Emerging risks in 2023: How to protect your data and employee disclosures

CAANZ

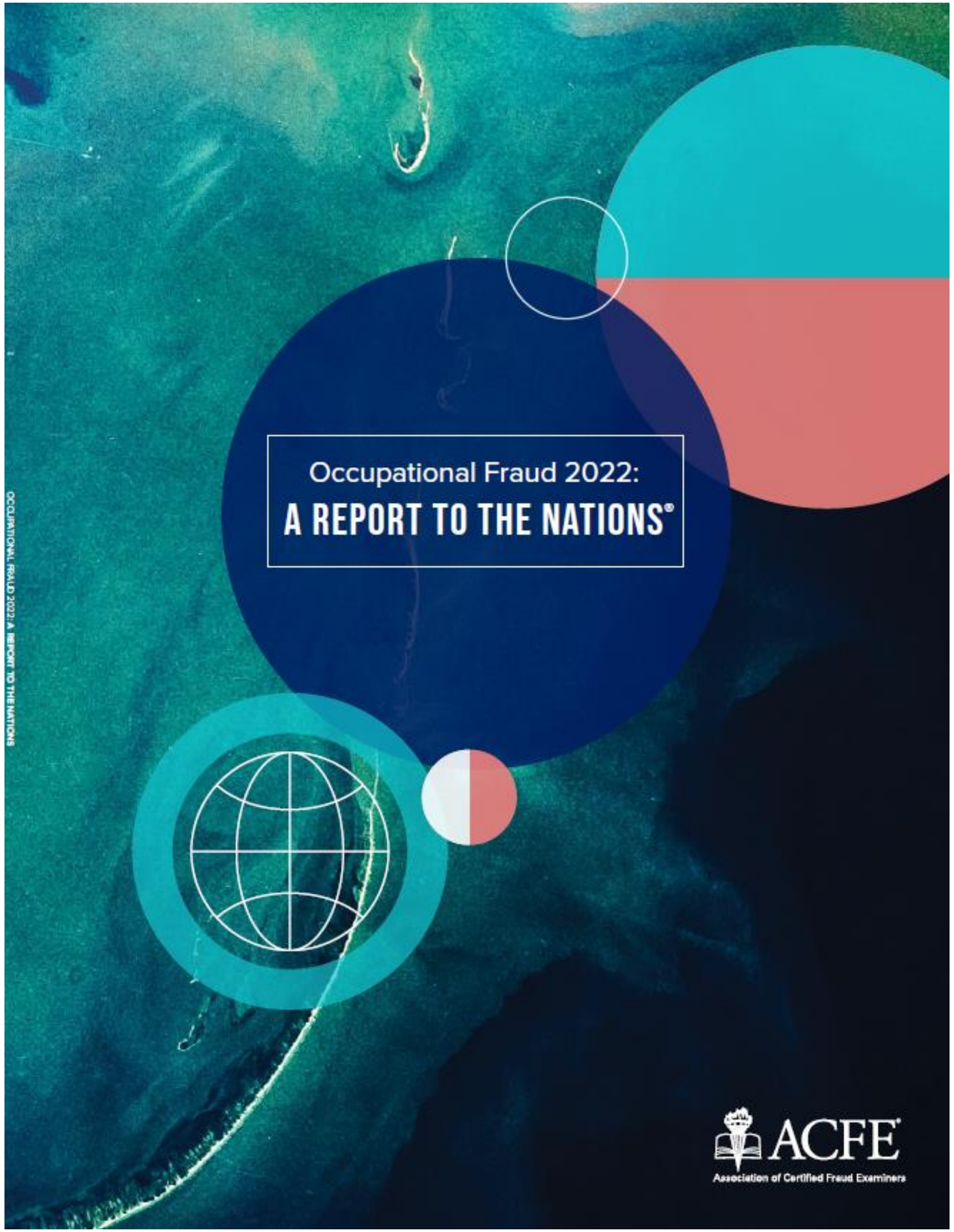
Focus on Management

November 2022

Incident Response

FORENSIC & CYBER

Whistleblower Update



Occupational Fraud 2022:

A REPORT TO THE NATIONS®

ACFE®

Association of Certified Fraud Examiners

OCCUPATIONAL FRAUD 2022: A REPORT TO THE NATIONS

This research provides valuable information about the:

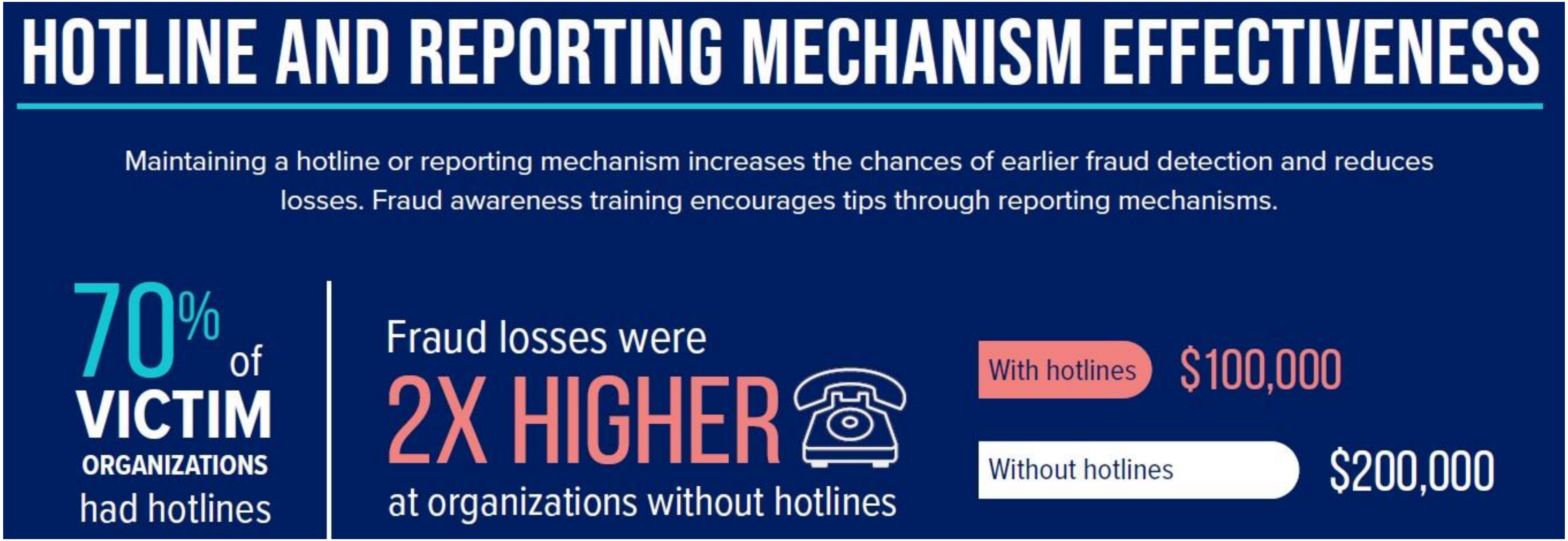
- costs
- methods
- perpetrators
- outcomes

of occupational fraud schemes derived from more than:

- 2,000 real cases of fraud
- 133 countries
- 23 industries

> *“A person who informs on a person or organisation engaged in an illicit activity”*

- The Oxford Dictionary



HOTLINE AND REPORTING MECHANISM EFFECTIVENESS

Maintaining a hotline or reporting mechanism increases the chances of earlier fraud detection and reduces losses. Fraud awareness training encourages tips through reporting mechanisms.

70% of **VICTIM ORGANIZATIONS** had hotlines

Fraud losses were **2X HIGHER** ☎ at organizations without hotlines

With hotlines	$100,000
Without hotlines	$200,000

42% of frauds were detected by tips,

which is nearly **3x** as many cases as the next most common method

More than **HALF** of all tips came from employees

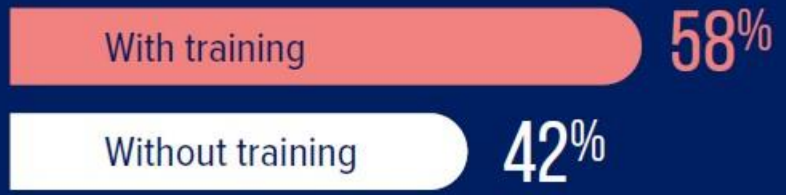
EFFECT OF EMPLOYEE AND MANAGER FRAUD AWARENESS TRAINING ON HOTLINES AND REPORTING

TRAINING INCREASES the likelihood of detection by tip

45% of cases detected by tip with training

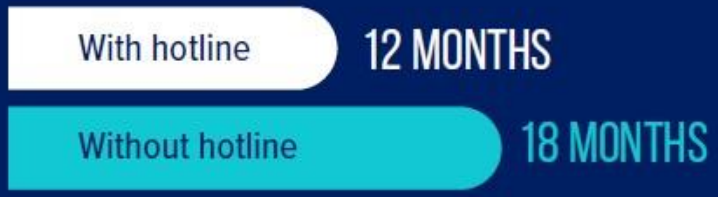
37% of cases detected by tip without training

Reports of fraud are **MORE LIKELY TO BE SUBMITTED** through hotlines with training

