Incident Response
FORENSIC & CYBER

Cyber Governance
Applying cyber controls using a 'lessons learned' approach

Tertiary ICT - September 2022

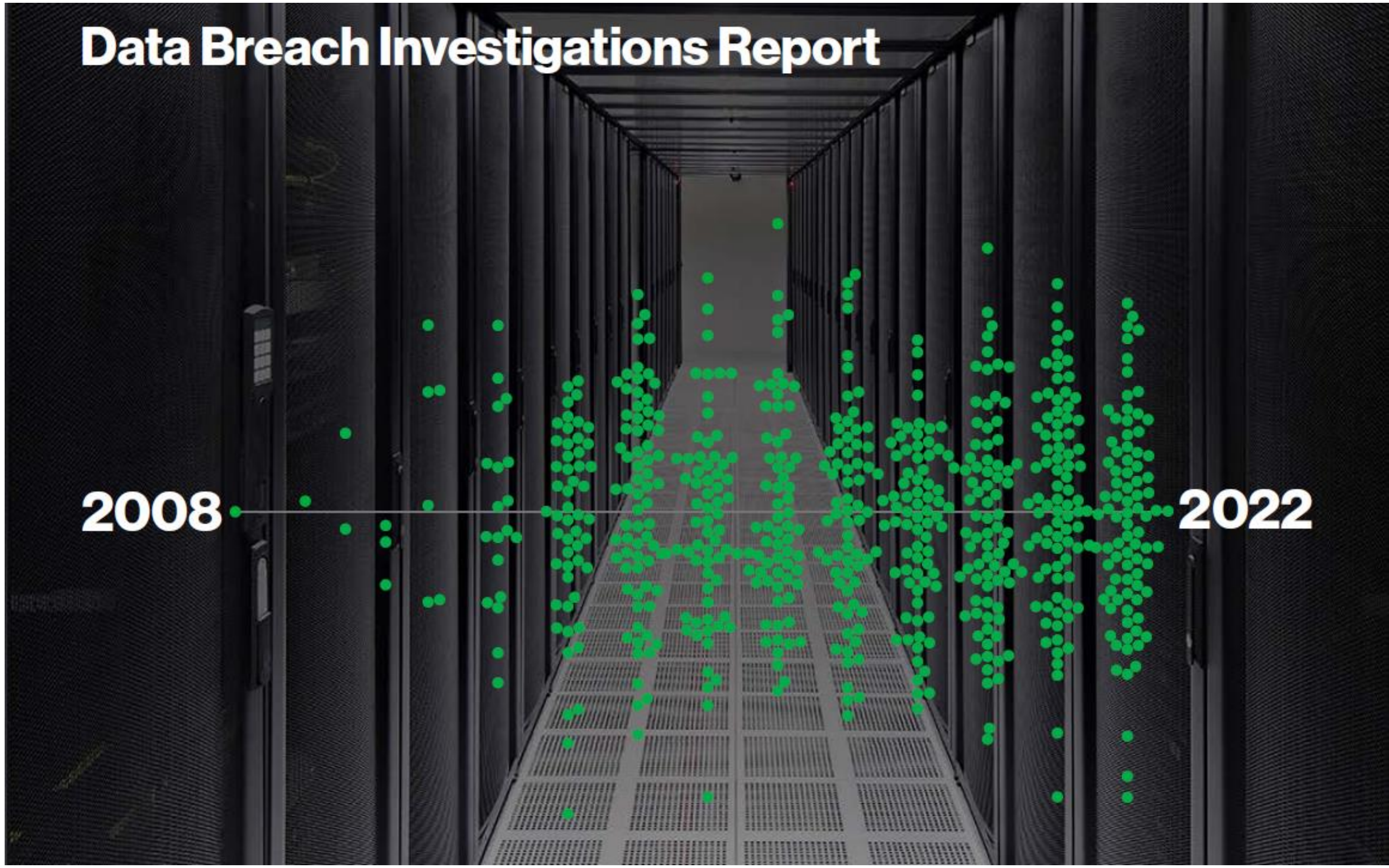
Cyber – Incidents and Breaches

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.

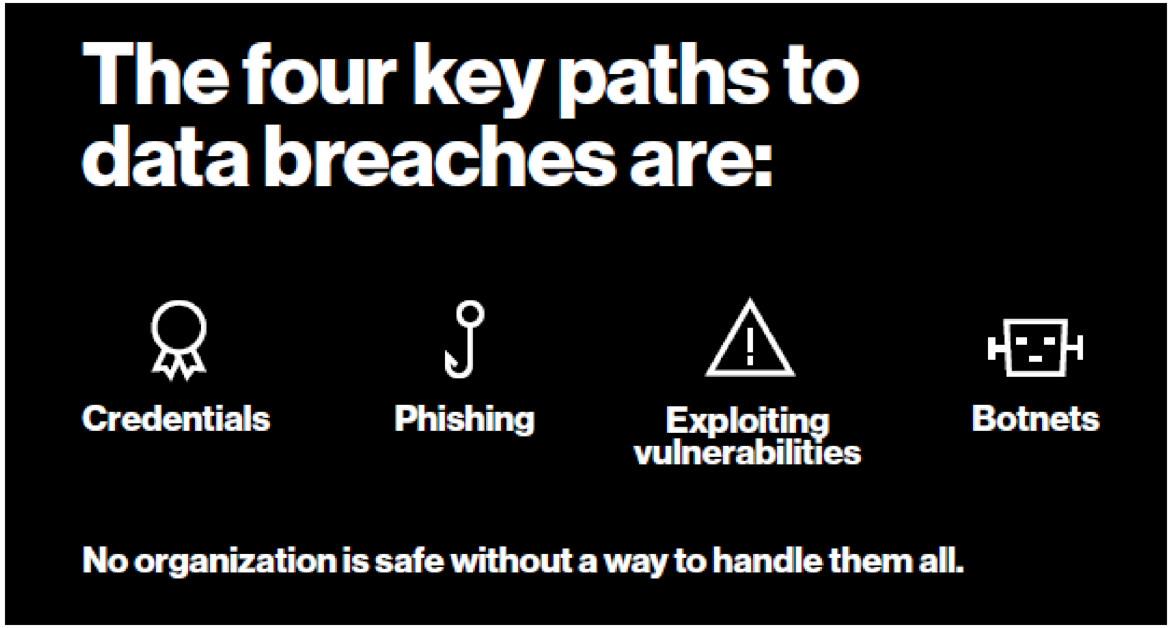


https://www.verizon.com/business/resources/reports/dbir

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:

