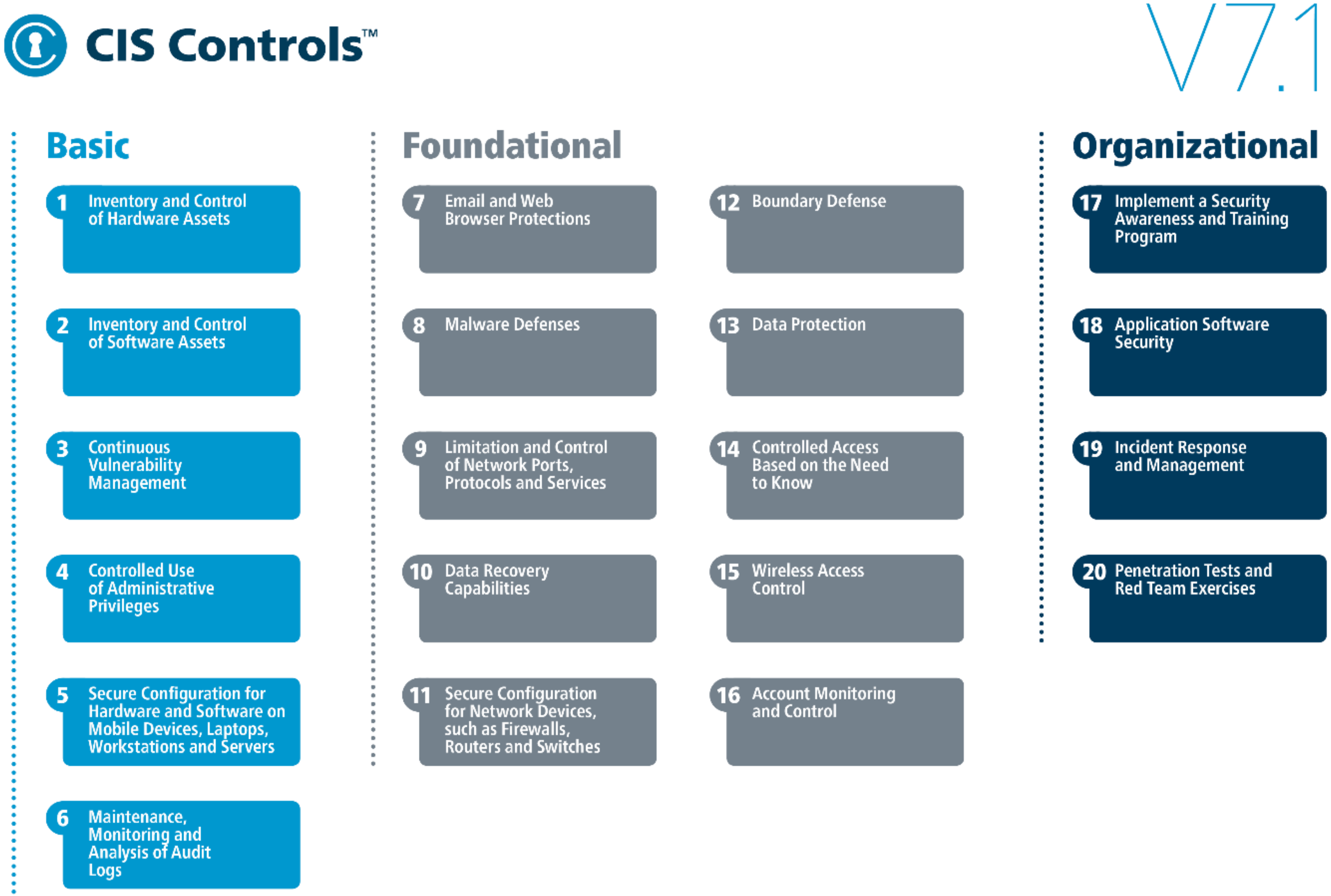


Function Unique Identifier	Function	Category Unique Identifier	Category
ID-P	Identify-P	ID.IM-P	Inventory and Mapping
		ID.BE-P	Business Environment
		ID.RA-P	Risk Assessment
		ID.DE-P	Data Processing Ecosystem Risk Management
GV-P	Govern-P	GV.PO-P	Governance Policies, Processes, and Procedures
		GV.RM-P	Risk Management Strategy
		GV.AT-P	Awareness and Training
		GV.MT-P	Monitoring and Review
CT-P	Control-P	CT.PO-P	Data Processing Policies, Processes, and Procedures
		CT.DM-P	Data Processing Management
		CT.DP-P	Disassociated Processing
CM-P	Communicate-P	CM.PO-P	Communication Policies, Processes, and Procedures
		CM.AW-P	Data Processing Awareness
PR-P	Protect-P	PR.PO-P	Data Protection Policies, Processes, and Procedures
		PR.AC-P	Identity Management, Authentication, and Access Control
		PR.DS-P	Data Security
		PR.MA-P	Maintenance
		PR.PT-P	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