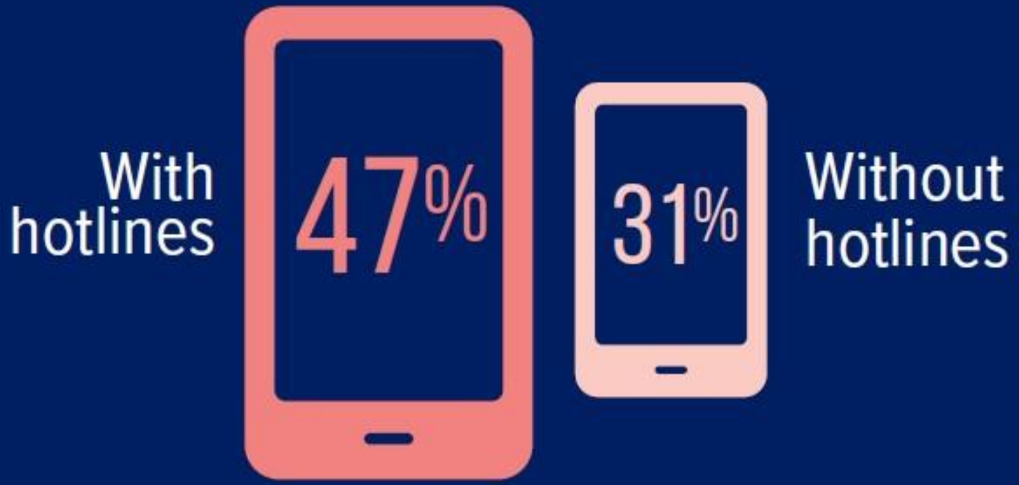


Percent of tips made through hotline

Organizations with hotlines detect frauds **MORE QUICKLY**



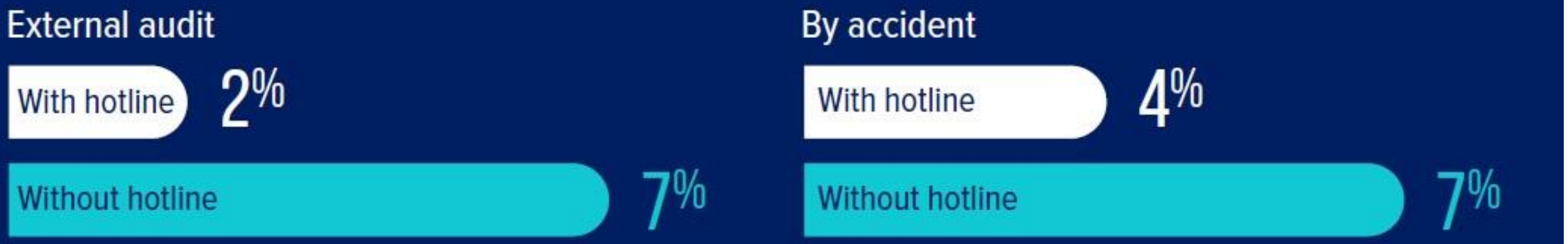
Organizations with hotlines are more likely to detect fraud **BY TIP**



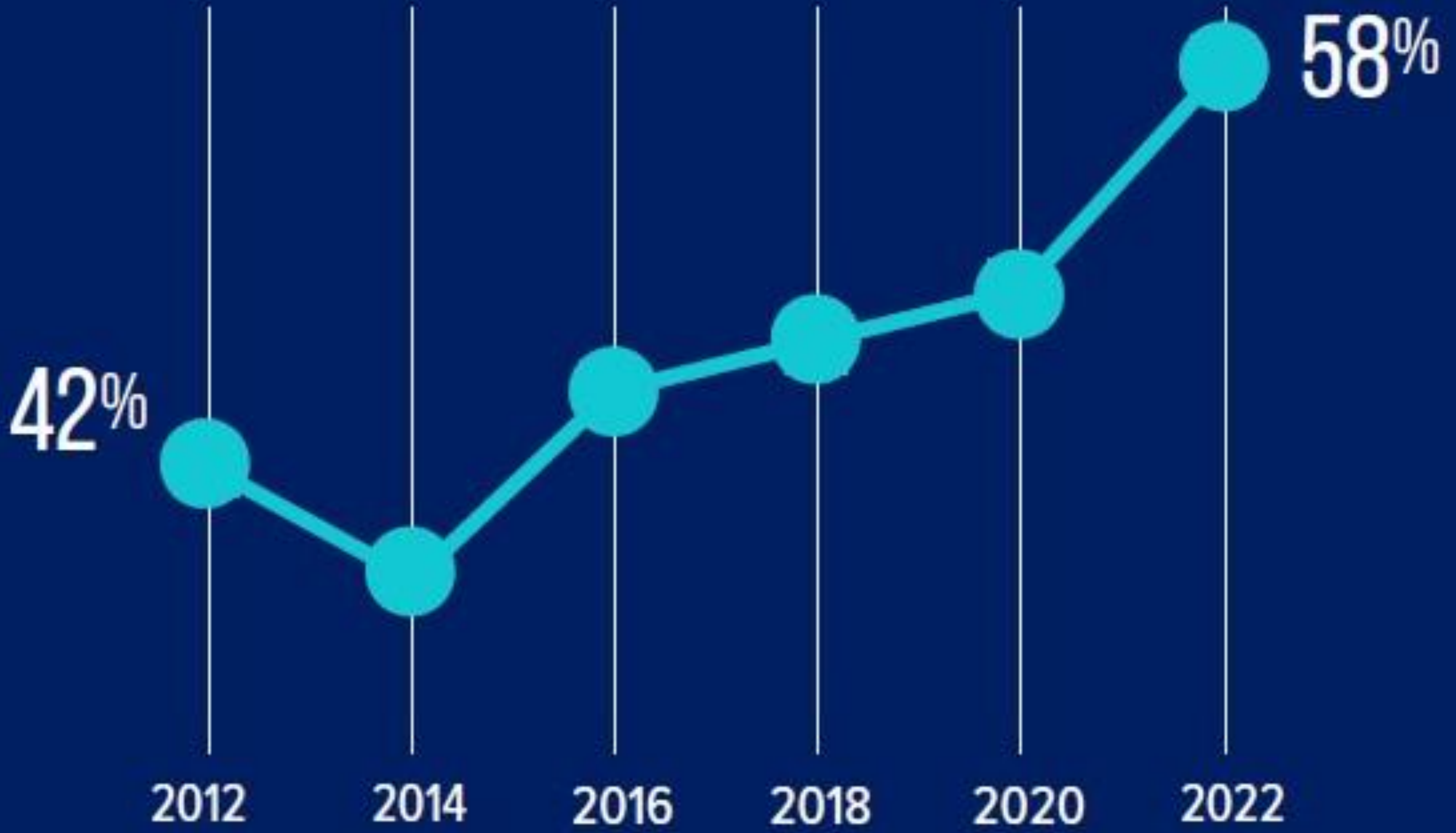
Percent of cases detected by tip

ORGANIZATIONS WITHOUT HOTLINES ARE 3.5X MORE LIKELY

to discover fraud through an external audit and nearly 2X more likely by accident

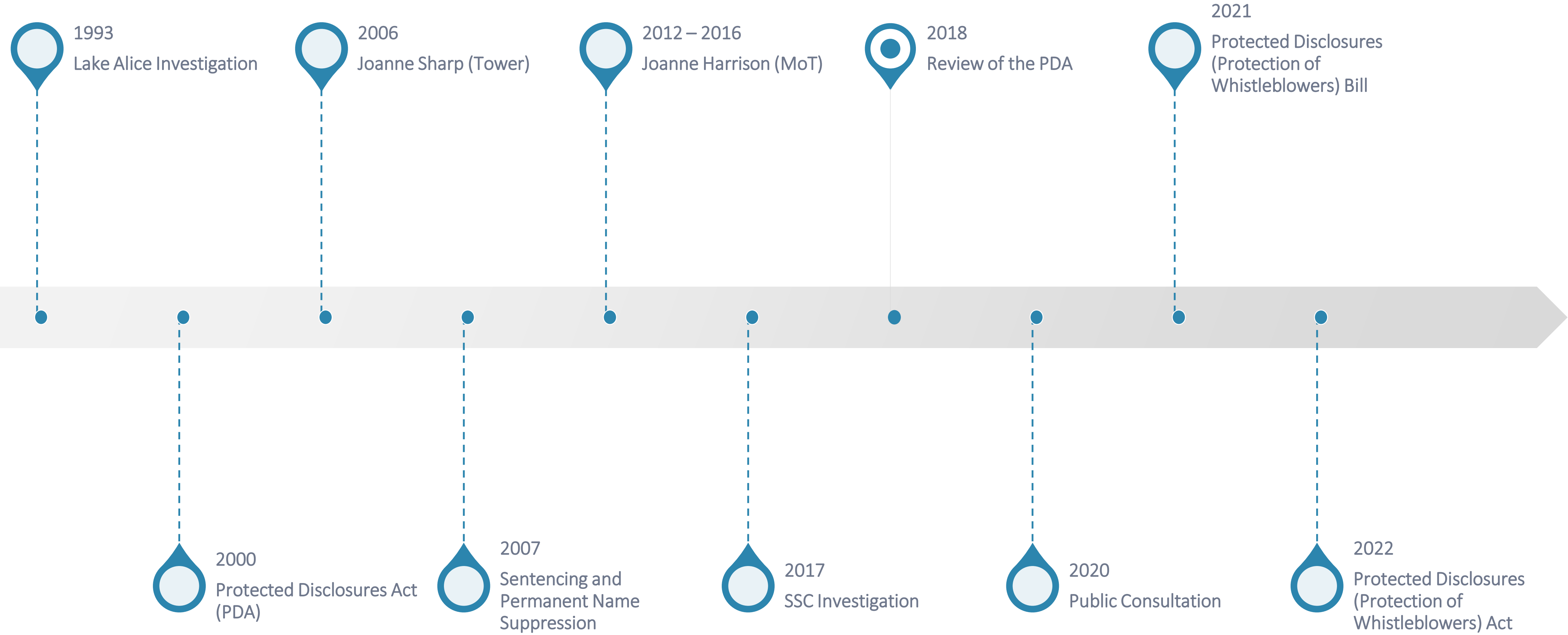


Since 2012, the percent of tips made through hotlines has **INCREASED DRAMATICALLY**



The Protected Disclosures (Protection of Whistleblowers) Act 2022 Timeline

Protected Disclosures (Protection of Whistleblowers) Act 2022



1993
Lake Alice Investigation

2000
Protected Disclosures Act (PDA)

2006
Joanne Sharp (Tower)

2007
Sentencing and Permanent Name Suppression

2012 – 2016
Joanne Harrison (MoT)

2017
SSC Investigation

2018
Review of the PDA

2020
Public Consultation

2021
Protected Disclosures (Protection of Whistleblowers) Bill

2022
Protected Disclosures (Protection of Whistleblowers) Act

Improvements from previous Act

Protected Disclosures (Protection of Whistleblowers) Act
2022

The 2022 Act addresses the following issues and improvements from the 2000 Act:

- extending serious wrongdoing to cover private sector use of public funds and behaviour that is a serious risk to the health and safety of any individual
- allowing people to report serious wrongdoing directly to an appropriate authority
- strengthening protections by specifying what a receiver of a disclosure should do
- clarifying internal procedure requirements for public sector organisations and requiring them to state how they will provide support to disclosers
- clarifying the potential forms of adverse conduct disclosers may face.

