

Forensic Technology

Aotea Security
March 2021



Agenda

1. Electronic Evidence - what is it and how can it help you?
2. A walk through of the forensic technology process
3. Cyber security considerations

What is Electronic Evidence

- Electronic evidence includes any data that may be located on a wide range of storage locations. e.g servers, personal computers, laptops, mobile devices, cloud repositories etc
- Electronic evidence is unique as it:
 - Can be distributed across physical and jurisdictional locations
 - Is volatile and can be easily altered, overwritten, damaged or permanently destroyed by a single keystroke or mouse click
 - Can be copied without degradation
 - May not be 'readily retrievable' if the necessary hardware and software is not preserved.


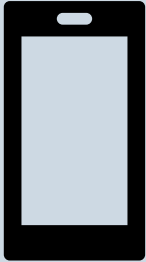


What is Forensic Technology

- A branch of forensic science that focuses on identifying, acquiring, processing, analysing and reporting on electronic data.
- Involves the handling of data for the purpose of legal proceedings.
- All processes must utilise sound forensic techniques to ensure that the findings are admissible in court.

Acquisition

- Preserve the integrity of the electronic evidence
- Identical copy without changing the content of the electronic evidence
- Creates a hash value to prove that the copy is sound
- Analysis typically performed on the copy

Acquisition

Computer	Mobile	Cloud	Warrant Return
			

Expert Witness and Professional Obligations

- 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

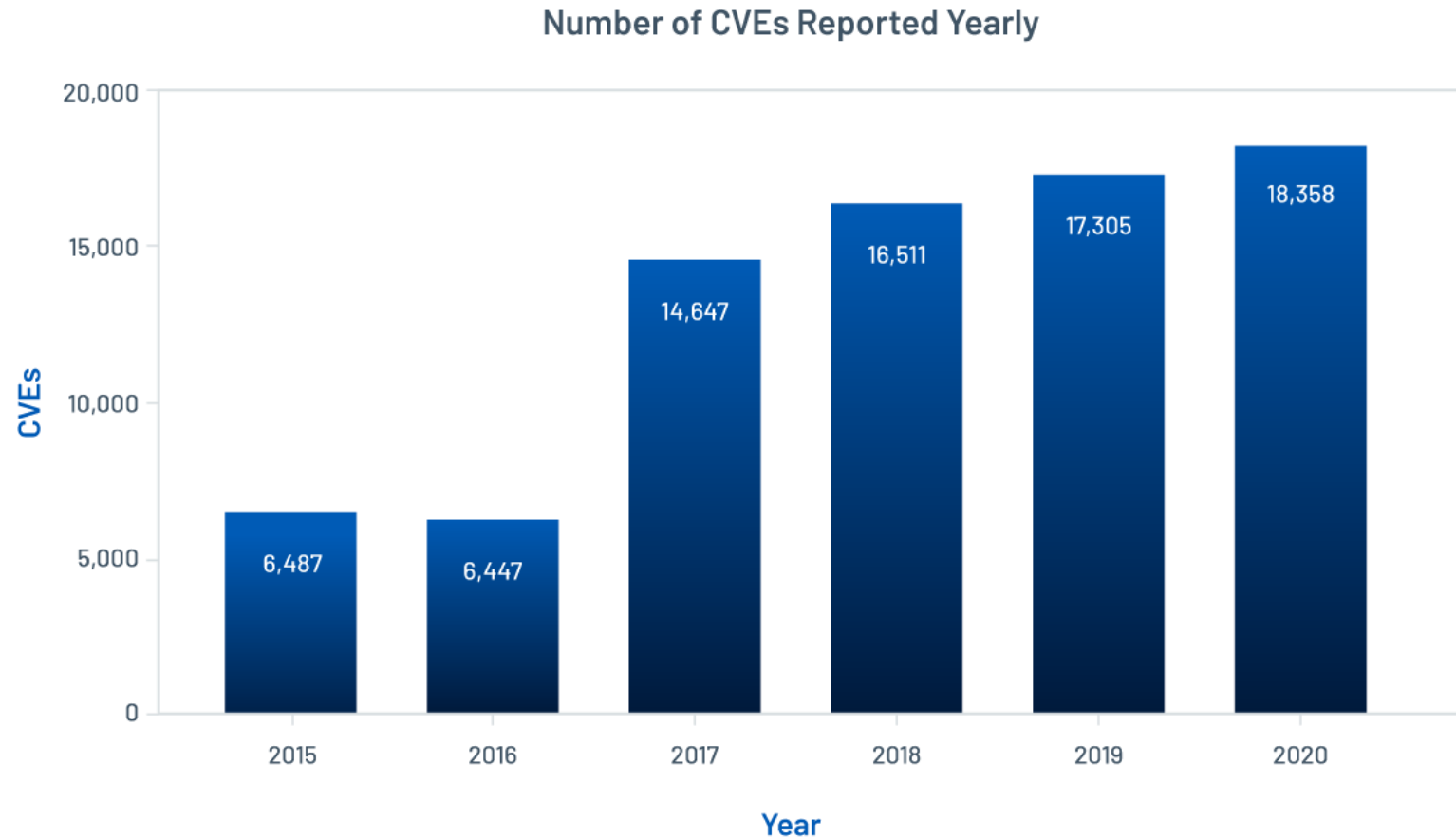
Incident Response Solutions Limited is licenced by the Ministry of Justice as Private Investigators, licence number: 20-072755.