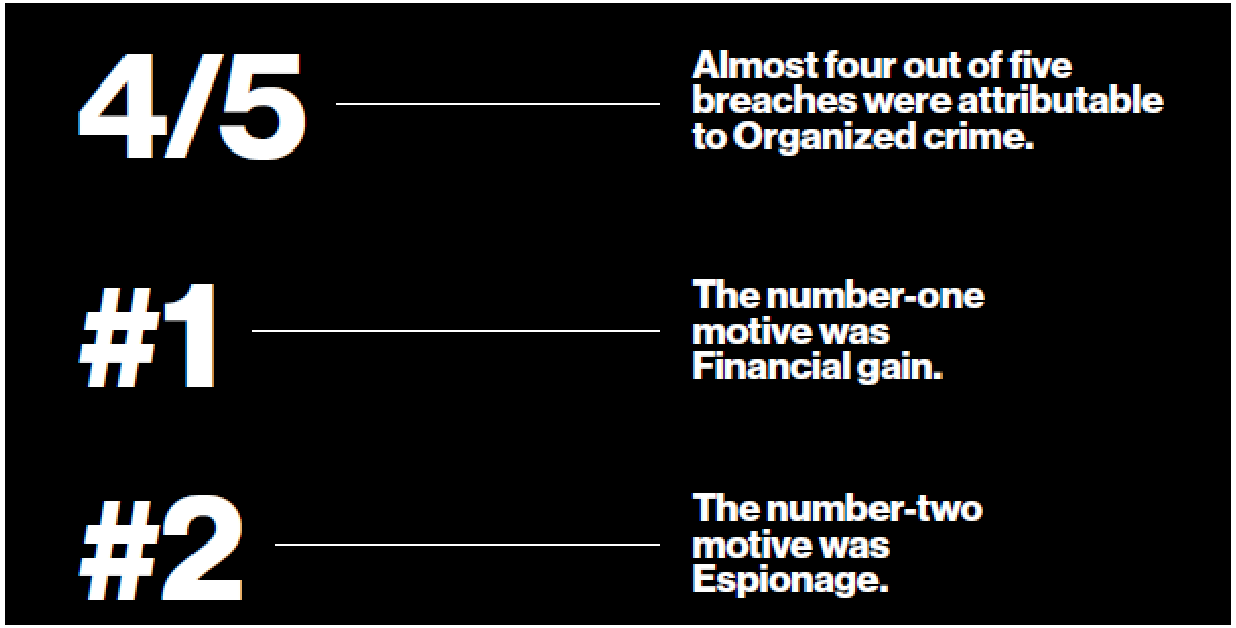
Credentials

Phishing

Exploiting vulnerabilities

Botnets

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

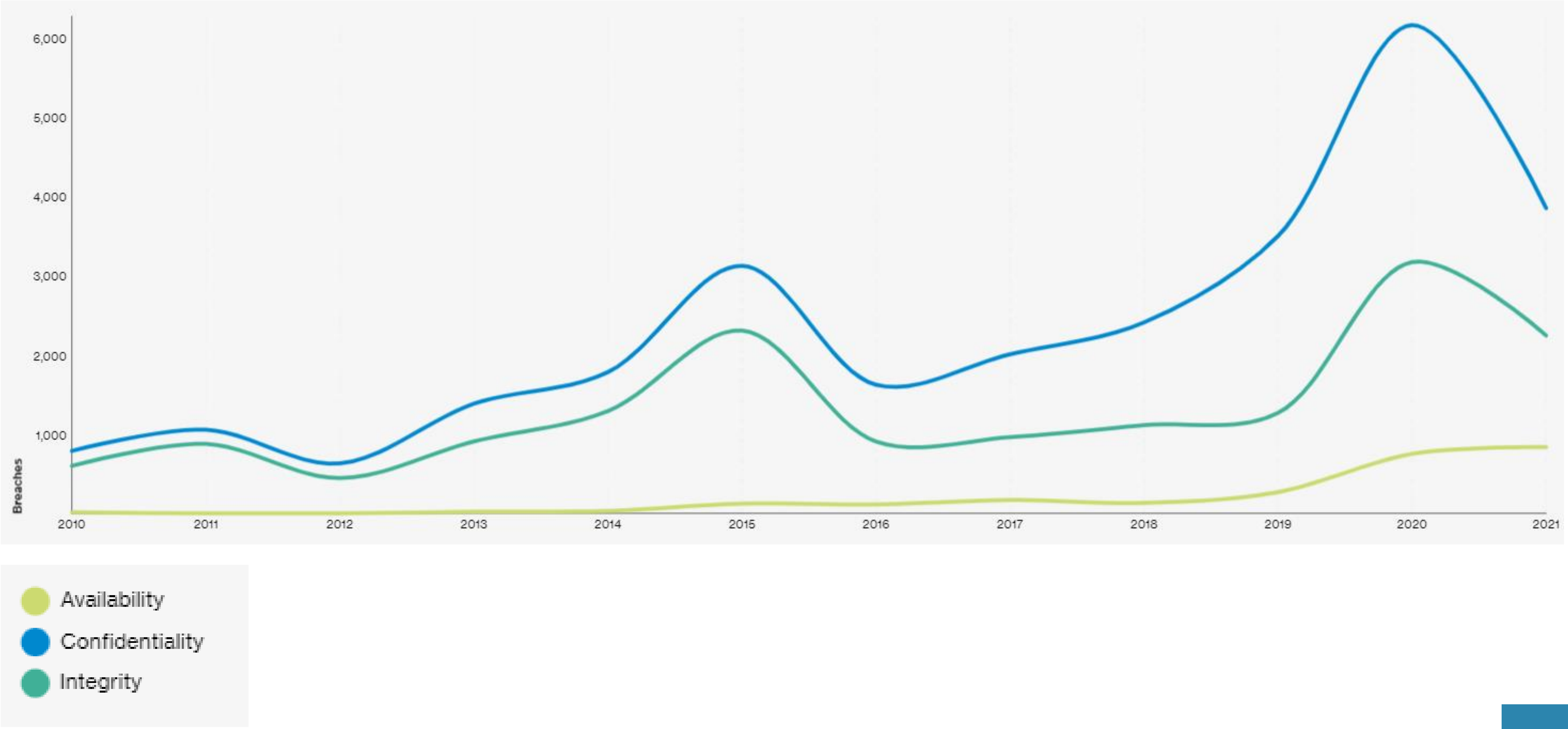


4/5 — Almost four out of five breaches were attributable to Organized crime.

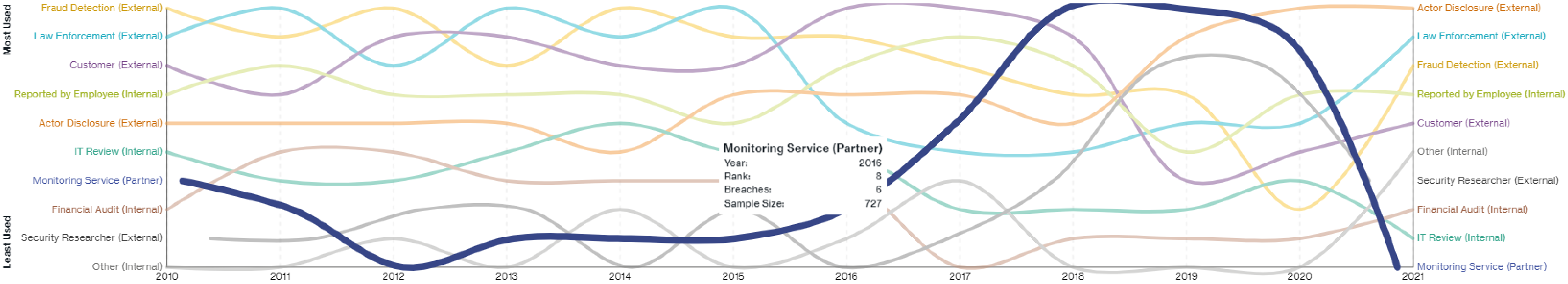
#1 — The number-one motive was Financial gain.

#2 — The number-two motive was Espionage.