NIST - Combined Frameworks



Mitigations - 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

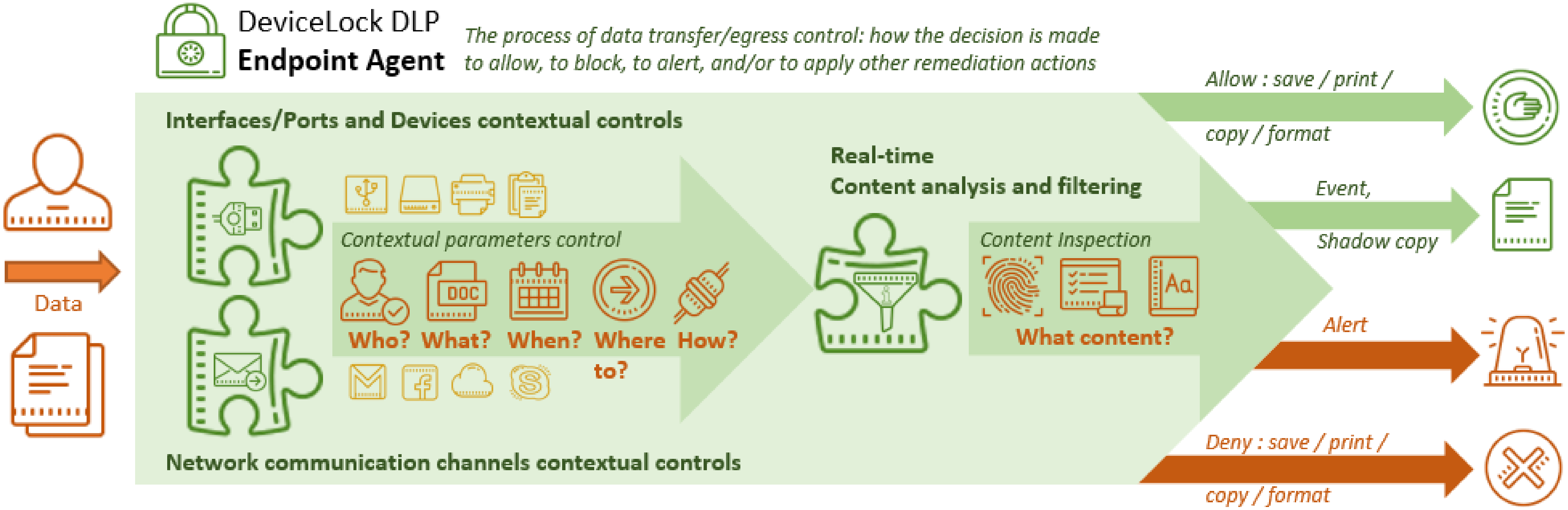
17 Implement a Security Awareness and Training Program