What is a protected disclosure?

Protected Disclosures (Protection of Whistleblowers) Act
2022

A protected disclosure is when the discloser:

- believes on reasonable grounds that there is, or has been, serious wrongdoing in or by the discloser’s organisation, and
- discloses information about that in accordance with the Act, and
- does not disclose it in bad faith.

Who is a discloser?

Protected Disclosures (Protection of Whistleblowers) Act
2022

A discloser, in relation to an organisation, means an individual who is (or was formerly):

- an employee
- a homeworker within the meaning given in section 5 of the Employment Relations Act 2000
- a secondee to the organisation
- engaged or contracted under a contract for services to do work for the organisation
- concerned in the management of the organisation (including, for example, a person who is or was a member of the board or governing body of the organisation)
- a member of the Armed Forces (in relation to the New Zealand Defence Force)
- a volunteer working for the organisation without reward or expectation of reward for that work.

What constitutes a protected disclosure?

Protected Disclosures (Protection of Whistleblowers) Act 2022

Serious wrongdoing includes an act, omission or course of conduct that is:

- An offence
- A serious risk to public health, or public safety, or the health or safety of any individual, or to the environment
- A serious risk to the maintenance of the law including the prevention, investigation and detection of offences or the right to a fair trial
- An unlawful, corrupt or irregular use of public funds or public resources
- Oppressive, unlawfully discriminatory, or grossly negligent or that is gross mismanagement by a public sector employee or a person performing a function or duty or exercising a power on behalf of a public sector organisation or the Government.

What must public and private sector organisations do as the receiver of a protected disclosure? (Guidance Only)

Protected Disclosures (Protection of Whistleblowers) Act 2022

Within 20 working days of receiving a protected disclosure, the receiver should acknowledge to the discloser the receipt of the disclosure, consider whether it warrants investigation, and deal with the matter by doing one or more of:

- investigating the disclosure
- addressing any serious wrongdoing by acting or recommending action
- referring the disclosure to an (or another) appropriate authority
- deciding that no action is required.

The receiver should then inform the discloser about what they have done or are doing to deal with the matter. If the receiver is unable to complete these actions within 20 working days, they should begin the process and inform the discloser how long it may take.

What you should look for in a Whistleblower Service

Independent

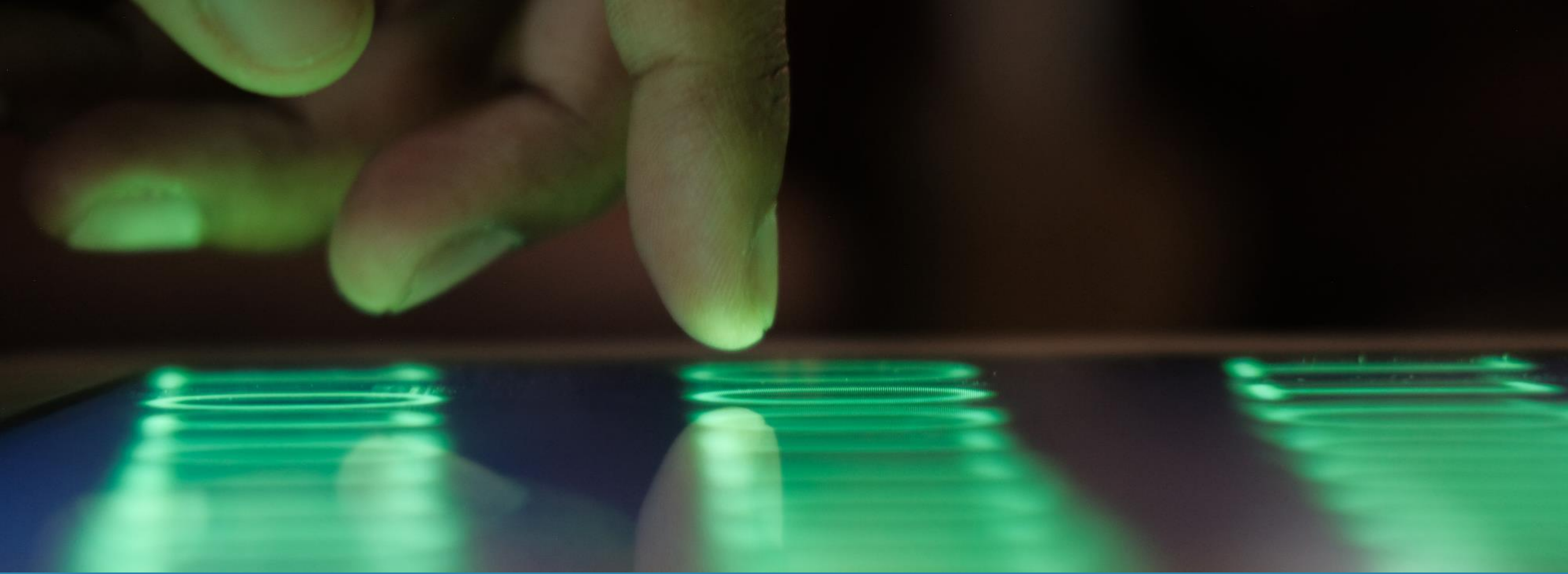
Multiple disclosure channels

Confidentiality and anonymity

24/7

Expertise

Incident Response
WHISTLEBLOWERS



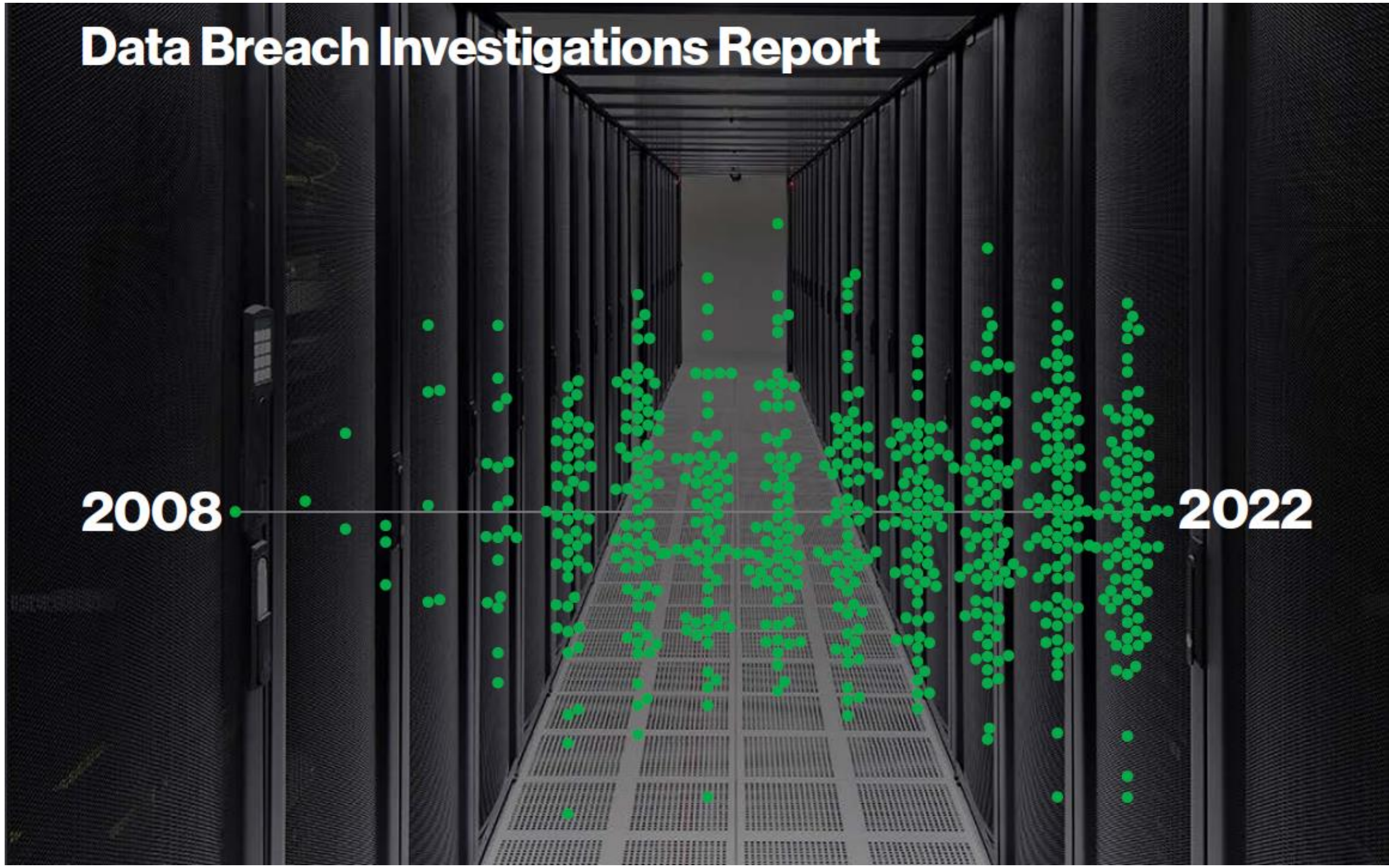
Cyber Update

Verizon Data Breach Investigations Report (15th Edition)

- The DBIR was created to provide a place for security practitioners to look for data-driven, real-world views on cybercrime.
- This data informs us of the steps we should take to protect ourselves.
- The report is used to increase awareness of the tactics attackers are likely to use against organisations in your industry.
- It is also used as a tool to encourage executives to support security initiatives and illustrate to employees the importance of security and how they can help.