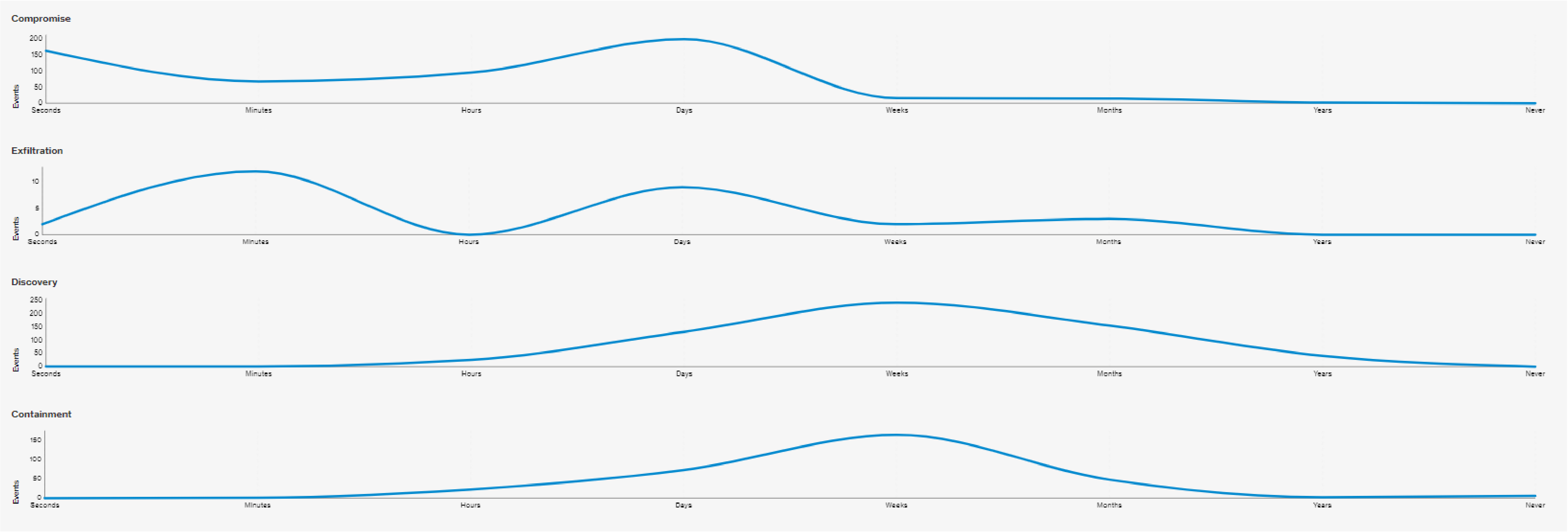
What Verizon Found - Breach Trends



What Verizon Found - Discovery Methods Used Over Time



What Verizon Found - Response Time For Breach Events - 2010



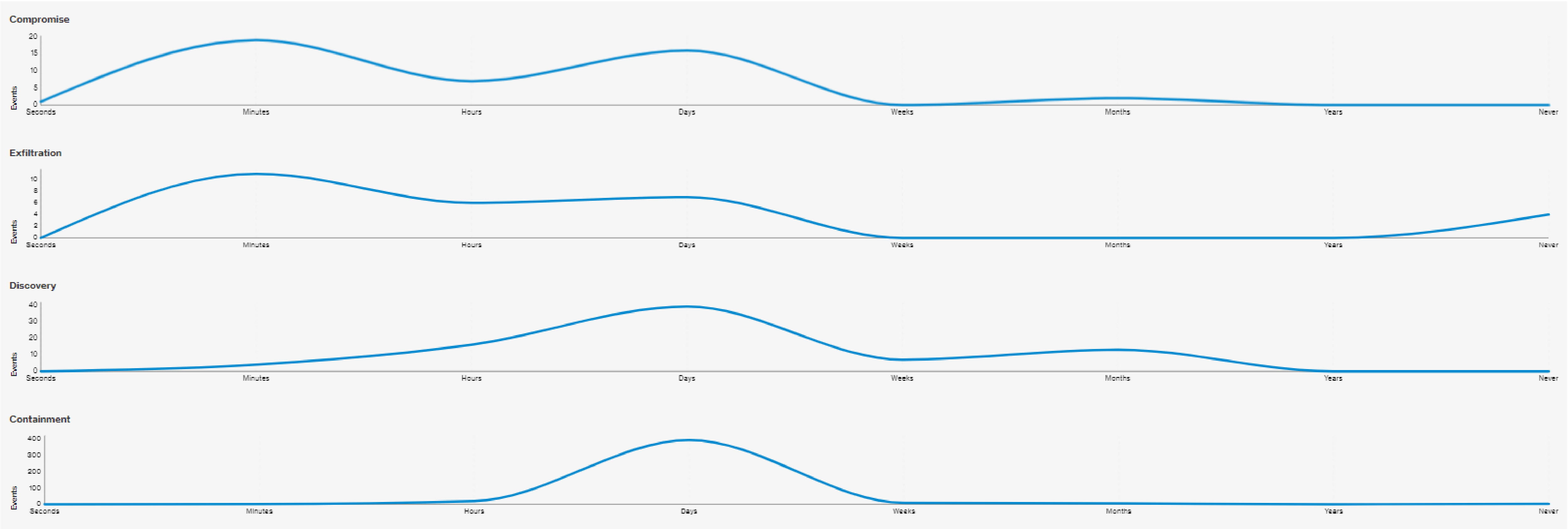
Compromise

Exfiltration

Discovery

Containment

What Verizon Found - Response Time For Breach Events – 2021



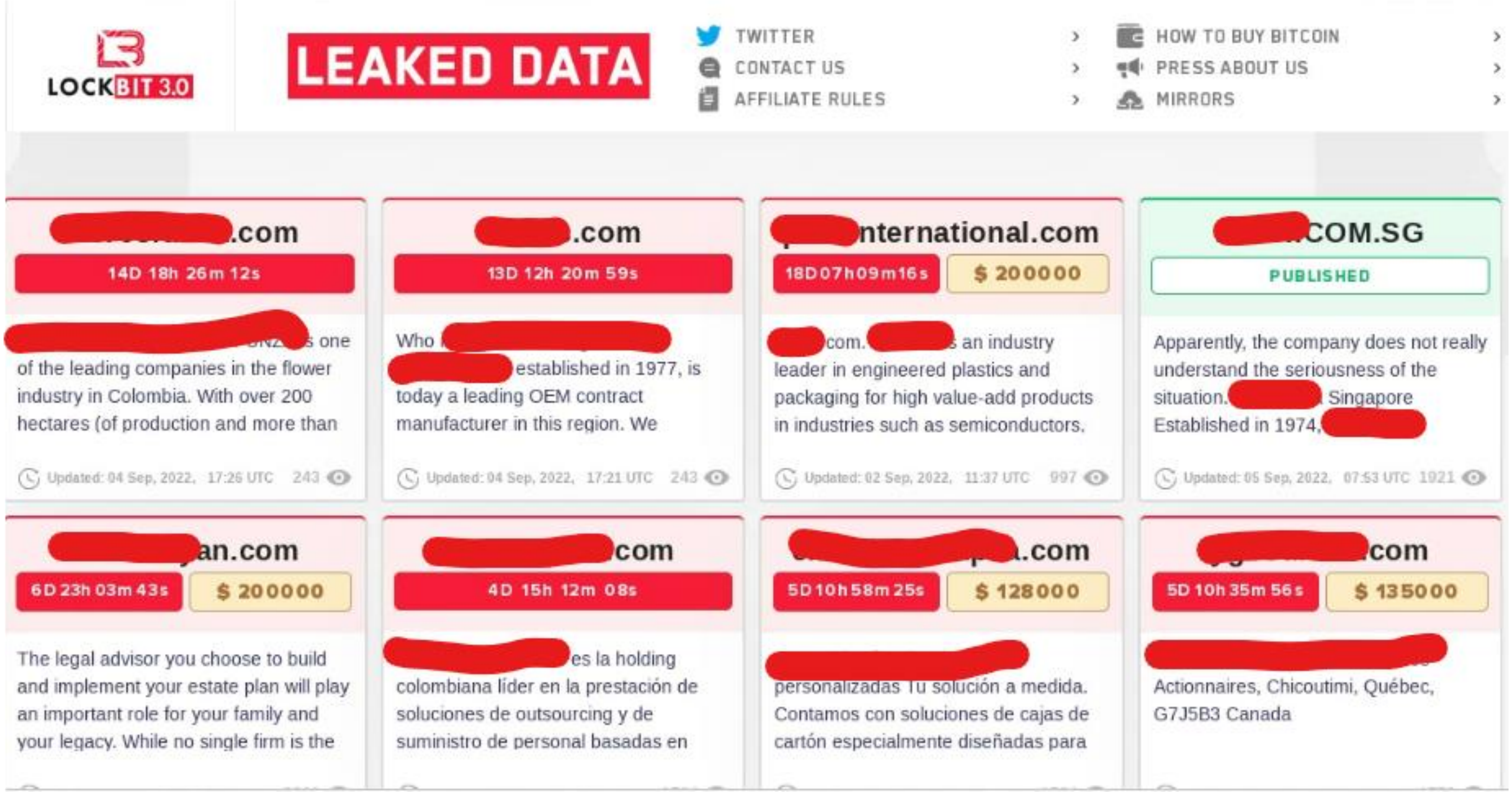
Compromise

Exfiltration

Discovery

Containment

Our observations over the last 12 months



[redacted].com

14D 18h 26m 12s

[redacted] one of the leading companies in the flower industry in Colombia. With over 200 hectares (of production and more than

Updated: 04 Sep, 2022, 17:26 UTC 243

[redacted].com

13D 12h 20m 59s

Who [redacted] [redacted] established in 1977, is today a leading OEM contract manufacturer in this region. We

Updated: 04 Sep, 2022, 17:21 UTC 243

[redacted]nternational.com

18D 07h 09m 16s $ 200000

[redacted]com. [redacted] an industry leader in engineered plastics and packaging for high value-add products in industries such as semiconductors.