18 Application Software Security

19 Incident Response and Management

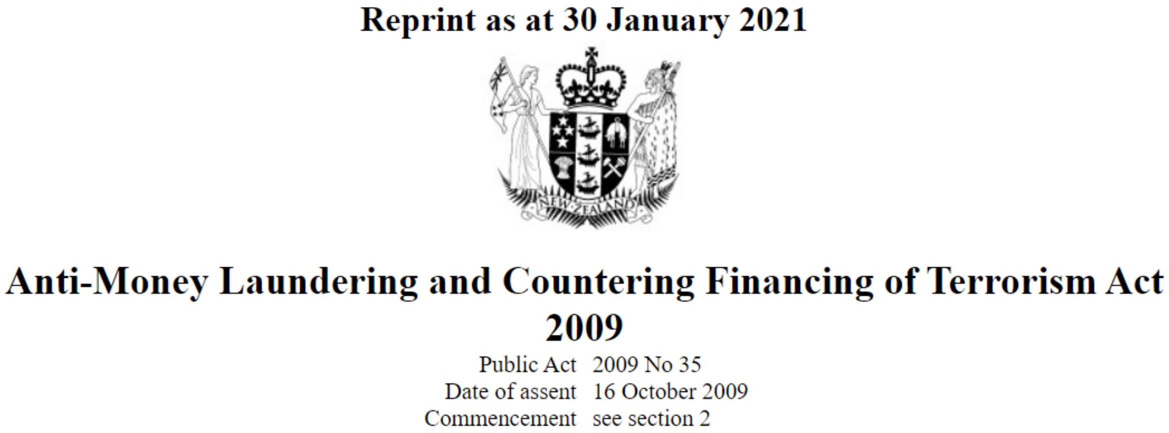
20 Penetration Tests and Red Team Exercises

Mitigations - Data Flows



DeviceLock DLP
Endpoint Agent
The process of data transfer/egress control: how the decision is made to allow, to block, to alert, and/or to apply other remediation actions
Data
Interfaces/Ports and Devices contextual controls
Contextual parameters control
Who? What? When? Where to? How?
DOC
Network communication channels contextual controls
Real-time
Content analysis and filtering
Content Inspection
Aa
What content?
Allow : save / print / copy / format
Event, Shadow copy
Alert
Deny : save / print / copy / format

