Cyber Incident Response
Westcon-Comstor
March 2024

Todays Presentation – in 60 Seconds

- Threat Landscape
- Cyber incident response procedures
- Working with insurers and lawyers
- Working with IT / MSP companies

Technology Risk Management

Theft of Information

Hackers and dissatisfied employees try to obtain personally identifiable information (PII), or steal credit card information, customer lists, intellectual property, and other sensitive information.

Password Theft

Attackers steal passwords to access company systems.

Phishing Attacks

Email designed to look like legitimate correspondence that tricks recipients into clicking on a link that installs malware on the system.

Ransomware

Malicious software blocks access to a computer so that criminals can hold your data for ransom.

Natural Disasters

Data loss occurs due to natural events and accidents like fires and floods.

Defacement and Downtime

Attackers force your website or other technology to no longer look or function properly. This could be as a joke, for political reasons, or to damage your reputation

Thinking Ahead. Being Prepared

In October 2018, the New Zealand National Cyber Security Centre (NCSC) published the results of its survey of 250 nationally significant organisations.

Key findings include:

i. An area of good practice that was identified is:

Readiness – Preparing the organisation to detect, respond and recover from a cyber-security incident.

ii. When an organisation becomes aware of an incident, being **ready** to respond can **reduce** its impact of a compromise.

iii. Having an **up-to-date plan** allows an organisation to react **quickly and decisively** when an incident occurs and serves as a framework to **preserve evidence** in the event legal action is sought following an incident.

iv. 63% of New Zealand's Nationally Significant Organisations have an incident response plan, but 33% have not **tested their plan** in the last year.

We are proud to be a 100% New Zealand owned and operated business.

Welcome to RansomLook !

March 8Th, 2024

Currently tracking `174` groups across `312` relays & mirrors - `86` *currently online*

There have been `10` posts within the last 24 hours

There have been `87` posts within the month of march

There have been `1103` posts within the last 90 days

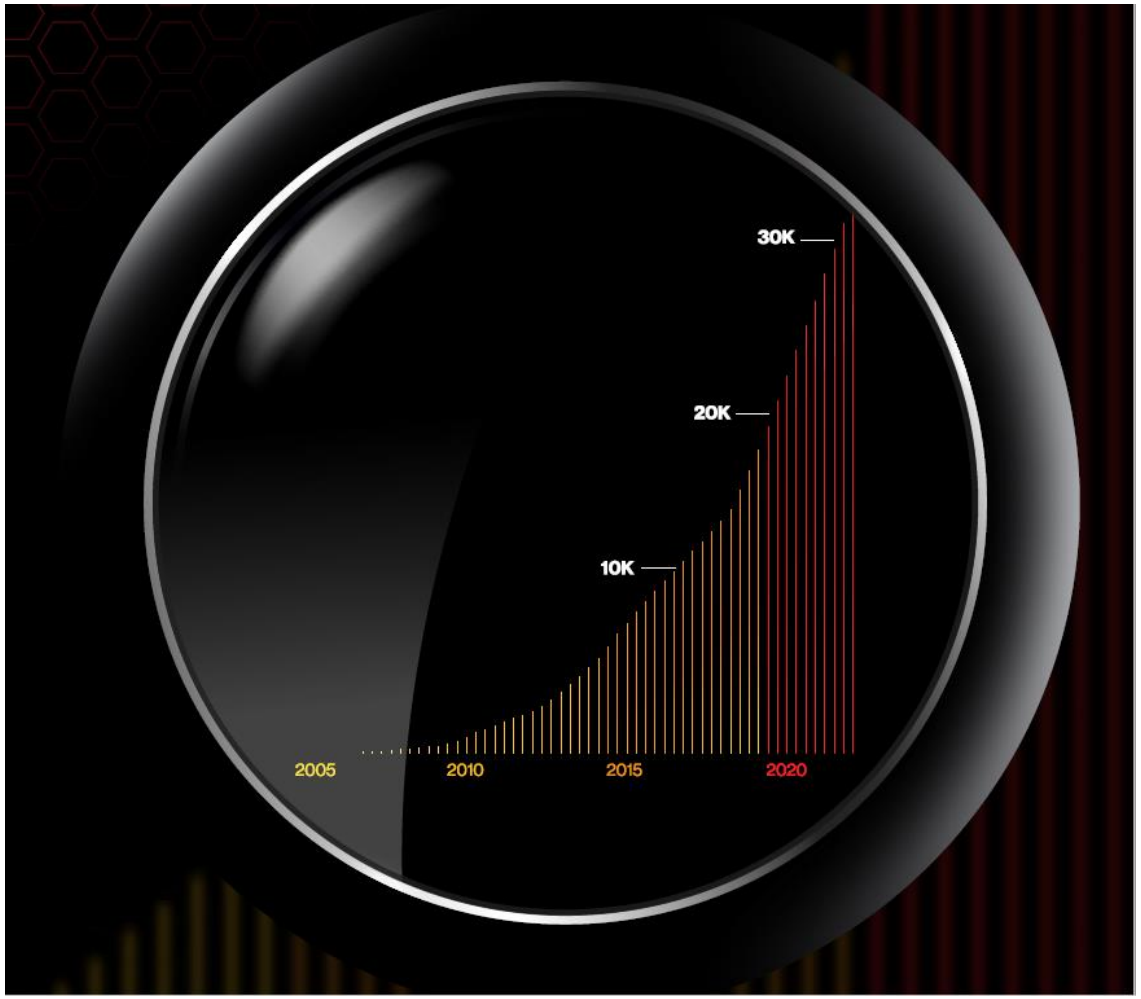
There have been `820` posts within the year of 2024