Updated: 02 Sep, 2022, 11:37 UTC 997

[redacted].COM.SG

PUBLISHED

Apparently, the company does not really understand the seriousness of the situation. [redacted] Singapore Established in 1974, [redacted]

Updated: 05 Sep, 2022, 07:53 UTC 1021

[redacted]an.com

6D 23h 03m 43s $ 200000

The legal advisor you choose to build and implement your estate plan will play an important role for your family and your legacy. While no single firm is the

[redacted]com

4D 15h 12m 08s

[redacted]es la holding colombiana líder en la prestación de soluciones de outsourcing y de suministro de personal basadas en

[redacted].com

5D 10h 58m 25s $ 128000

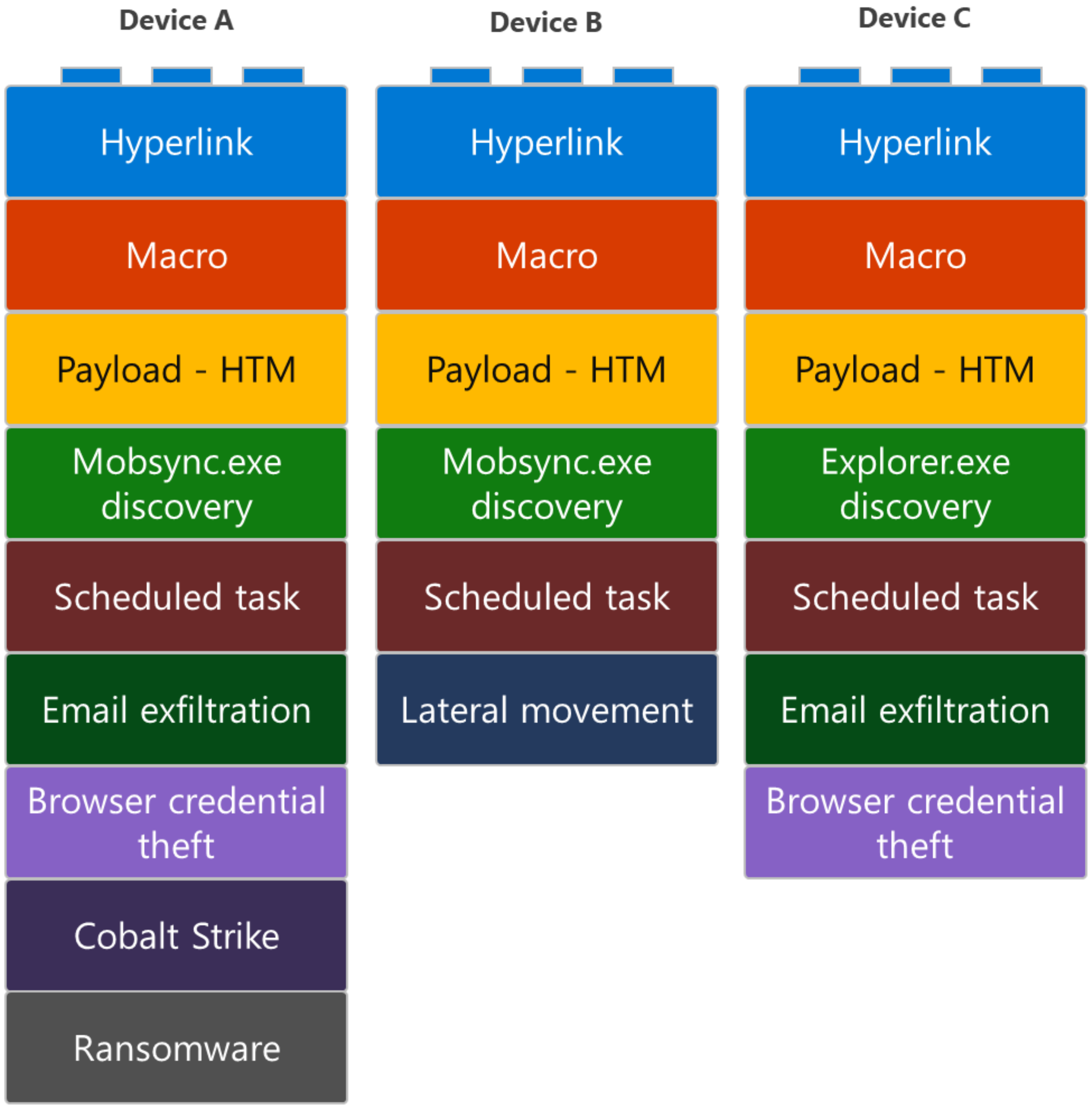
[redacted] personalizadas Tu solución a medida. Contamos con soluciones de cajas de cartón especialmente diseñadas para

[redacted]com

5D 10h 35m 56s $ 135000

[redacted] Actionnaires, Chicoutimi, Québec, G7J5B3 Canada

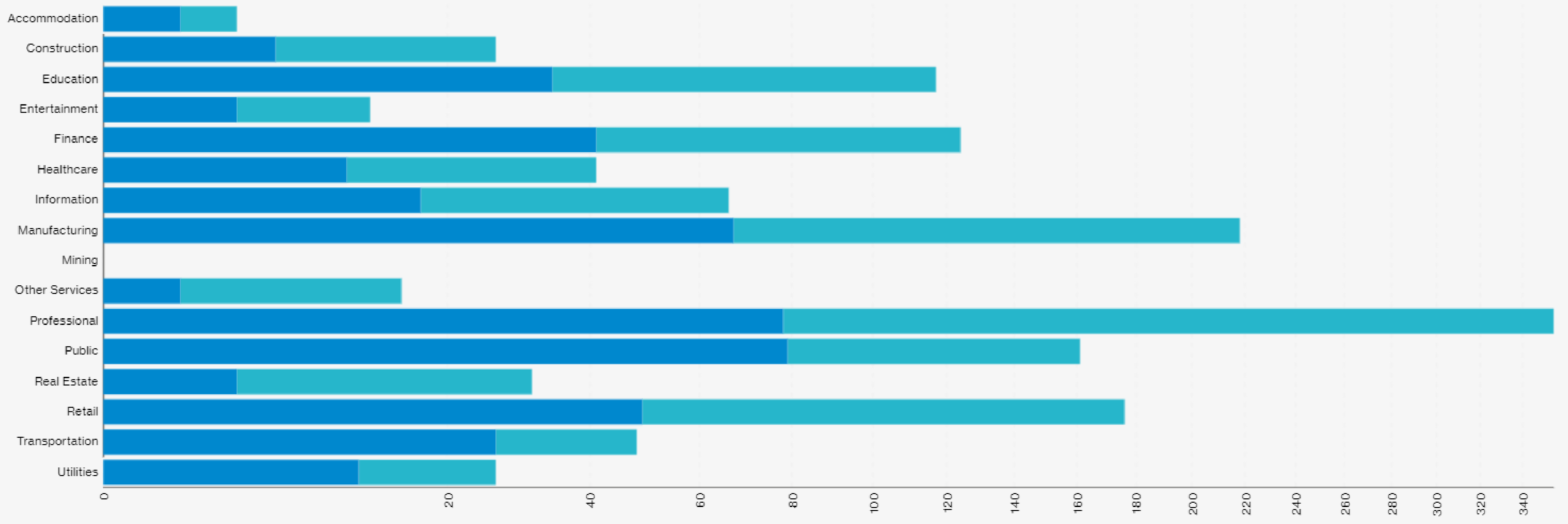
Our observations over the last 12 months