Verizon Data Breach Investigations Report (15th Edition)

- 23,896 security incidents that compromised the integrity, confidentiality or availability of an information asset.
- 5,212 breaches that resulted in the confirmed disclosure of data to an unauthorised party.

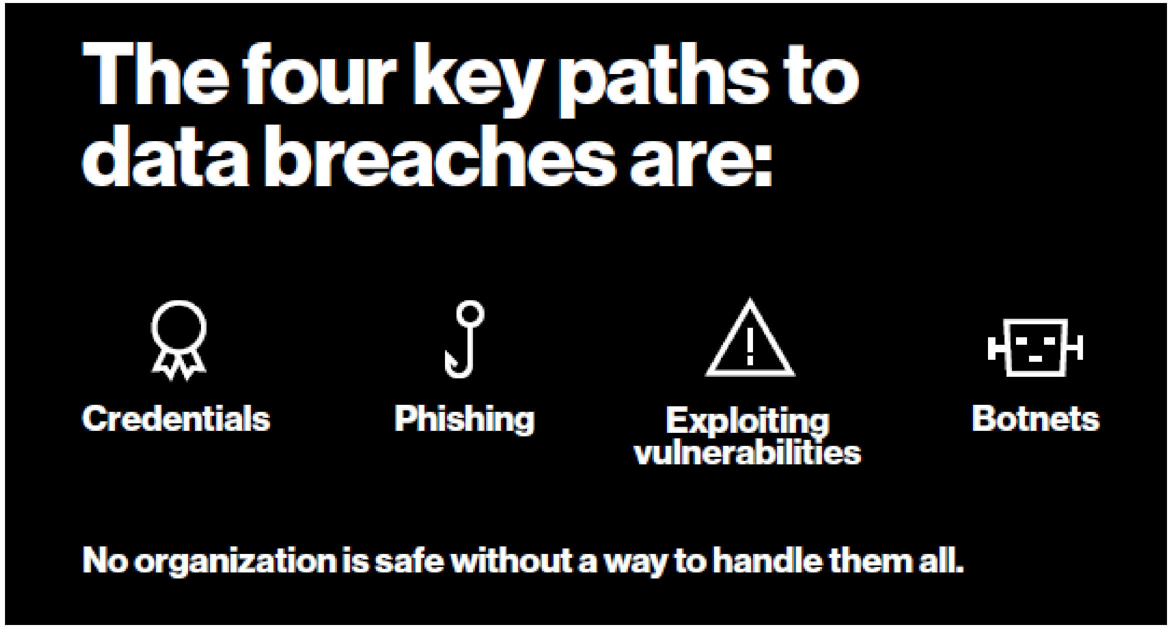


https://www.verizon.com/business/resources/reports/dbir

What Verizon Found – Key Statistics

- 82% of breaches involved a human element.
- Over half of breaches involved the use of either remote access or web applications.
- Partners accounted for 62% of System Intrusion incidents, although this was mostly due to single supply chain breaches.
- About two-thirds of breaches involved Phishing, Stolen credentials and/or Ransomware.
- 95% had five or fewer steps. Phishing, Downloader, Ransomware.

What Verizon Found – Key Statistics



The four key paths to data breaches are:

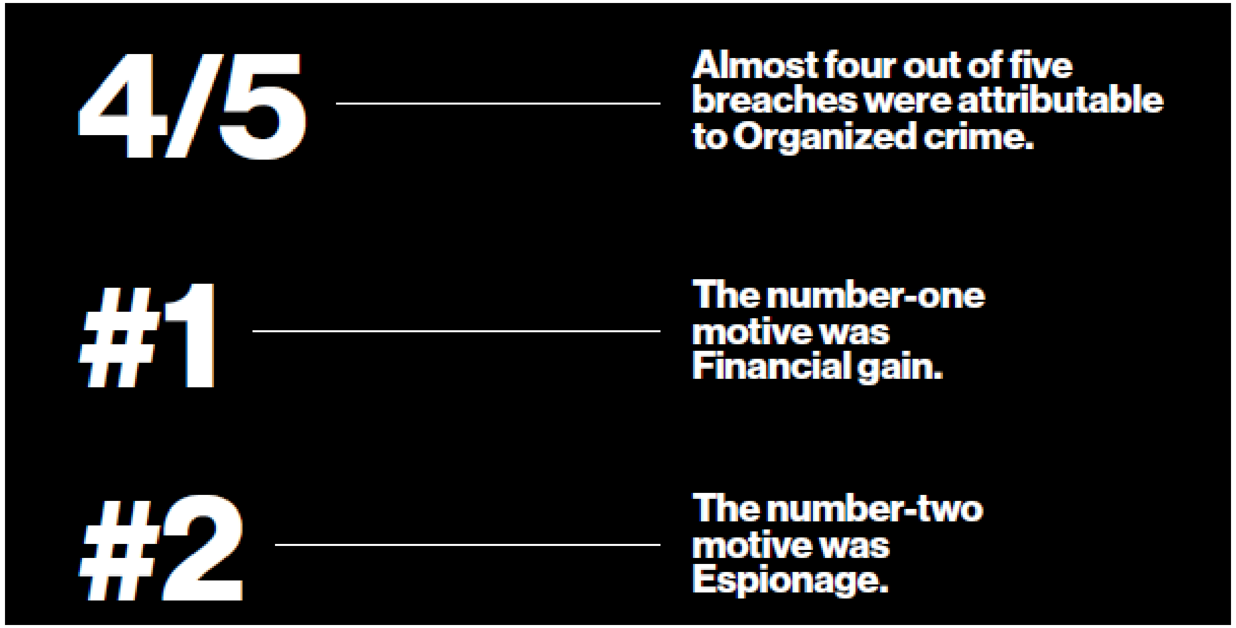
Credentials

Phishing

Exploiting vulnerabilities

Botnets

No organization is safe without a way to handle them all.

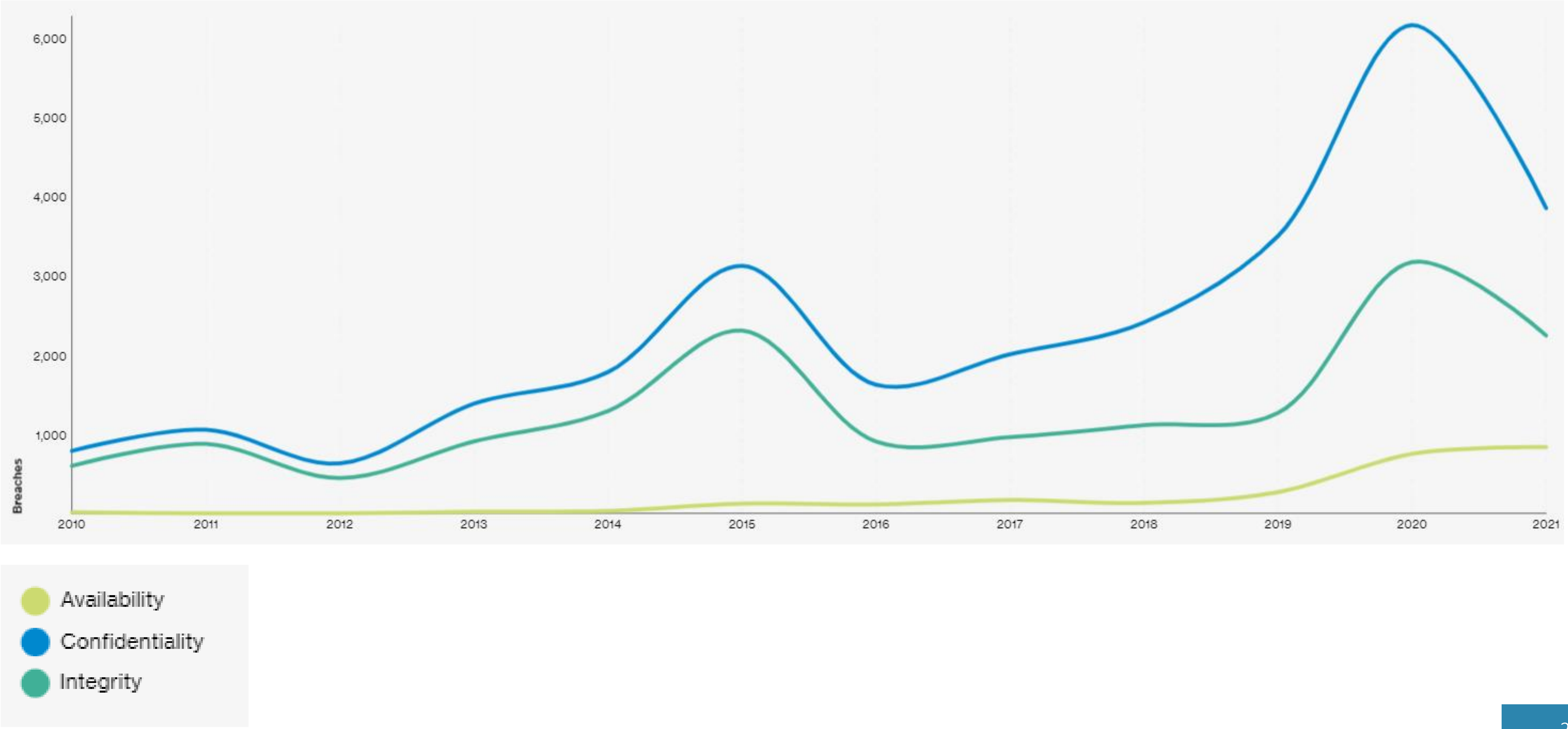


4/5 — Almost four out of five breaches were attributable to Organized crime.