There have been `12890` posts since the dawn of ransomlook

There are `99` custom parsers indexing posts

Verizon Data Breach Investigations Report (16th Edition)

- 16,312 security incidents that compromised the integrity, confidentiality or availability of an information asset.
- 5,199 breaches that resulted in the confirmed disclosure of data to an unauthorised party.
- *Total Set*
  - *953,894 incidents*
  - *254,968 breaches*



verizon.com/dbir

What Verizon Found – Key Statistics

- **74%** of all breaches include the human element

  Error, Privilege Misuse, stolen credentials or Social Engineering

- **50%** of all Social Engineering incidents used pretexting

  An invented scenario that tricks someone, that may result in a breach

- **24%** of all breaches involved ransomware

  Maliciously encrypting data and demanding a ransom to return or unlock it

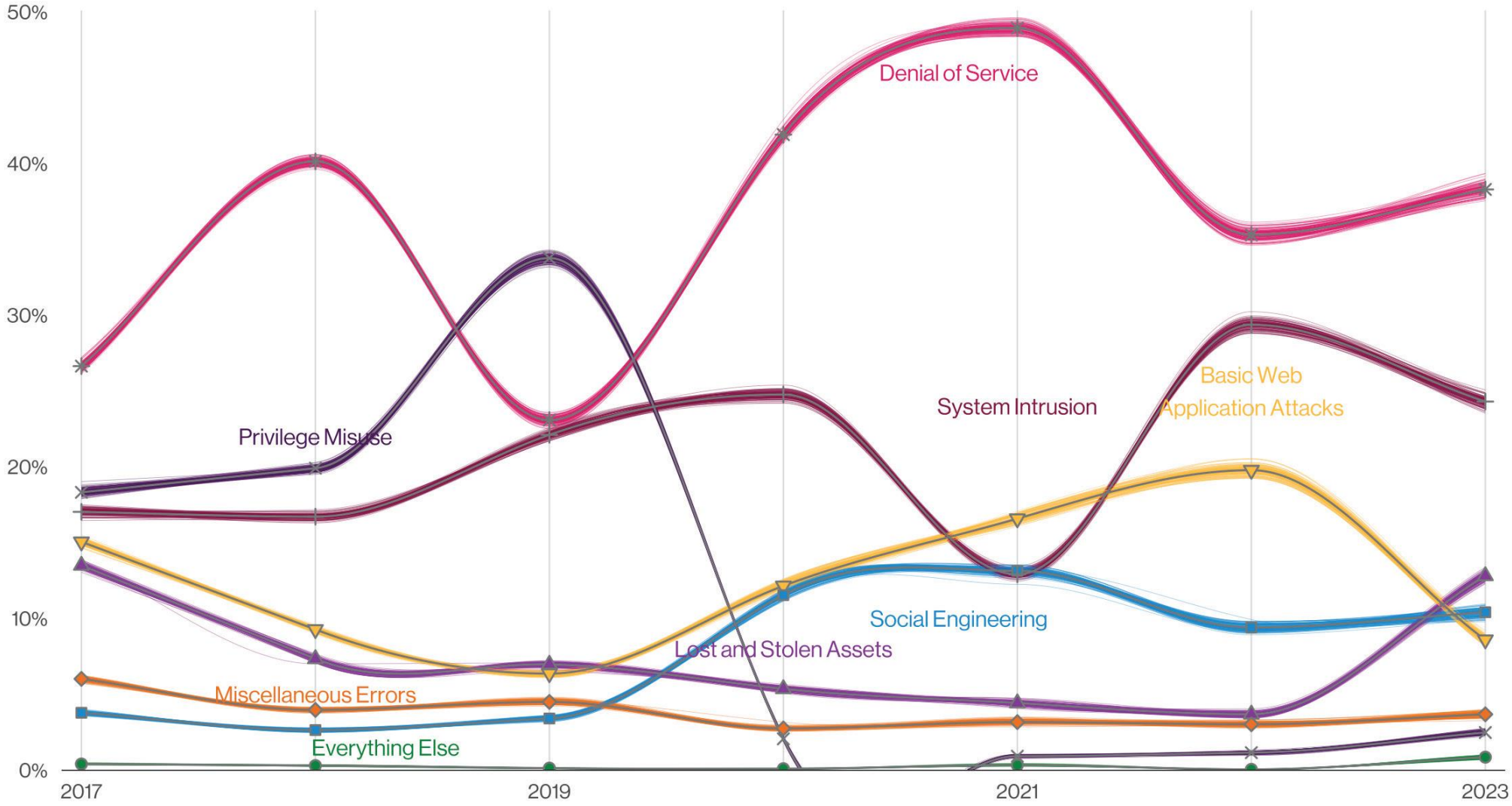
- **19%** involved internal actors

  Intentional and unintentional harm through misuse and simple human errors

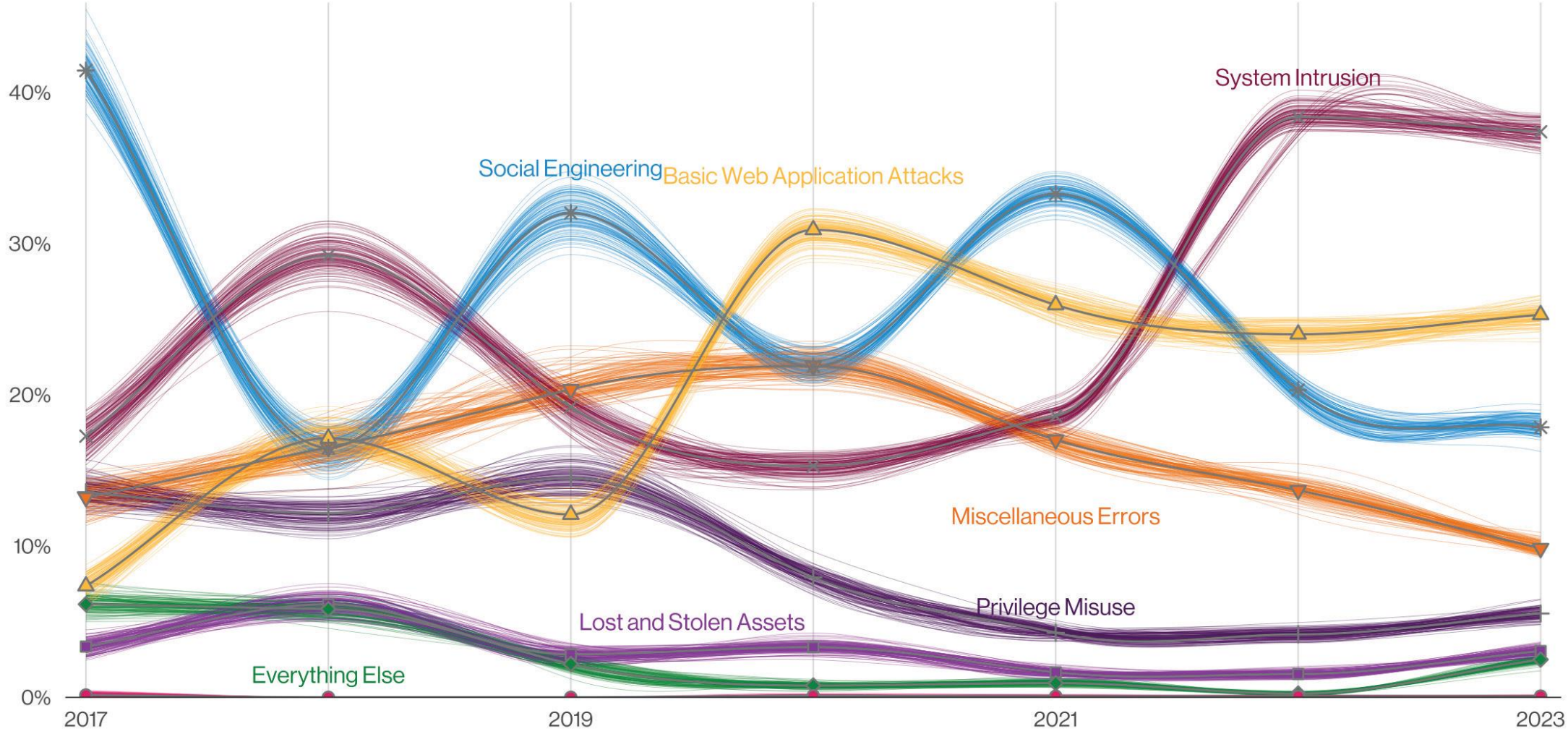
- **95%** of breaches are financially driven