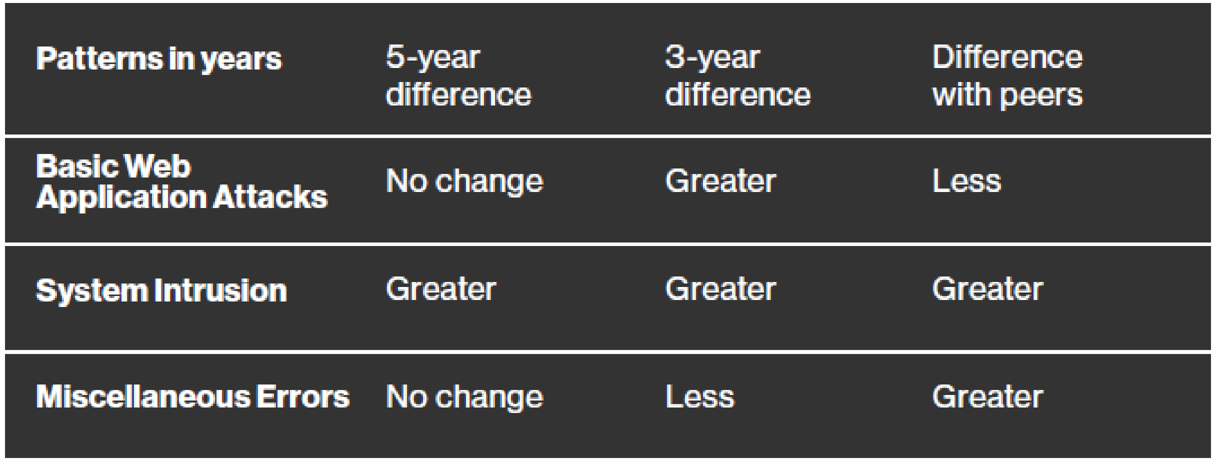
Device A	Device B	Device C
Hyperlink	Hyperlink	Hyperlink
Macro	Macro	Macro
Payload - HTM	Payload - HTM	Payload - HTM
Mobsync.exe discovery	Mobsync.exe discovery	Explorer.exe discovery
Scheduled task	Scheduled task	Scheduled task
Email exfiltration	Lateral movement	Email exfiltration
Browser credential theft		Browser credential theft
Cobalt Strike		
Ransomware		

Education Sector

What Verizon Found - Industry Breakdown by Organization Size



What Verizon Found – Education Sector



Patterns in years	5-year difference	3-year difference	Difference with peers
Basic Web Application Attacks	No change	Greater	Less
System Intrusion	Greater	Greater	Greater
Miscellaneous Errors	No change	Less	Greater

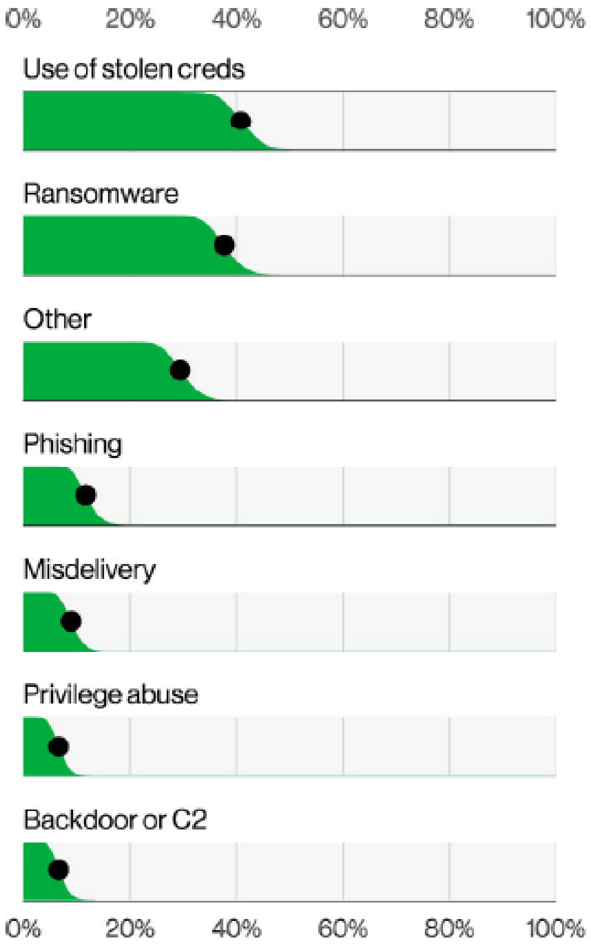
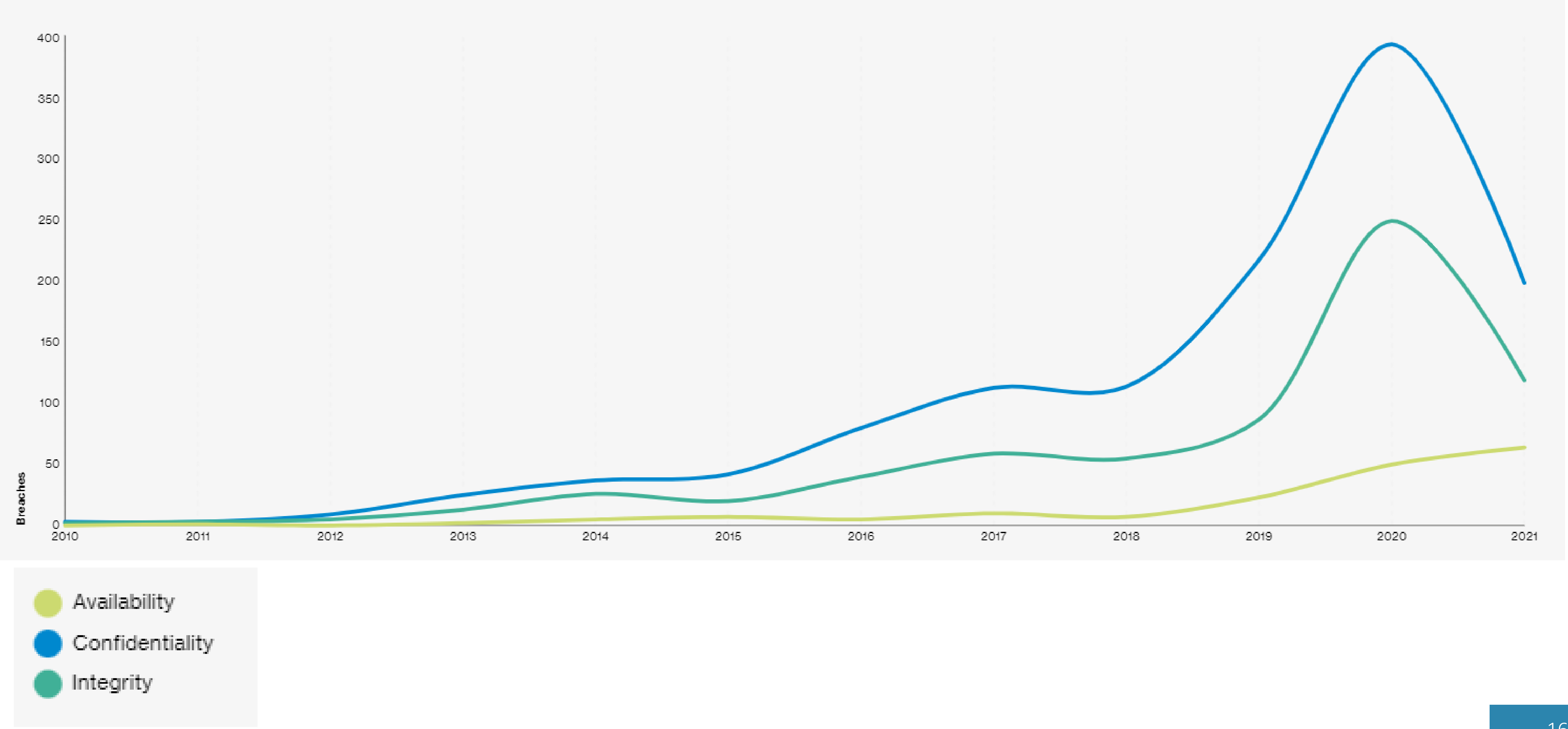
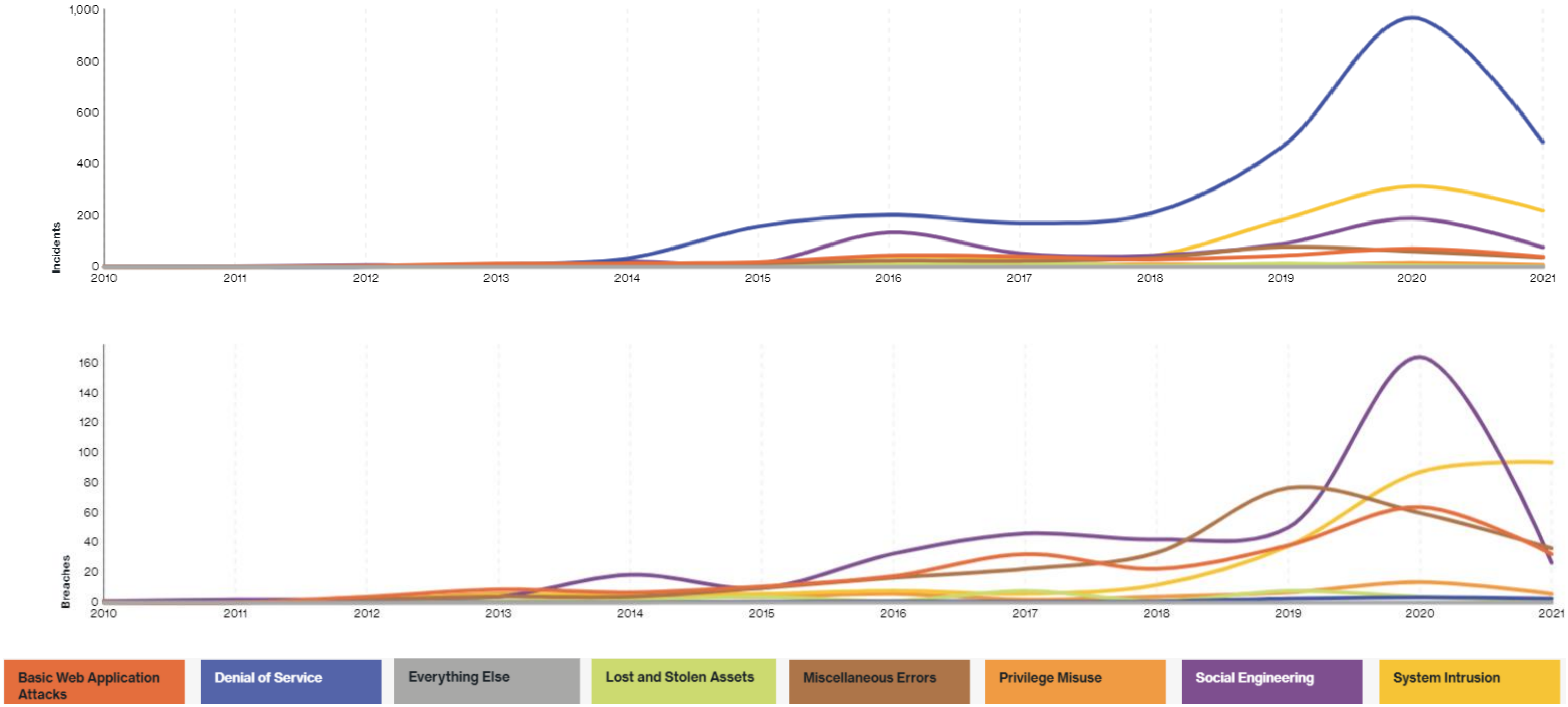