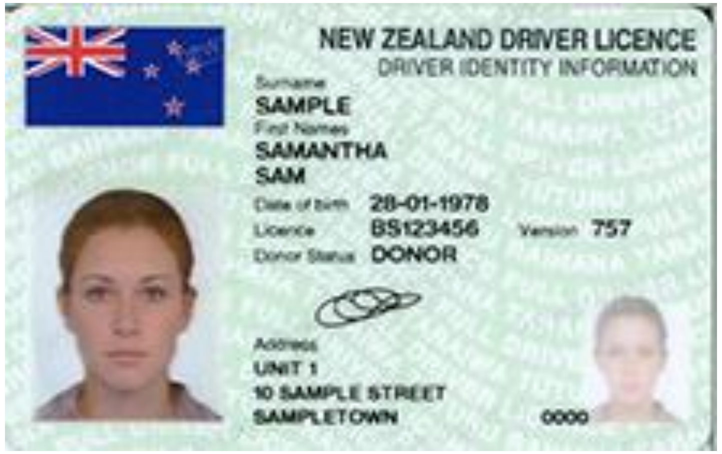
Mitigations - PII Assessment



Reprint as at 30 January 2021

Anti-Money Laundering and Countering Financing of Terrorism Act 2009

Public Act	2009 No 35
Date of assent	16 October 2009
Commencement	see section 2

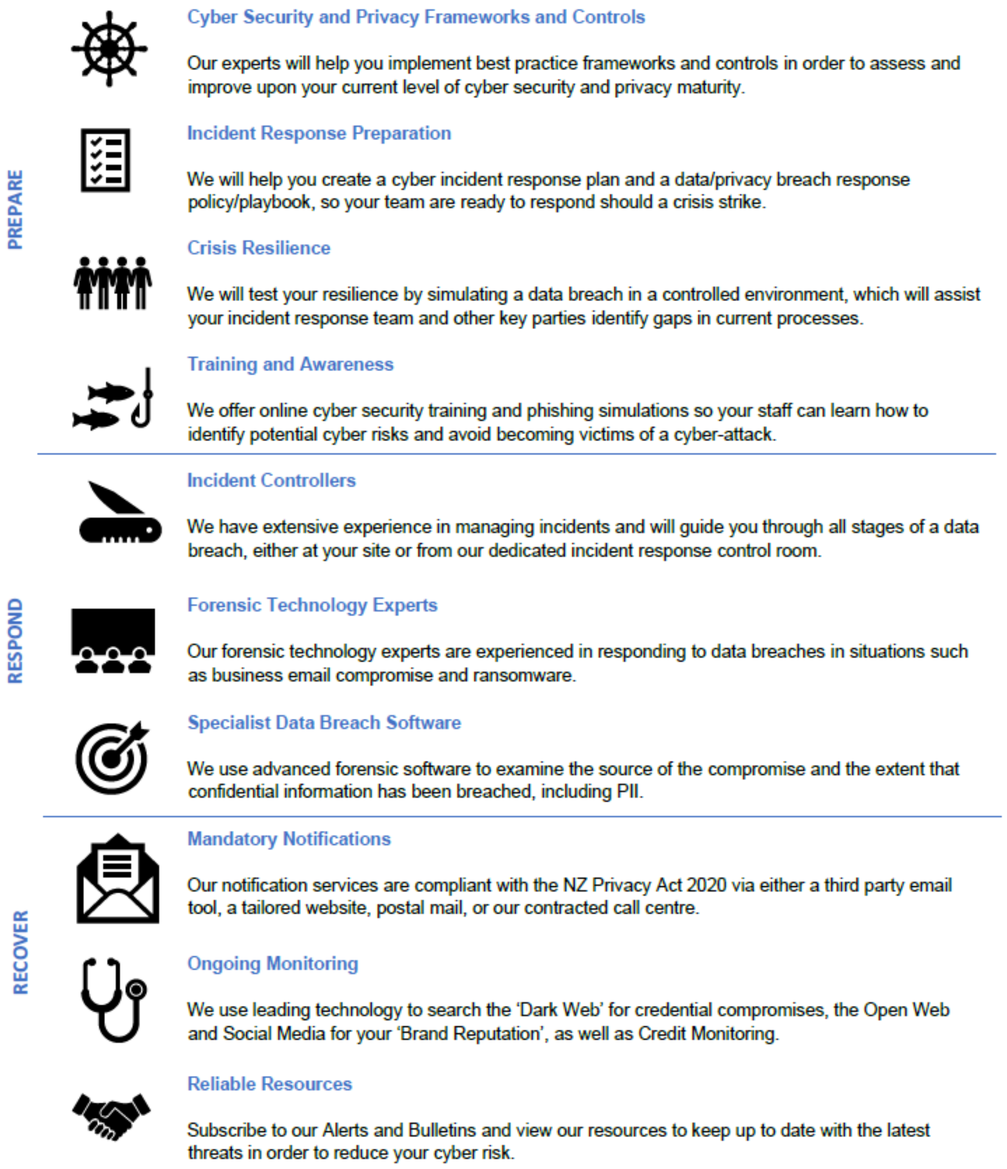


NEW ZEALAND DRIVER LICENCE
DRIVER IDENTITY INFORMATION

Surname
SAMPLE
First Names
SAMANTHA
SAM
Date of birth 28-01-1978
Licence BS123456 Version 757
Donor Status DONOR

Address
UNIT 1
10 SAMPLE STREET
SAMPLETOWN 0000

Mitigations – Data Breach Response



PREPARE

Cyber Security and Privacy Frameworks and Controls

Our experts will help you implement best practice frameworks and controls in order to assess and improve upon your current level of cyber security and privacy maturity.

Incident Response Preparation

We will help you create a cyber incident response plan and a data/privacy breach response policy/playbook, so your team are ready to respond should a crisis strike.

Crisis Resilience

We will test your resilience by simulating a data breach in a controlled environment, which will assist your incident response team and other key parties identify gaps in current processes.

Training and Awareness

We offer online cyber security training and phishing simulations so your staff can learn how to identify potential cyber risks and avoid becoming victims of a cyber-attack.

RESPOND

Incident Controllers

We have extensive experience in managing incidents and will guide you through all stages of a data breach, either at your site or from our dedicated incident response control room.

Forensic Technology Experts

Our forensic technology experts are experienced in responding to data breaches in situations such as business email compromise and ransomware.

Specialist Data Breach Software

We use advanced forensic software to examine the source of the compromise and the extent that confidential information has been breached, including PII.

RECOVER

Mandatory Notifications

Our notification services are compliant with the NZ Privacy Act 2020 via either a third party email tool, a tailored website, postal mail, or our contracted call centre.

Ongoing Monitoring

We use leading technology to search the 'Dark Web' for credential compromises, the Open Web and Social Media for your 'Brand Reputation', as well as Credit Monitoring.

Reliable Resources

Subscribe to our Alerts and Bulletins and view our resources to keep up to date with the latest threats in order to reduce your cyber risk.

Thank you

Campbell McKenzie

0800 WITNESS
campbell@incidentresponse.co.nz
incidentresponse.co.nz

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

Incident
Response
FORENSIC & CYBER