  It's (almost) always about the money

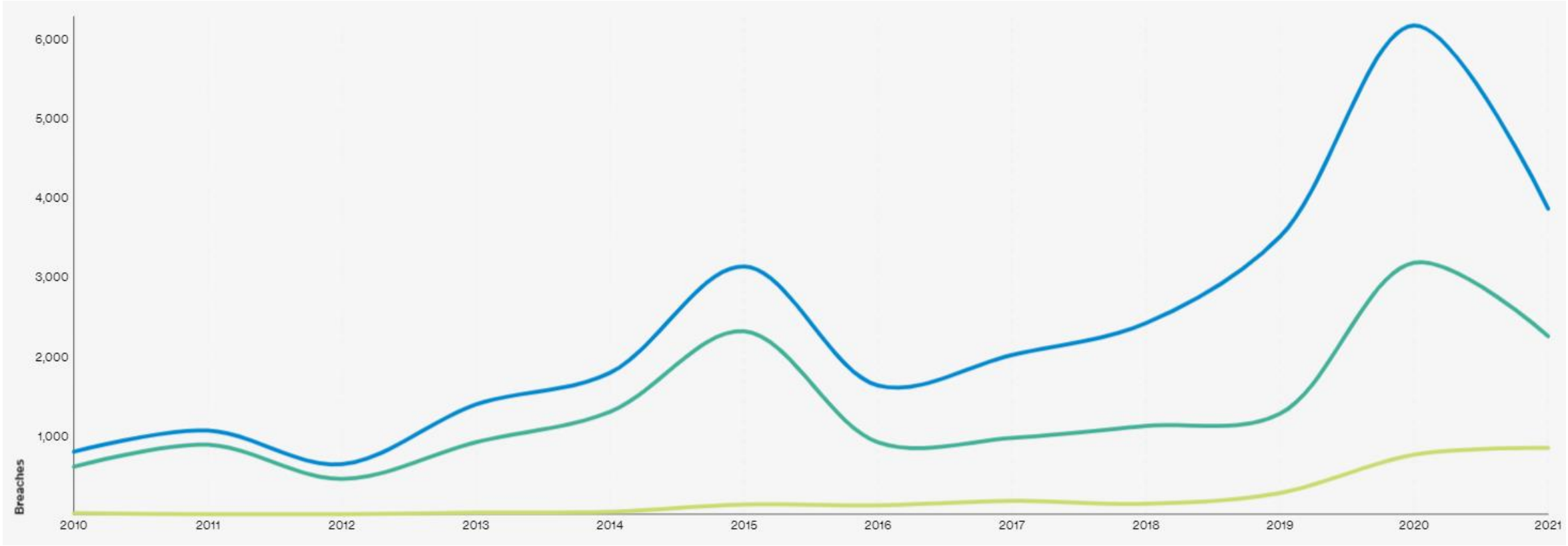
Patterns over time in incidents



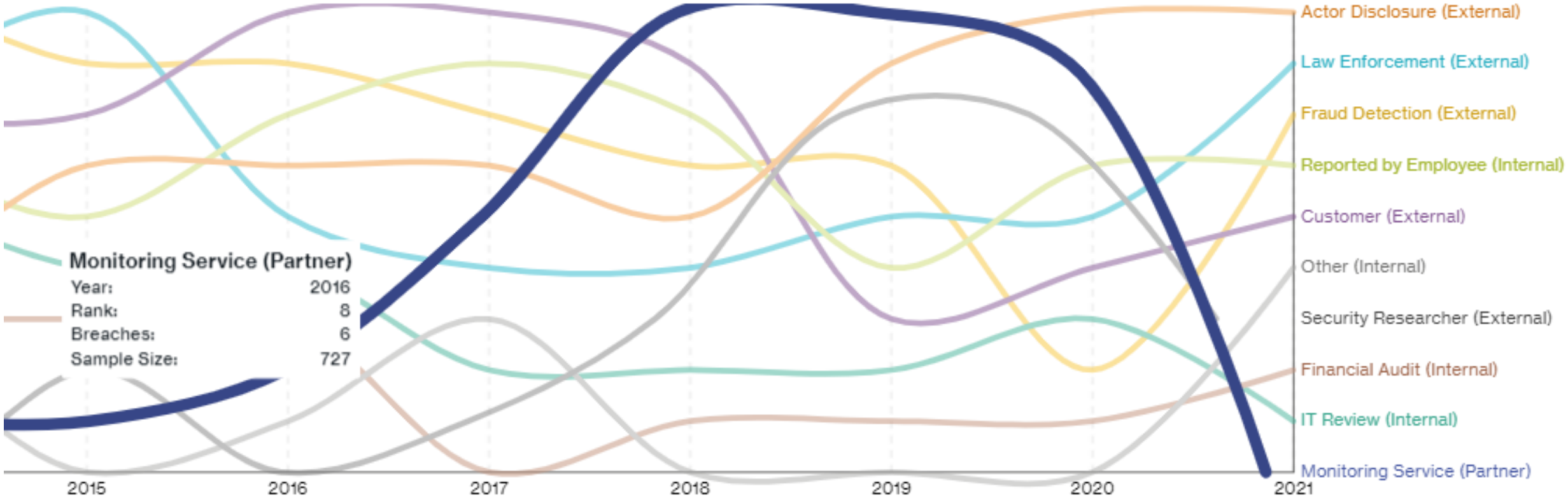