Figure 84. Top Action varieties in Educational Services breaches (n=218)

What Verizon Found – Education Sector

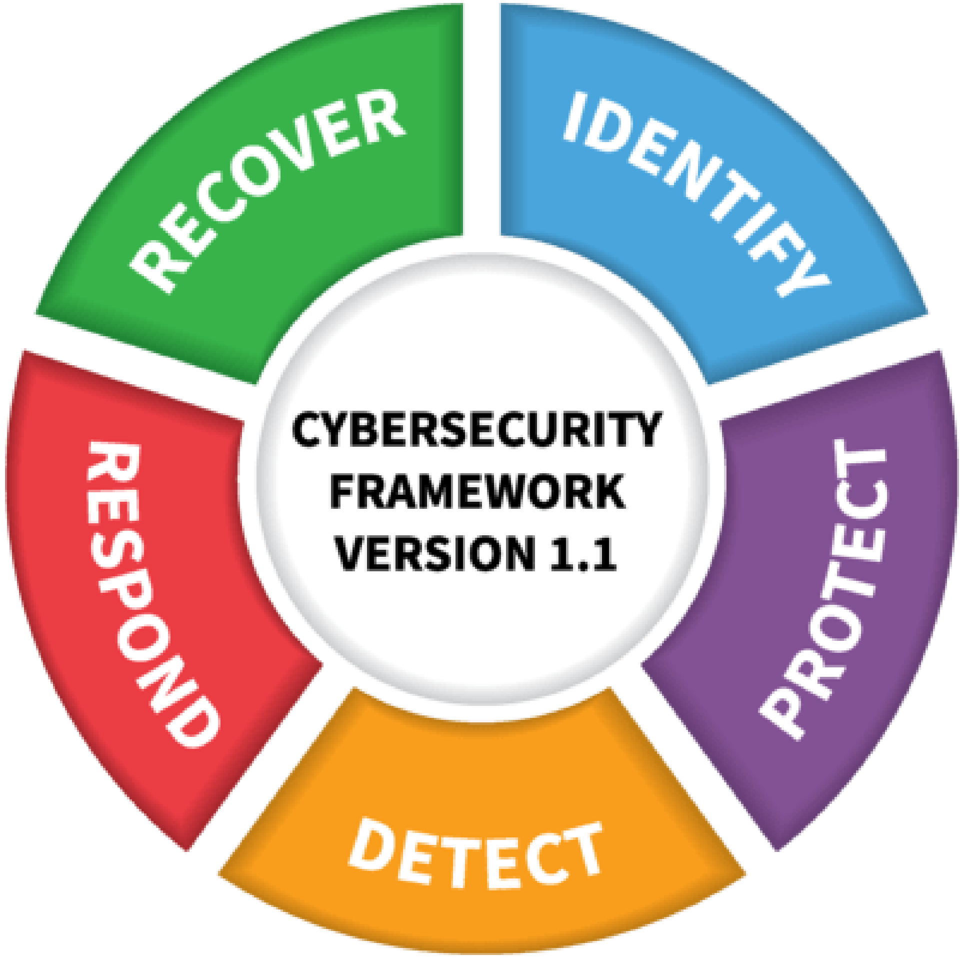


What Verizon Found – Education Sector

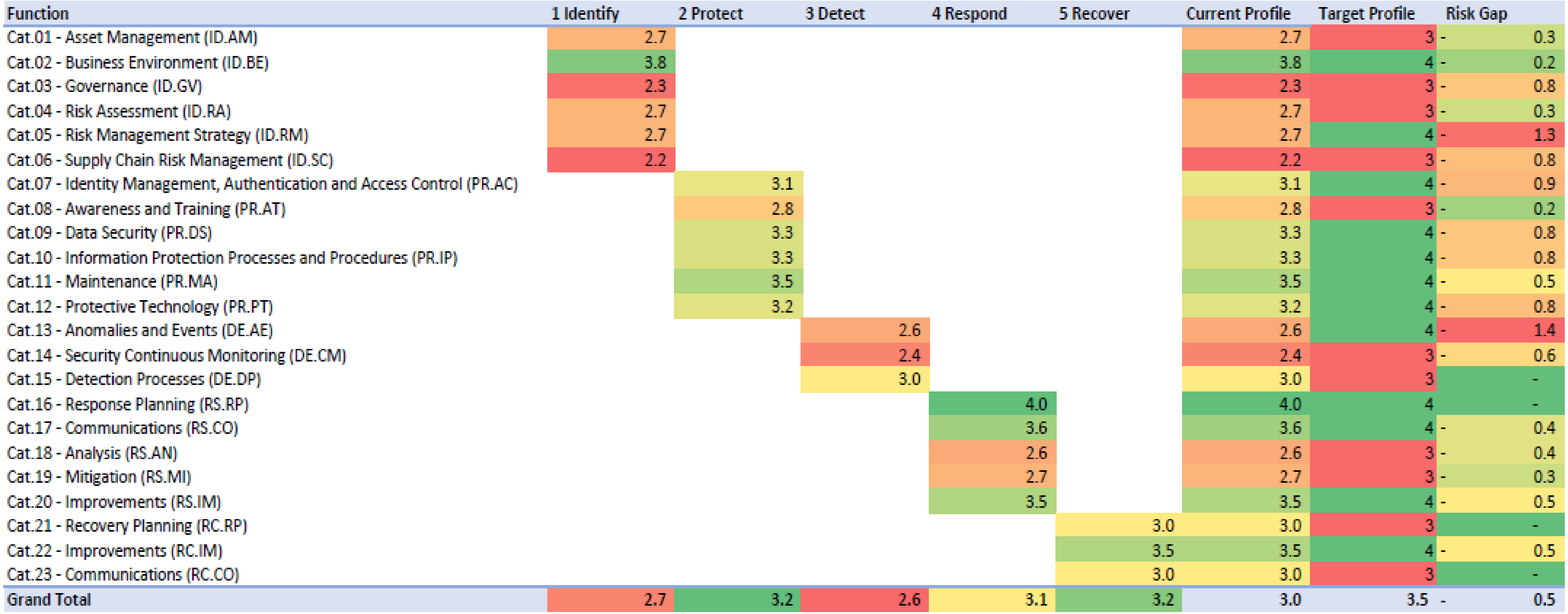


Cyber Governance

NIST Cyber Security Framework

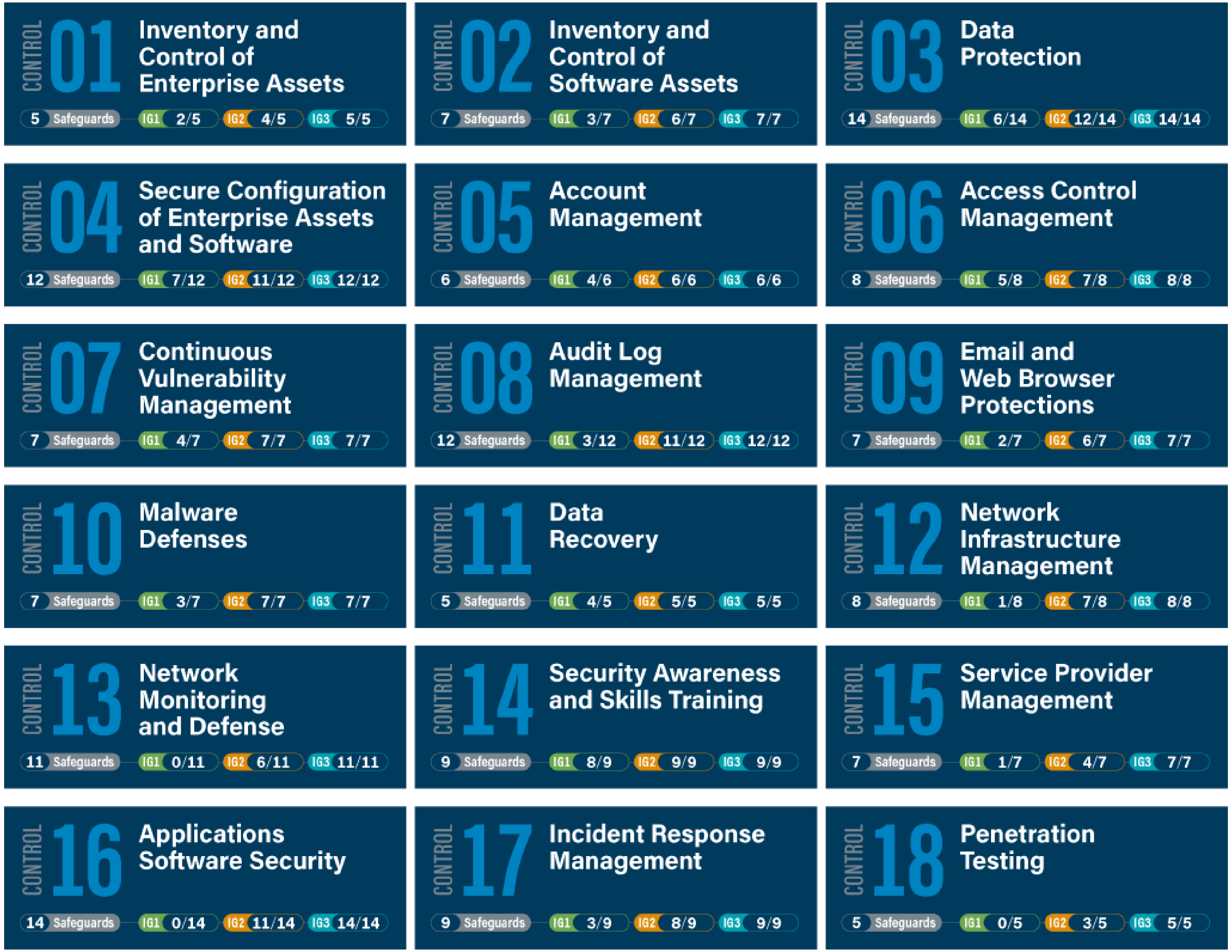


Completed Framework Example



Function	1 Identify	2 Protect	3 Detect	4 Respond	5 Recover	Current Profile	Target Profile	Risk Gap
Cat.01 - Asset Management (ID.AM)	2.7					2.7	3	- 0.3
Cat.02 - Business Environment (ID.BE)	3.8					3.8	4	- 0.2
Cat.03 - Governance (ID.GV)	2.3					2.3	3	- 0.8
Cat.04 - Risk Assessment (ID.RA)	2.7					2.7	3	- 0.3
Cat.05 - Risk Management Strategy (ID.RM)	2.7					2.7	4	- 1.3
Cat.06 - Supply Chain Risk Management (ID.SC)	2.2					2.2	3	- 0.8
Cat.07 - Identity Management, Authentication and Access Control (PR.AC)		3.1				3.1	4	- 0.9
Cat.08 - Awareness and Training (PR.AT)		2.8				2.8	3	- 0.2
Cat.09 - Data Security (PR.DS)		3.3				3.3	4	- 0.8
Cat.10 - Information Protection Processes and Procedures (PR.IP)		3.3				3.3	4	- 0.8
Cat.11 - Maintenance (PR.MA)		3.5				3.5	4	- 0.5
Cat.12 - Protective Technology (PR.PT)		3.2				3.2	4	- 0.8
Cat.13 - Anomalies and Events (DE.AE)			2.6			2.6	4	- 1.4
Cat.14 - Security Continuous Monitoring (DE.CM)			2.4			2.4	3	- 0.6
Cat.15 - Detection Processes (DE.DP)			3.0			3.0	3	-
Cat.16 - Response Planning (RS.RP)				4.0		4.0	4	-
Cat.17 - Communications (RS.CO)				3.6		3.6	4	- 0.4
Cat.18 - Analysis (RS.AN)				2.6		2.6	3	- 0.4
Cat.19 - Mitigation (RS.MI)				2.7		2.7	3	- 0.3
Cat.20 - Improvements (RS.IM)				3.5		3.5	4	- 0.5
Cat.21 - Recovery Planning (RC.RP)					3.0	3.0	3	-
Cat.22 - Improvements (RC.IM)					3.5	3.5	4	- 0.5
Cat.23 - Communications (RC.CO)					3.0	3.0	3	-
Grand Total	2.7	3.2	2.6	3.1	3.2	3.0	3.5	- 0.5

CIS Controls



CONTROL		Safeguards	IG1	IG2	IG3
01	Inventory and Control of Enterprise Assets	5	2/5	4/5	5/5
02	Inventory and Control of Software Assets	7	3/7	6/7	7/7
03	Data Protection	14	6/14	12/14	14/14
04	Secure Configuration of Enterprise Assets and Software	12	7/12	11/12	12/12
05	Account Management	6	4/6	6/6	6/6
06	Access Control Management	8	5/8	7/8	8/8
07	Continuous Vulnerability Management	7	4/7	7/7	7/7
08	Audit Log Management	12	3/12	11/12	12/12
09	Email and Web Browser Protections	7	2/7	6/7	7/7
10	Malware Defenses	7	3/7	7/7	7/7
11	Data Recovery	5	4/5	5/5	5/5
12	Network Infrastructure Management	8	1/8	7/8	8/8
13	Network Monitoring and Defense	11	0/11	6/11	11/11
14	Security Awareness and Skills Training	9	8/9	9/9	9/9
15	Service Provider Management	7	1/7	4/7	7/7
16	Applications Software Security	14	0/14	11/14	14/14
17	Incident Response Management	9	3/9	8/9	9/9
18	Penetration Testing	5	0/5	3/5	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.