Cyber Landscape



Landscape - Vulnerabilities



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%).

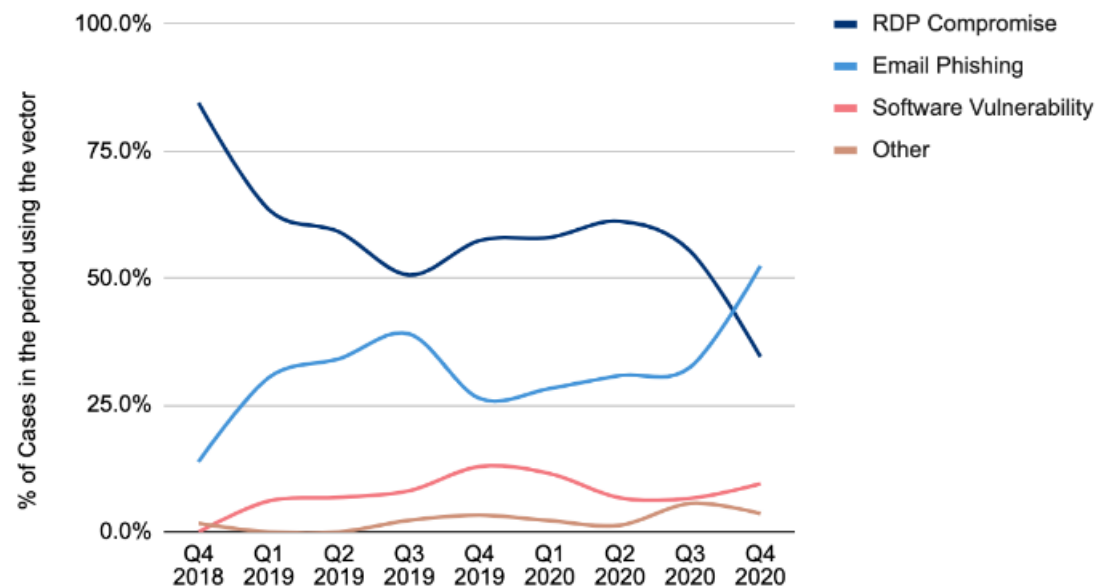
Landscape - Data Breach



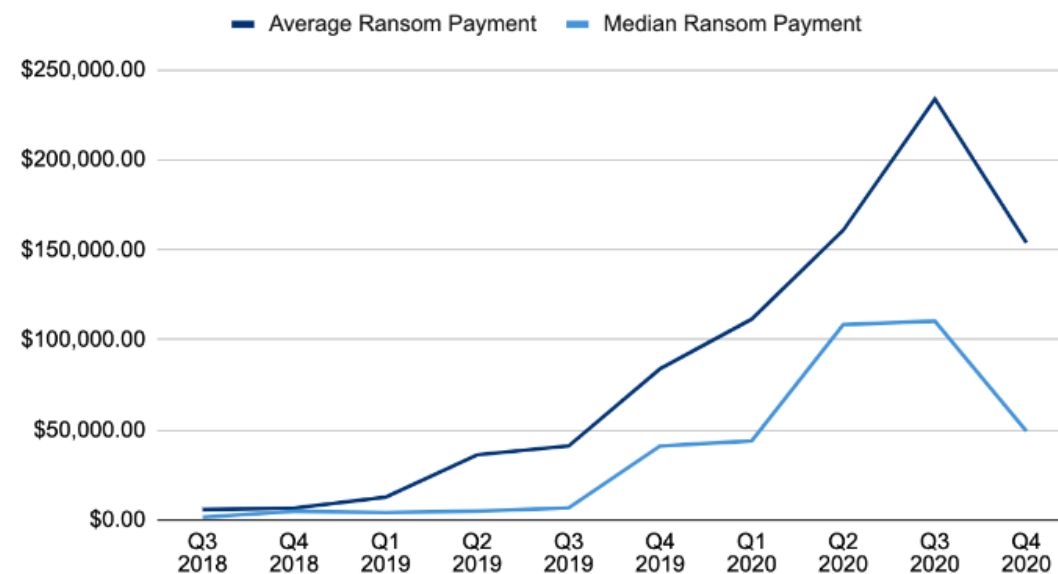
Source - <https://www.ibm.com/security/digital-assets/cost-data-breach-report>

Landscape - Ransomware

Ransomware Attack Vectors



Ransom Payments By Quarter



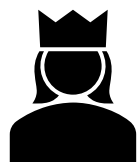
Privacy Act 2020

- 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.



Cyber Framework and Controls



NIST CSF Framework



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



Case Studies and Questions



Case Study 1

249 Accessing computer system for dishonest purpose

- (1) Every one is liable to imprisonment for a term not exceeding 7 years who, directly or indirectly, accesses any computer system and thereby, dishonestly or by deception, and without claim of right,—
 - (a) obtains any property, privilege, service, pecuniary advantage, benefit, or valuable consideration; or
 - (b) causes loss to any other person.
- (2) Every one is liable to imprisonment for a term not exceeding 5 years who, directly or indirectly, accesses any computer system with intent, dishonestly or by deception, and without claim of right,—
 - (a) to obtain any property, privilege, service, pecuniary advantage, benefit, or valuable consideration; or