Patterns over time in breaches



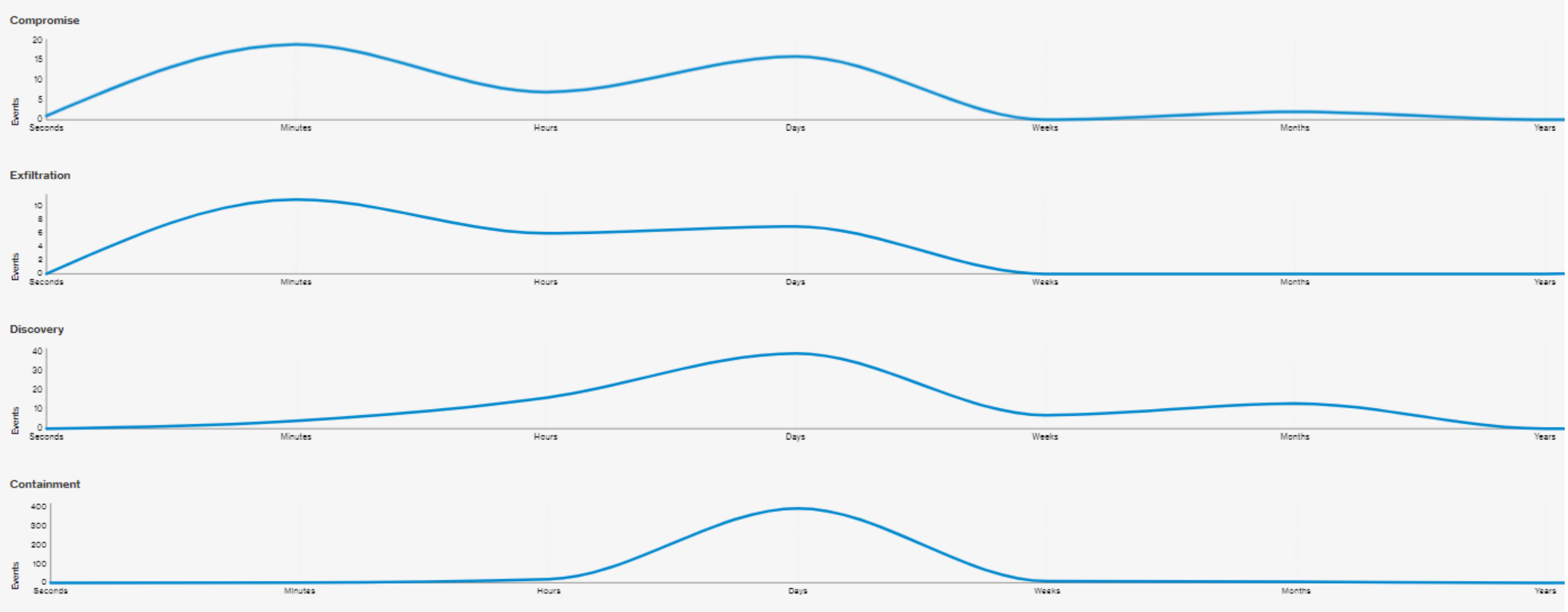
What Verizon Found - Breach Trends (15th Edition)