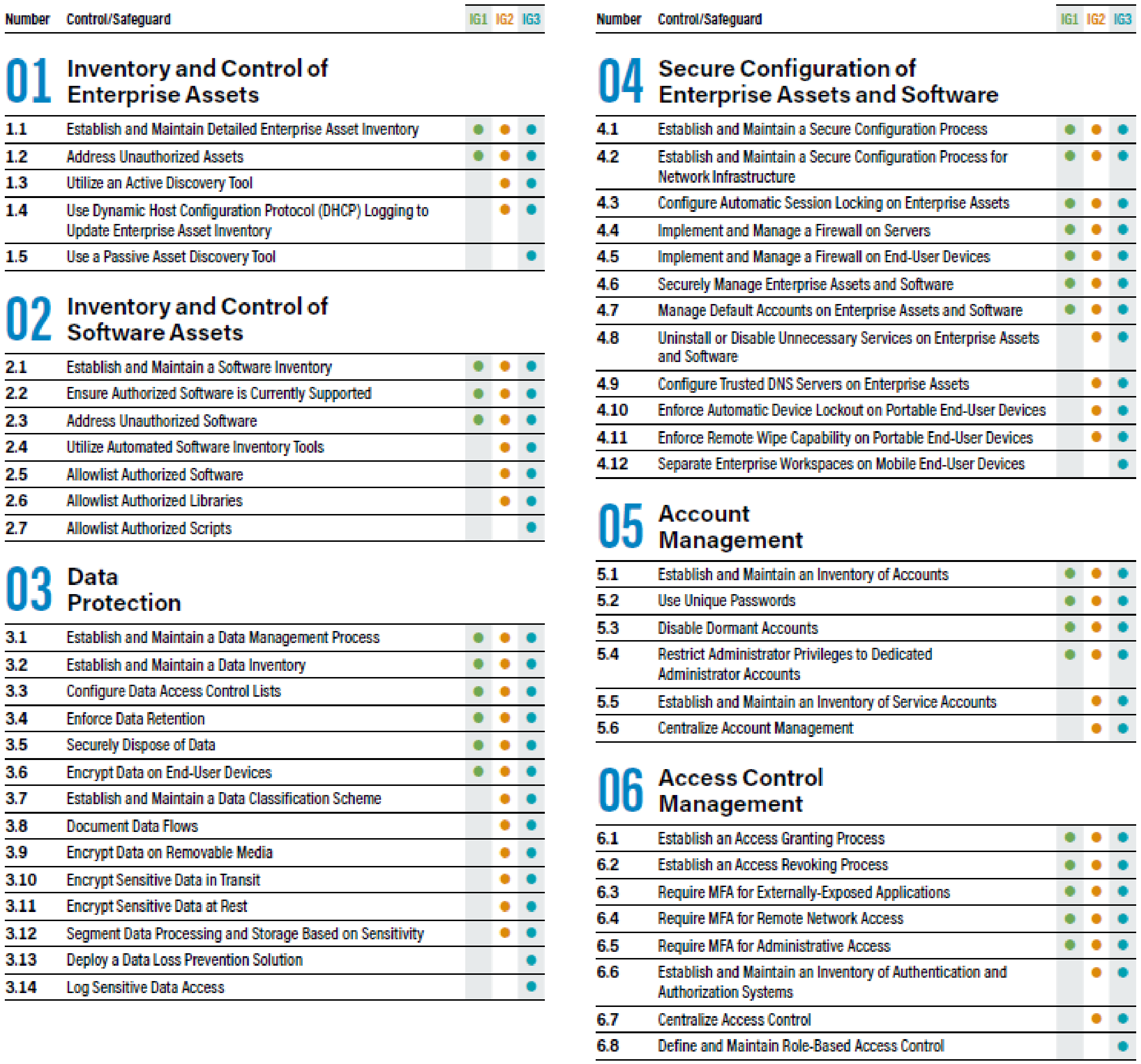
74 Additional cyber defense Safeguards

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

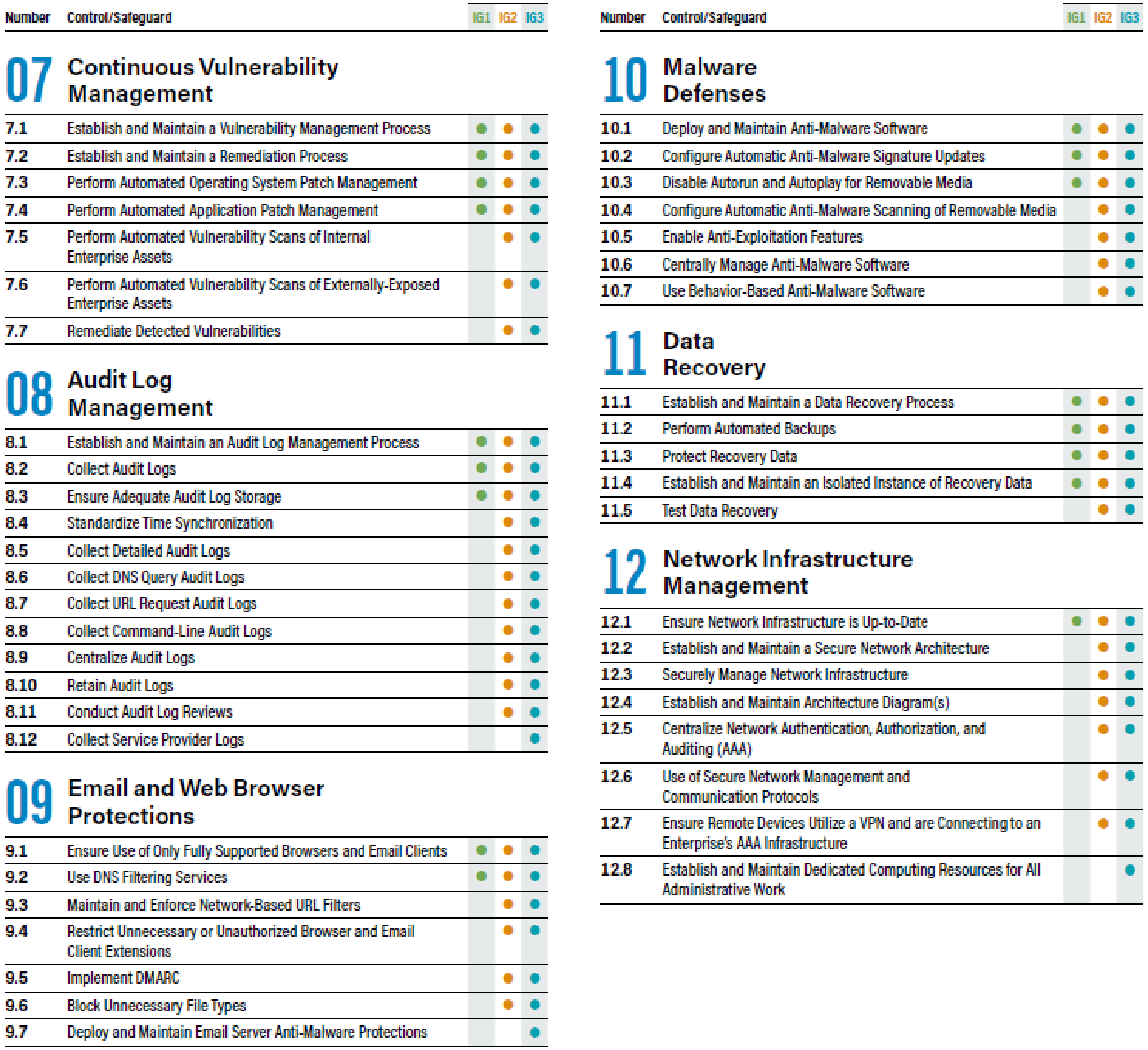
CIS Controls



Number	Control/Safeguard	IG1	IG2	IG3
01	**Inventory and Control of Enterprise Assets**			
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**			
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**			
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			●

Number	Control/Safeguard	IG1	IG2	IG3
04	**Secure Configuration of Enterprise Assets and Software**			
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**			
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**			
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



07 Continuous Vulnerability Management

Number	Control/Safeguard	IG1	IG2	IG3
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

Number	Control/Safeguard	IG1	IG2	IG3
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

Number	Control/Safeguard	IG1	IG2	IG3
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

Number	Control/Safeguard	IG1	IG2	IG3
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		●	●

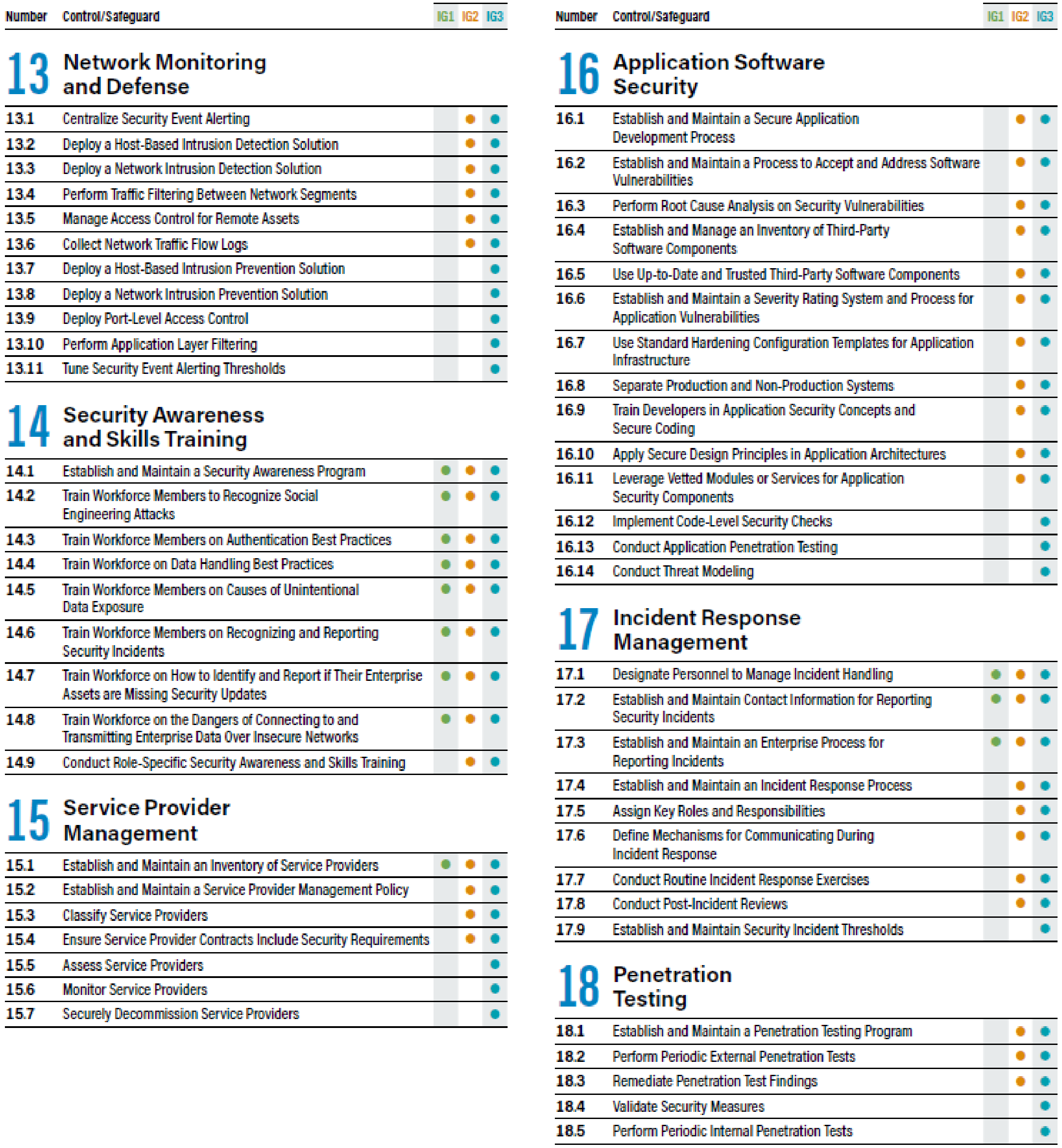
11 Data Recovery

Number	Control/Safeguard	IG1	IG2	IG3
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

Number	Control/Safeguard	IG1	IG2	IG3
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



13 Network Monitoring and Defense

Number	Control/Safeguard	IG1	IG2	IG3
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

Number	Control/Safeguard	IG1	IG2	IG3
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

Number	Control/Safeguard	IG1	IG2	IG3
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			●

16 Application Software Security

Number	Control/Safeguard	IG1	IG2	IG3
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			●