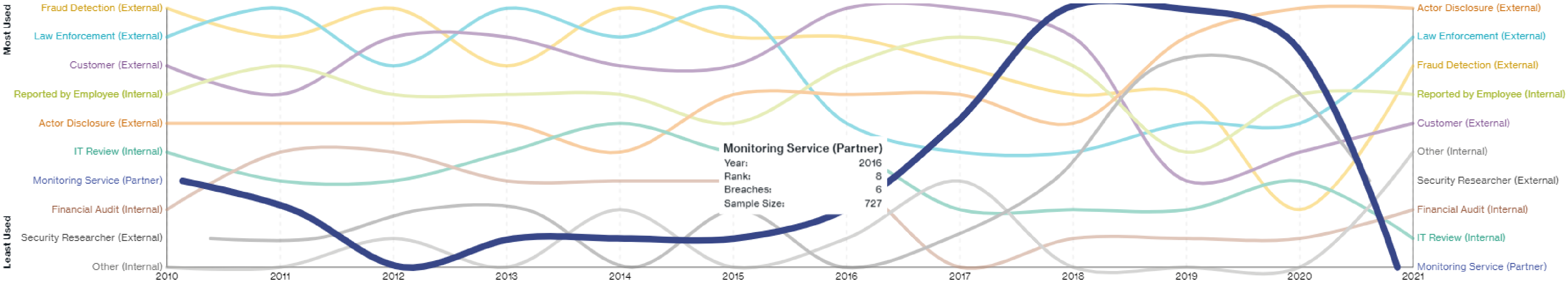
#1 — The number-one motive was Financial gain.

#2 — The number-two motive was Espionage.

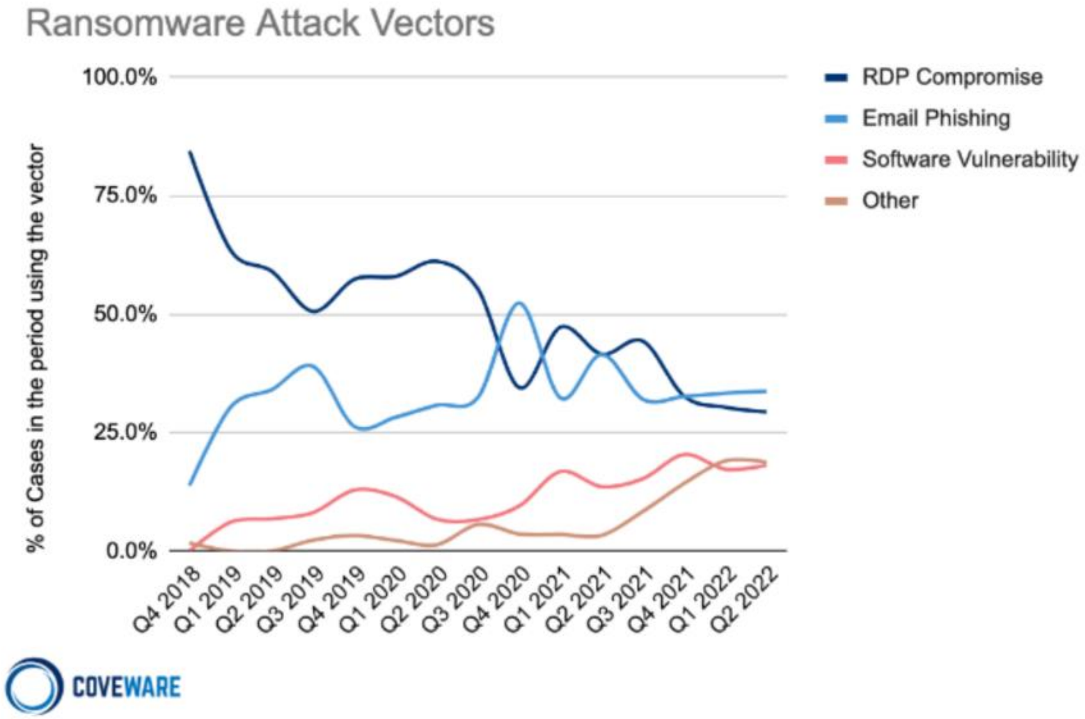
What Verizon Found - Breach Trends

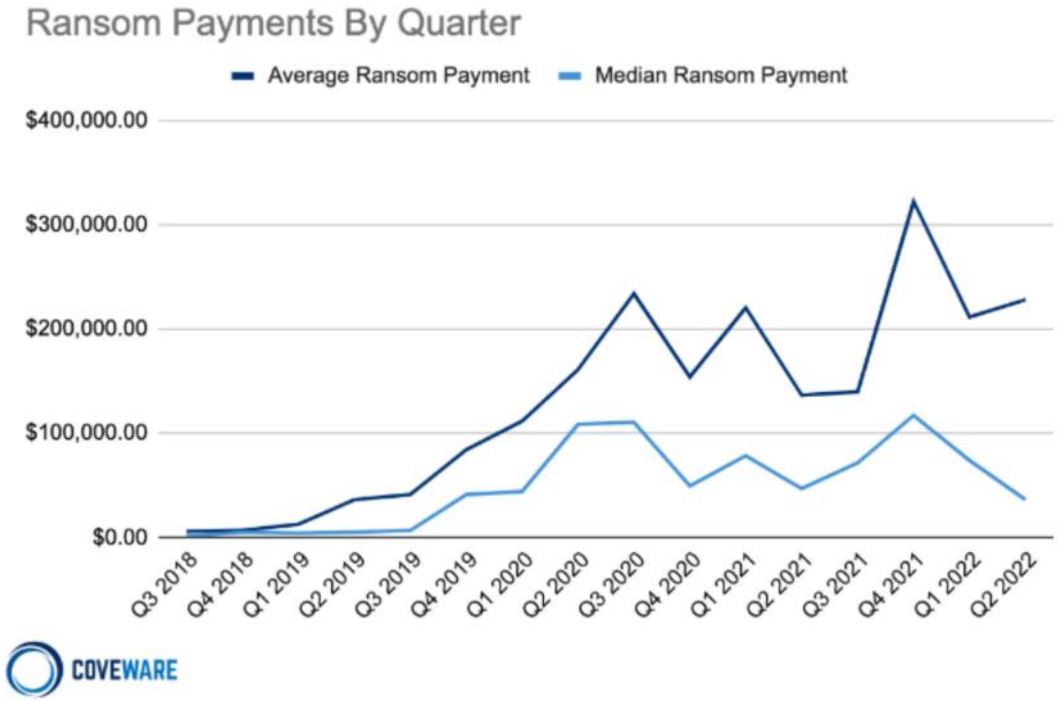


What Verizon Found - Discovery Methods Used Over Time



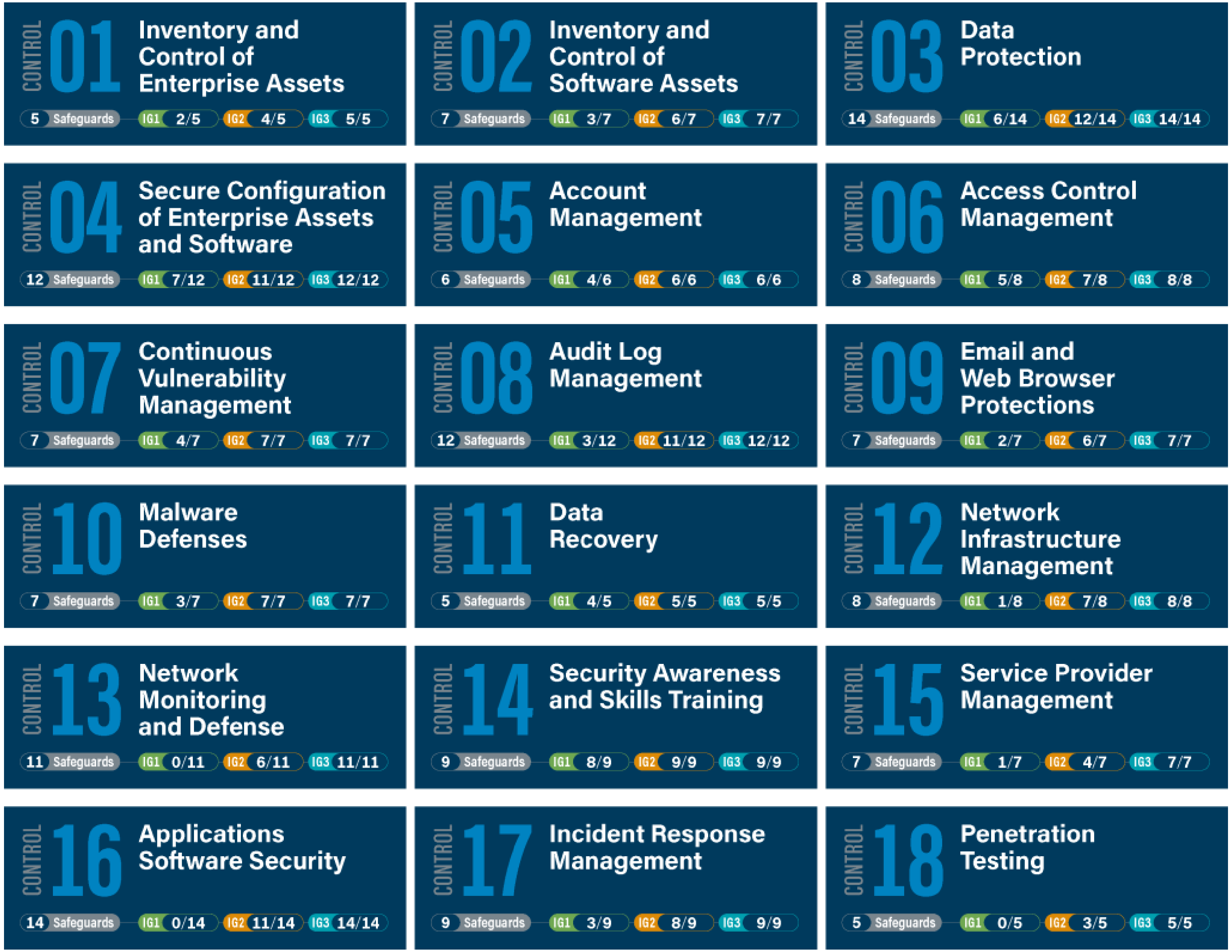
Ransomware Update





https://www.coveware.com/blog/2022/7/27/fewer-ransomware-victims-pay-as-medium-ransom-falls-in-q2-2022

CIS Controls



CONTROL 01 Inventory and Control of Enterprise Assets
5 Safeguards IG1 2/5 IG2 4/5 IG3 5/5