 - (b) to cause loss to any other person.
- (3) In this section, **deception** has the same meaning as in [section 240\(2\)](#).

Section 249: replaced, on 1 October 2003, by [section 15](#) of the Crimes Amendment Act 2003 (2003 No 39).

Case Study 2

250 Damaging or interfering with computer system

- (1) Every one is liable to imprisonment for a term not exceeding 10 years who intentionally or recklessly destroys, damages, or alters any computer system if he or she knows or ought to know that danger to life is likely to result.
- (2) Every one is liable to imprisonment for a term not exceeding 7 years who intentionally or recklessly, and without authorisation, knowing that he or she is not authorised, or being reckless as to whether or not he or she is authorised,—
 - (a) damages, deletes, modifies, or otherwise interferes with or impairs any data or software in any computer system; or
 - (b) causes any data or software in any computer system to be damaged, deleted, modified, or otherwise interfered with or impaired; or
 - (c) causes any computer system to—
 - (i) fail; or
 - (ii) deny service to any authorised users.

Section 250: replaced, on 1 October 2003, by [section 15](#) of the Crimes Amendment Act 2003 (2003 No 39).

Thank you

Campbell McKenzie

0800 WITNESS or 021 779 310

campbell@incidentresponse.co.nz

incidentresponse.co.nz

whistleblowers.co.nz