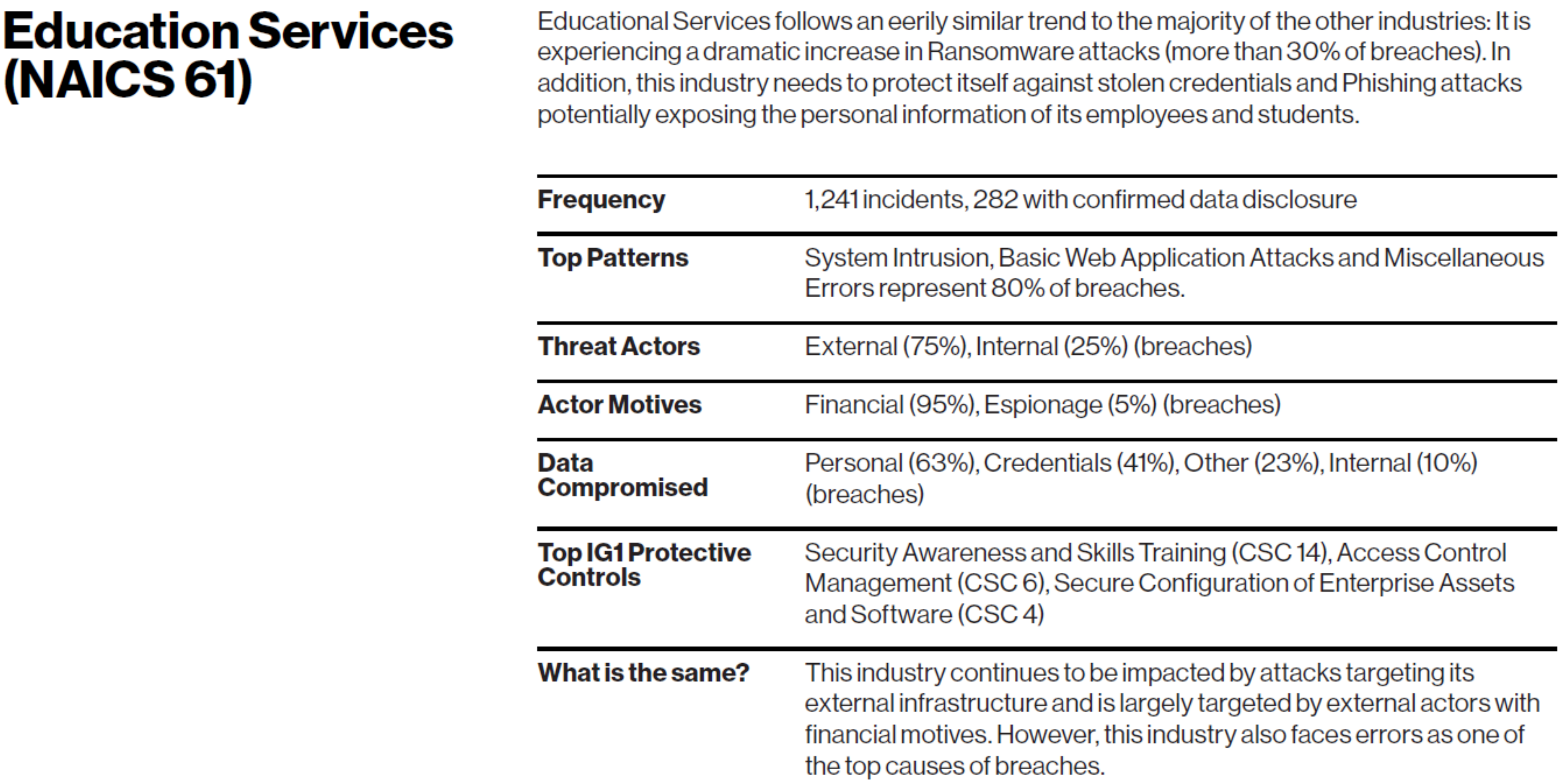
17 Incident Response Management

Number	Control/Safeguard	IG1	IG2	IG3
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

Number	Control/Safeguard	IG1	IG2	IG3
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			●

Applying Controls from the lessons learned

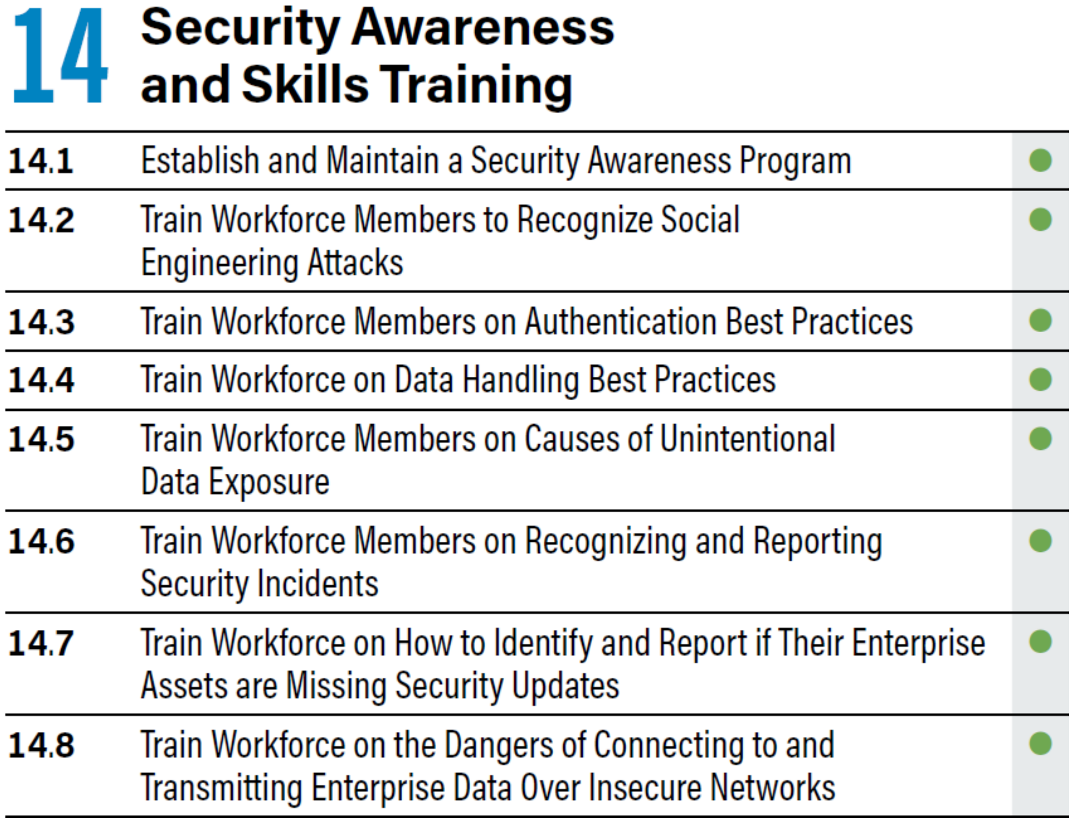


Education Services (NAICS 61)

Educational Services follows an eerily similar trend to the majority of the other industries: It is experiencing a dramatic increase in Ransomware attacks (more than 30% of breaches). In addition, this industry needs to protect itself against stolen credentials and Phishing attacks potentially exposing the personal information of its employees and students.

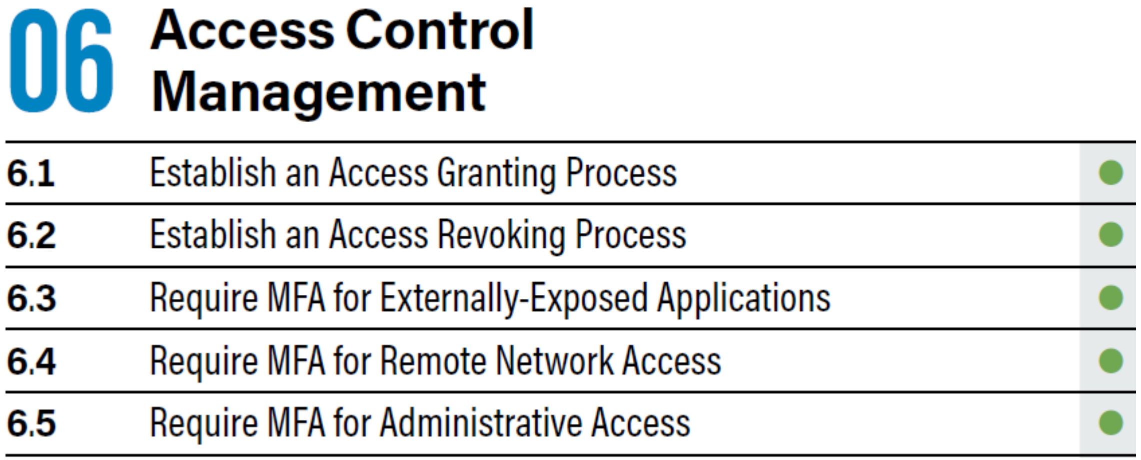
Frequency	1,241 incidents, 282 with confirmed data disclosure
Top Patterns	System Intrusion, Basic Web Application Attacks and Miscellaneous Errors represent 80% of breaches.
Threat Actors	External (75%), Internal (25%) (breaches)
Actor Motives	Financial (95%), Espionage (5%) (breaches)
Data Compromised	Personal (63%), Credentials (41%), Other (23%), Internal (10%) (breaches)
Top IG1 Protective Controls	Security Awareness and Skills Training (CSC 14), Access Control Management (CSC 6), Secure Configuration of Enterprise Assets and Software (CSC 4)
What is the same?	This industry continues to be impacted by attacks targeting its external infrastructure and is largely targeted by external actors with financial motives. However, this industry also faces errors as one of the top causes of breaches.

Applying Controls from the lessons learned



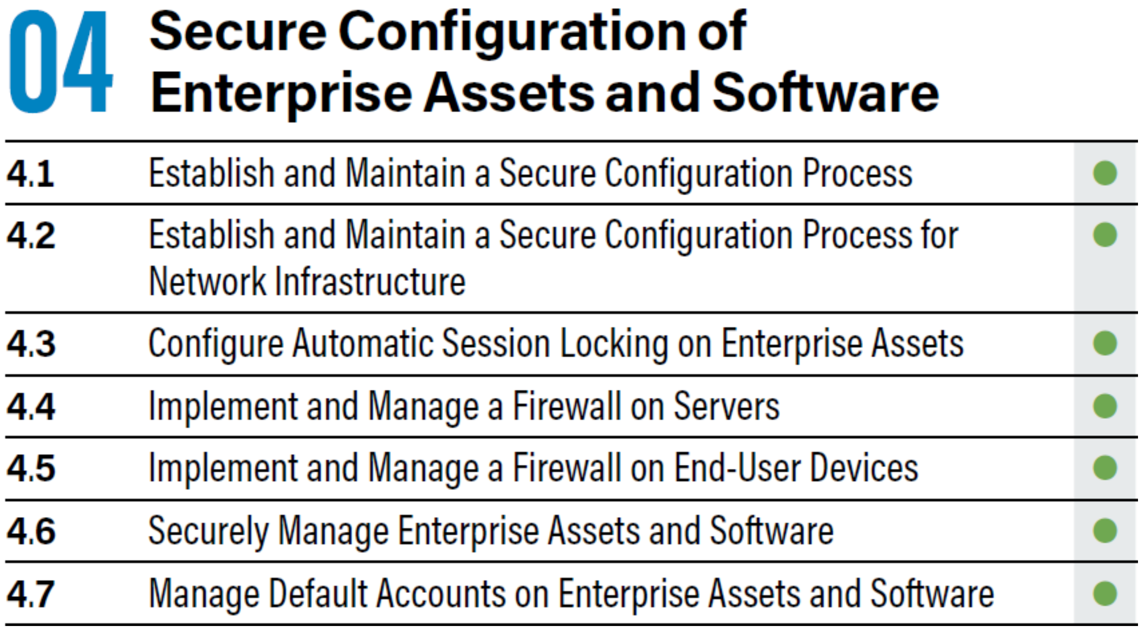
14 Security Awareness and Skills Training

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	●



06 Access Control Management

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	●



04 Secure Configuration of Enterprise Assets and Software

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	●

What services are clients engaging in?

- Cyber framework
- Cyber controls
- Incident response plans and playbooks
- Incident response control room
- Tabletop simulations
- Responding to incidents including forensics
- Incident response retainer

Thank you

Campbell McKenzie

0800 WITNESS or 021 779 310

campbell@incidentresponse.co.nz

incidentresponse.co.nz

whistleblowers.co.nz

Incident Response
FORENSIC & CYBER