CONTROL 02 Inventory and Control of Software Assets
7 Safeguards IG1 3/7 IG2 6/7 IG3 7/7

CONTROL 03 Data Protection
14 Safeguards IG1 6/14 IG2 12/14 IG3 14/14

CONTROL 04 Secure Configuration of Enterprise Assets and Software
12 Safeguards IG1 7/12 IG2 11/12 IG3 12/12

CONTROL 05 Account Management
6 Safeguards IG1 4/6 IG2 6/6 IG3 6/6

CONTROL 06 Access Control Management
8 Safeguards IG1 5/8 IG2 7/8 IG3 8/8

CONTROL 07 Continuous Vulnerability Management
7 Safeguards IG1 4/7 IG2 7/7 IG3 7/7

CONTROL 08 Audit Log Management
12 Safeguards IG1 3/12 IG2 11/12 IG3 12/12

CONTROL 09 Email and Web Browser Protections
7 Safeguards IG1 2/7 IG2 6/7 IG3 7/7

CONTROL 10 Malware Defenses
7 Safeguards IG1 3/7 IG2 7/7 IG3 7/7

CONTROL 11 Data Recovery
5 Safeguards IG1 4/5 IG2 5/5 IG3 5/5

CONTROL 12 Network Infrastructure Management
8 Safeguards IG1 1/8 IG2 7/8 IG3 8/8

CONTROL 13 Network Monitoring and Defense
11 Safeguards IG1 0/11 IG2 6/11 IG3 11/11

CONTROL 14 Security Awareness and Skills Training
9 Safeguards IG1 8/9 IG2 9/9 IG3 9/9

CONTROL 15 Service Provider Management
7 Safeguards IG1 1/7 IG2 4/7 IG3 7/7

CONTROL 16 Applications Software Security
14 Safeguards IG1 0/14 IG2 11/14 IG3 14/14

CONTROL 17 Incident Response Management
9 Safeguards IG1 3/9 IG2 8/9 IG3 9/9

CONTROL 18 Penetration Testing
5 Safeguards IG1 0/5 IG2 3/5 IG3 5/5

CIS Controls

IG1 is the definition of basic cyber hygiene and represents a minimum standard of information security for all enterprises. IG1 assists enterprises with limited cybersecurity expertise thwart general, non-targeted attacks.

56
Cyber defense Safeguards

IG2 assists enterprises managing IT infrastructure of multiple departments with differing risk profiles. IG2 aims to help enterprises cope with increased operational complexity.

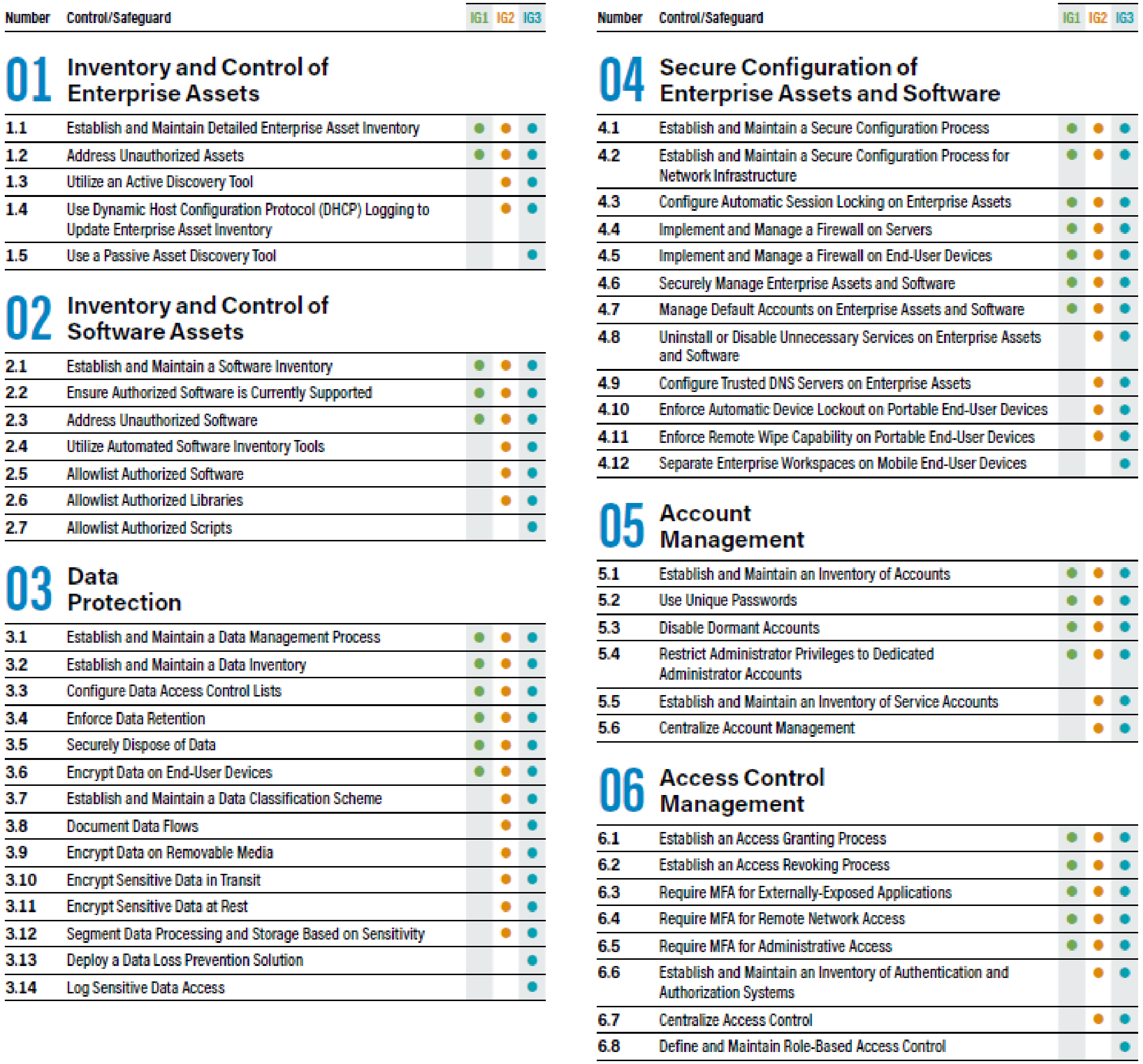
74
Additional cyber defense Safeguards

IG3 assists enterprises with IT security experts secure sensitive and confidential data. IG3 aims to prevent and/or lessen the impact of sophisticated attacks.

23
Additional cyber defense Safeguards

Total Safeguards 153

CIS Controls



01 Inventory and Control of Enterprise Assets

Number	Control/Safeguard	IG1	IG2	IG3
1.1	Establish and Maintain Detailed Enterprise Asset Inventory	●	●	●
1.2	Address Unauthorized Assets	●	●	●
1.3	Utilize an Active Discovery Tool		●	●
1.4	Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory		●	●
1.5	Use a Passive Asset Discovery Tool			●

02 Inventory and Control of Software Assets

Number	Control/Safeguard	IG1	IG2	IG3
2.1	Establish and Maintain a Software Inventory	●	●	●
2.2	Ensure Authorized Software is Currently Supported	●	●	●
2.3	Address Unauthorized Software	●	●	●
2.4	Utilize Automated Software Inventory Tools		●	●
2.5	Allowlist Authorized Software		●	●
2.6	Allowlist Authorized Libraries		●	●
2.7	Allowlist Authorized Scripts			●

03 Data Protection

Number	Control/Safeguard	IG1	IG2	IG3
3.1	Establish and Maintain a Data Management Process	●	●	●
3.2	Establish and Maintain a Data Inventory	●	●	●
3.3	Configure Data Access Control Lists	●	●	●
3.4	Enforce Data Retention	●	●	●
3.5	Securely Dispose of Data	●	●	●
3.6	Encrypt Data on End-User Devices	●	●	●
3.7	Establish and Maintain a Data Classification Scheme		●	●
3.8	Document Data Flows		●	●
3.9	Encrypt Data on Removable Media		●	●
3.10	Encrypt Sensitive Data in Transit		●	●
3.11	Encrypt Sensitive Data at Rest		●	●
3.12	Segment Data Processing and Storage Based on Sensitivity		●	●
3.13	Deploy a Data Loss Prevention Solution			●
3.14	Log Sensitive Data Access			●

04 Secure Configuration of Enterprise Assets and Software

Number	Control/Safeguard	IG1	IG2	IG3
4.1	Establish and Maintain a Secure Configuration Process	●	●	●
4.2	Establish and Maintain a Secure Configuration Process for Network Infrastructure	●	●	●
4.3	Configure Automatic Session Locking on Enterprise Assets	●	●	●
4.4	Implement and Manage a Firewall on Servers	●	●	●
4.5	Implement and Manage a Firewall on End-User Devices	●	●	●
4.6	Securely Manage Enterprise Assets and Software	●	●	●
4.7	Manage Default Accounts on Enterprise Assets and Software	●	●	●
4.8	Uninstall or Disable Unnecessary Services on Enterprise Assets and Software		●	●
4.9	Configure Trusted DNS Servers on Enterprise Assets		●	●
4.10	Enforce Automatic Device Lockout on Portable End-User Devices		●	●
4.11	Enforce Remote Wipe Capability on Portable End-User Devices		●	●
4.12	Separate Enterprise Workspaces on Mobile End-User Devices			●

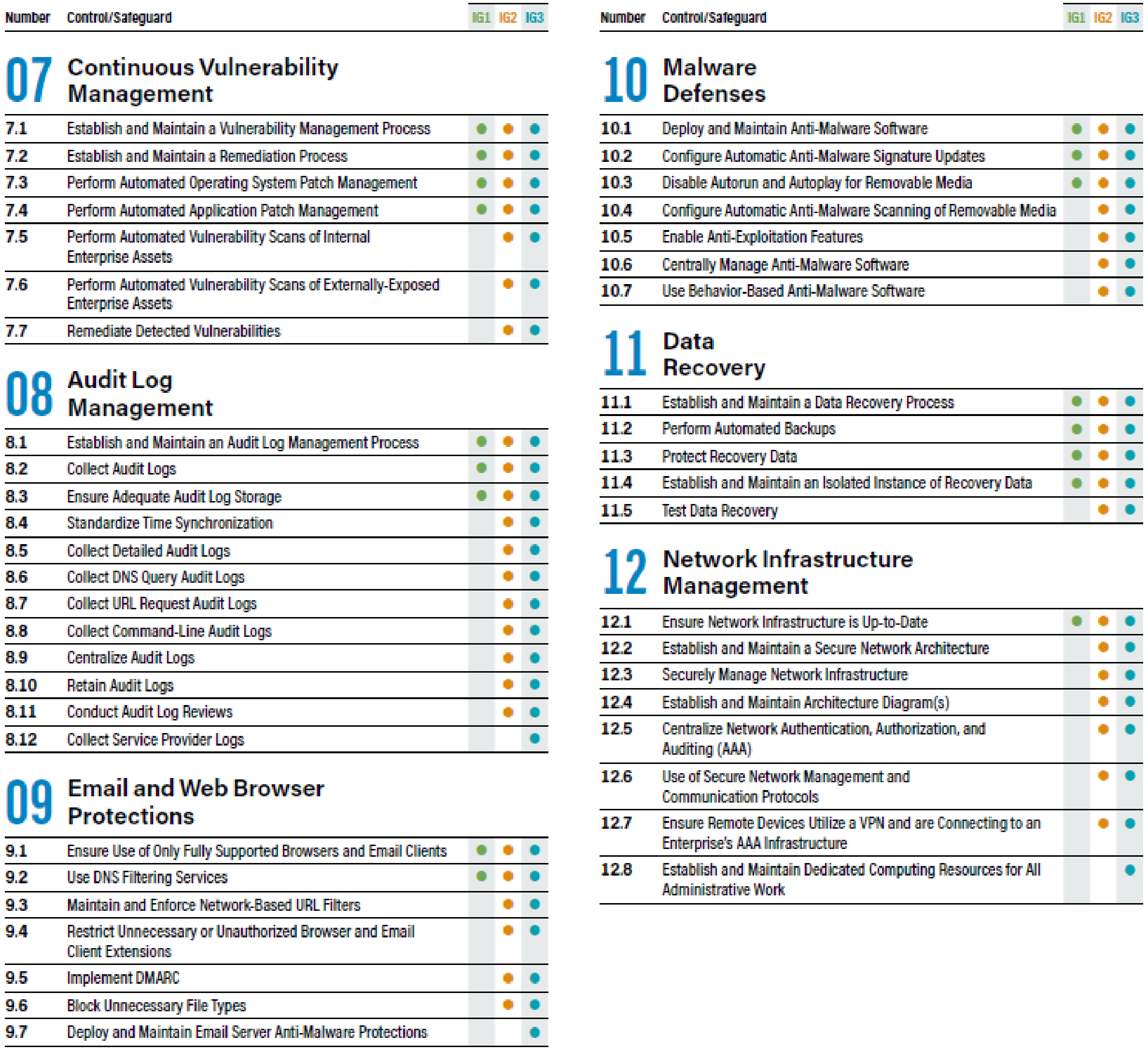
05 Account Management

Number	Control/Safeguard	IG1	IG2	IG3
5.1	Establish and Maintain an Inventory of Accounts	●	●	●
5.2	Use Unique Passwords	●	●	●
5.3	Disable Dormant Accounts	●	●	●
5.4	Restrict Administrator Privileges to Dedicated Administrator Accounts	●	●	●
5.5	Establish and Maintain an Inventory of Service Accounts		●	●
5.6	Centralize Account Management		●	●

06 Access Control Management

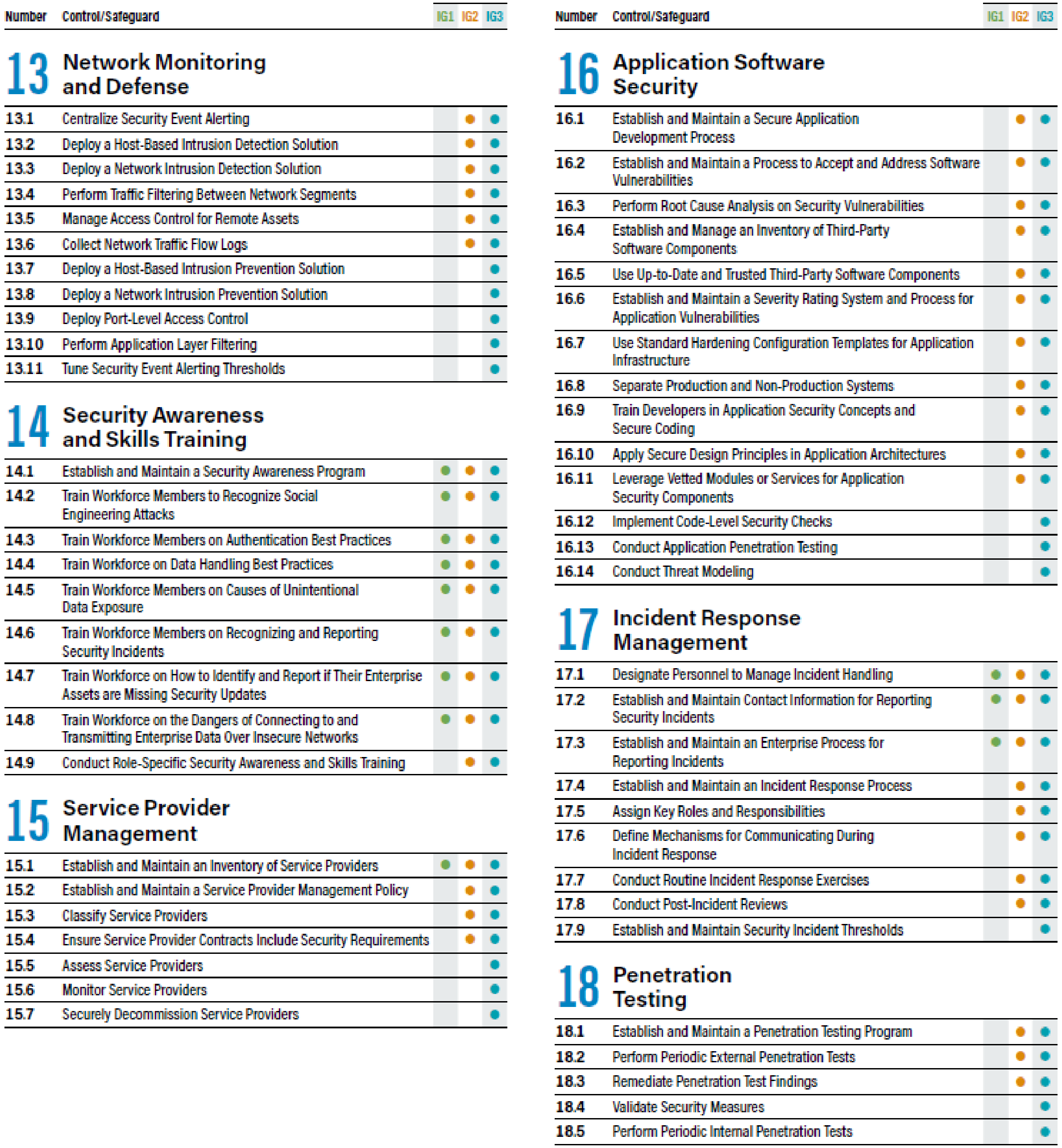
Number	Control/Safeguard	IG1	IG2	IG3
6.1	Establish an Access Granting Process	●	●	●
6.2	Establish an Access Revoking Process	●	●	●
6.3	Require MFA for Externally-Exposed Applications	●	●	●
6.4	Require MFA for Remote Network Access	●	●	●
6.5	Require MFA for Administrative Access	●	●	●
6.6	Establish and Maintain an Inventory of Authentication and Authorization Systems		●	●
6.7	Centralize Access Control		●	●
6.8	Define and Maintain Role-Based Access Control			●

CIS Controls



Number	Control/Safeguard	IG1	IG2	IG3
07	Continuous Vulnerability Management			
7.1	Establish and Maintain a Vulnerability Management Process	●	●	●
7.2	Establish and Maintain a Remediation Process	●	●	●
7.3	Perform Automated Operating System Patch Management	●	●	●
7.4	Perform Automated Application Patch Management	●	●	●
7.5	Perform Automated Vulnerability Scans of Internal Enterprise Assets		●	●
7.6	Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets		●	●
7.7	Remediate Detected Vulnerabilities		●	●
08	Audit Log Management			
8.1	Establish and Maintain an Audit Log Management Process	●	●	●
8.2	Collect Audit Logs	●	●	●
8.3	Ensure Adequate Audit Log Storage	●	●	●
8.4	Standardize Time Synchronization		●	●
8.5	Collect Detailed Audit Logs		●	●
8.6	Collect DNS Query Audit Logs		●	●
8.7	Collect URL Request Audit Logs		●	●
8.8	Collect Command-Line Audit Logs		●	●
8.9	Centralize Audit Logs		●	●
8.10	Retain Audit Logs		●	●
8.11	Conduct Audit Log Reviews		●	●
8.12	Collect Service Provider Logs			●
09	Email and Web Browser Protections			
9.1	Ensure Use of Only Fully Supported Browsers and Email Clients	●	●	●
9.2	Use DNS Filtering Services	●	●	●
9.3	Maintain and Enforce Network-Based URL Filters		●	●
9.4	Restrict Unnecessary or Unauthorized Browser and Email Client Extensions		●	●
9.5	Implement DMARC		●	●
9.6	Block Unnecessary File Types		●	●
9.7	Deploy and Maintain Email Server Anti-Malware Protections			●
10	Malware Defenses			
10.1	Deploy and Maintain Anti-Malware Software	●	●	●
10.2	Configure Automatic Anti-Malware Signature Updates	●	●	●
10.3	Disable Autorun and Autoplay for Removable Media	●	●	●
10.4	Configure Automatic Anti-Malware Scanning of Removable Media		●	●
10.5	Enable Anti-Exploitation Features		●	●
10.6	Centrally Manage Anti-Malware Software		●	●
10.7	Use Behavior-Based Anti-Malware Software		●	●
11	Data Recovery			
11.1	Establish and Maintain a Data Recovery Process	●	●	●
11.2	Perform Automated Backups	●	●	●
11.3	Protect Recovery Data	●	●	●
11.4	Establish and Maintain an Isolated Instance of Recovery Data	●	●	●
11.5	Test Data Recovery		●	●
12	Network Infrastructure Management			
12.1	Ensure Network Infrastructure is Up-to-Date	●	●	●
12.2	Establish and Maintain a Secure Network Architecture		●	●
12.3	Securely Manage Network Infrastructure		●	●
12.4	Establish and Maintain Architecture Diagram(s)		●	●
12.5	Centralize Network Authentication, Authorization, and Auditing (AAA)		●	●
12.6	Use of Secure Network Management and Communication Protocols		●	●
12.7	Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure		●	●
12.8	Establish and Maintain Dedicated Computing Resources for All Administrative Work			●

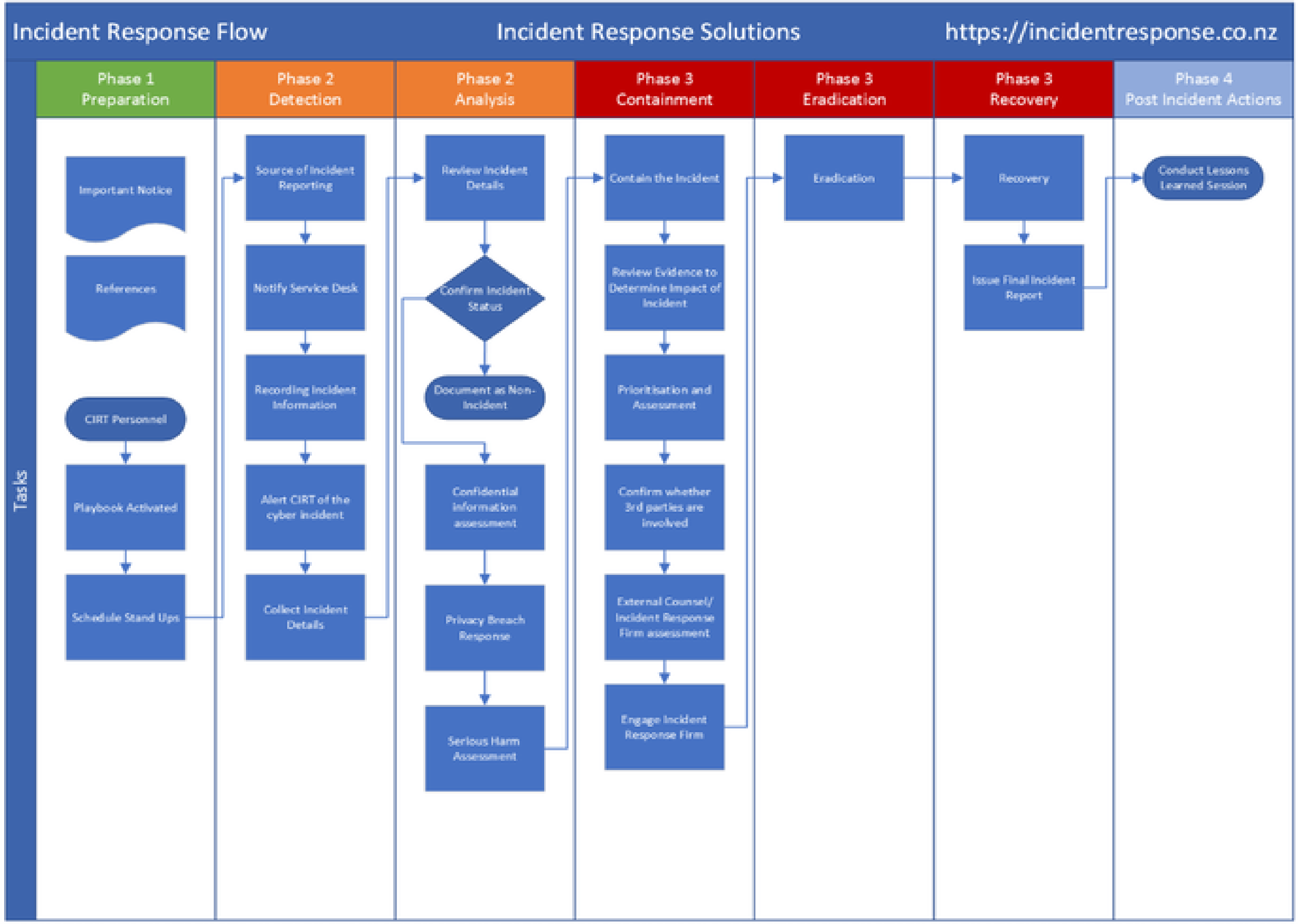
CIS Controls



Number	Control/Safeguard	IG1	IG2	IG3
13	**Network Monitoring and Defense**			
13.1	Centralize Security Event Alerting		●	●
13.2	Deploy a Host-Based Intrusion Detection Solution		●	●
13.3	Deploy a Network Intrusion Detection Solution		●	●
13.4	Perform Traffic Filtering Between Network Segments		●	●
13.5	Manage Access Control for Remote Assets		●	●
13.6	Collect Network Traffic Flow Logs		●	●
13.7	Deploy a Host-Based Intrusion Prevention Solution			●
13.8	Deploy a Network Intrusion Prevention Solution			●
13.9	Deploy Port-Level Access Control			●
13.10	Perform Application Layer Filtering			●
13.11	Tune Security Event Alerting Thresholds			●
14	**Security Awareness and Skills Training**			
14.1	Establish and Maintain a Security Awareness Program	●	●	●
14.2	Train Workforce Members to Recognize Social Engineering Attacks	●	●	●
14.3	Train Workforce Members on Authentication Best Practices	●	●	●
14.4	Train Workforce on Data Handling Best Practices	●	●	●
14.5	Train Workforce Members on Causes of Unintentional Data Exposure	●	●	●
14.6	Train Workforce Members on Recognizing and Reporting Security Incidents	●	●	●
14.7	Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates	●	●	●
14.8	Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks	●	●	●
14.9	Conduct Role-Specific Security Awareness and Skills Training		●	●
15	**Service Provider Management**			
15.1	Establish and Maintain an Inventory of Service Providers	●	●	●
15.2	Establish and Maintain a Service Provider Management Policy		●	●
15.3	Classify Service Providers		●	●
15.4	Ensure Service Provider Contracts Include Security Requirements		●	●
15.5	Assess Service Providers			●
15.6	Monitor Service Providers			●
15.7	Securely Decommission Service Providers			●

Number	Control/Safeguard	IG1	IG2	IG3
16	**Application Software Security**			
16.1	Establish and Maintain a Secure Application Development Process		●	●
16.2	Establish and Maintain a Process to Accept and Address Software Vulnerabilities		●	●
16.3	Perform Root Cause Analysis on Security Vulnerabilities		●	●
16.4	Establish and Manage an Inventory of Third-Party Software Components		●	●
16.5	Use Up-to-Date and Trusted Third-Party Software Components		●	●
16.6	Establish and Maintain a Severity Rating System and Process for Application Vulnerabilities		●	●
16.7	Use Standard Hardening Configuration Templates for Application Infrastructure		●	●
16.8	Separate Production and Non-Production Systems		●	●
16.9	Train Developers in Application Security Concepts and Secure Coding		●	●
16.10	Apply Secure Design Principles in Application Architectures		●	●
16.11	Leverage Vetted Modules or Services for Application Security Components		●	●
16.12	Implement Code-Level Security Checks			●
16.13	Conduct Application Penetration Testing			●
16.14	Conduct Threat Modeling			●
17	**Incident Response Management**			
17.1	Designate Personnel to Manage Incident Handling	●	●	●
17.2	Establish and Maintain Contact Information for Reporting Security Incidents	●	●	●
17.3	Establish and Maintain an Enterprise Process for Reporting Incidents	●	●	●
17.4	Establish and Maintain an Incident Response Process		●	●
17.5	Assign Key Roles and Responsibilities		●	●
17.6	Define Mechanisms for Communicating During Incident Response		●	●
17.7	Conduct Routine Incident Response Exercises		●	●
17.8	Conduct Post-Incident Reviews		●	●
17.9	Establish and Maintain Security Incident Thresholds			●
18	**Penetration Testing**			
18.1	Establish and Maintain a Penetration Testing Program		●	●
18.2	Perform Periodic External Penetration Tests		●	●
18.3	Remediate Penetration Test Findings		●	●
18.4	Validate Security Measures			●
18.5	Perform Periodic Internal Penetration Tests			●

Incident Response Plan



Incident Response Flow

Incident Response Solutions

https://incidentresponse.co.nz

Tasks

Phase 1
Preparation

- Important Notice
- References
- CIRT Personnel
- Playbook Activated
- Schedule Stand Ups

Phase 2
Detection

- Source of Incident Reporting
- Notify Service Desk
- Recording Incident Information
- Alert CIRT of the cyber incident
- Collect Incident Details

Phase 2
Analysis

- Review Incident Details
- Confirm Incident Status
- Document as Non-Incident
- Confidential information assessment
- Privacy Breach Response
- Serious Harm Assessment

Phase 3
Containment

- Contain the Incident
- Review Evidence to Determine Impact of Incident
- Prioritisation and Assessment
- Confirm whether 3rd parties are involved
- External Counsel/ Incident Response Firm assessment
- Engage Incident Response Firm

Phase 3
Eradication

- Eradication

Phase 3
Recovery

- Recovery
- Issue Final Incident Report

Phase 4
Post Incident Actions

- Conduct Lessons Learned Session

Thank you

Campbell McKenzie

0800 WITNESS or 021 779 310

campbell@incidentresponse.co.nz

incidentresponse.co.nz

whistleblowers.co.nz

Incident Response

FORENSIC & CYBER