Discovery Methods Used Over Time (15th Edition)



Response Time For Breach Events – 2021 (15th Edition)



MITRE ATT&CK®

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 39 techniques	Credential Access 15 techniques	Discovery 27 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning ≡	Acquire Infrastructure ≡	Valid Accounts ≡	Scheduled Task/Job ≡			Modify Authentication Process ≡	System Service Discovery	Remote Services ≡	Data from Local System	Data Obfuscation ≡	Exfiltration Over Other Network Medium ≡	Data Destruction
Gather Victim Host Information ≡	Compromise Accounts ≡	Replication Through Removable Media	Windows Management Instrumentation	Valid Accounts ≡		Network Sniffing	Software Deployment Tools	Data from Removable Media	Fallback Channels	Data Encrypted for Impact
Gather Victim Identity Information ≡	Compromise Infrastructure ≡	Trusted Relationship	Software Deployment Tools	Hijack Execution Flow ≡		OS Credential Dumping ≡	Application Window Discovery	Replication Through Removable Media	Input Capture ≡	Application Layer Protocol ≡	Scheduled Transfer	Service Stop
Gather Victim Network Information ≡	Develop Capabilities ≡	Supply Chain Compromise ≡	Shared Modules	Boot or Logon Initialization Scripts ≡	Direct Volume Access	Input Capture ≡	System Network Configuration Discovery ≡	Internal Spearphishing	Data Staged ≡	Proxy ≡	Data Transfer Size Limits	Inhibit System Recovery
Gather Victim Org Information ≡	Establish Accounts ≡	Hardware Additions	User Execution ≡	Create or Modify System Process ≡	Rootkit	Brute Force ≡	System Owner/User Discovery	Use Alternate Authentication Material ≡	Email Collection ≡	Communication Through Removable Media	Exfiltration Over C2 Channel	Defacement ≡
Phishing for Information ≡	Obtain Capabilities ≡	Exploit Public-Facing Application	Exploitation for Client Execution	Event Triggered Execution ≡	Obfuscated Files or Information ≡	Two-Factor Authentication Interception	System Network Connections Discovery	Lateral Tool Transfer	Clipboard Data	Web Service ≡	Exfiltration Over Physical Medium ≡	Firmware Corruption
Search Closed Sources ≡	Stage Capabilities ≡	Phishing ≡	System Services ≡	Boot or Logon Autostart Execution ≡		Exploitation for Credential Access	Permission Groups Discovery ≡	Taint Shared Content	Automated Collection	Multi-Stage Channels	Exfiltration Over Web Service ≡	Resource Hijacking
Search Open Technical Databases ≡		External Remote Services	Command and Scripting Interpreter ≡	Account Manipulation ≡	Process Injection ≡	Steal Web Session Cookie	File and Directory Discovery	Exploitation of Remote Services	Audio Capture	Ingress Tool Transfer	Automated Exfiltration ≡	Network Denial of Service ≡
Search Open Websites/Domains ≡		Drive-by Compromise	Native API	External Remote Services	Access Token Manipulation ≡	Unsecured Credentials ≡	Peripheral Device Discovery	Remote Service Session Hijacking ≡	Video Capture	Traffic Signaling ≡	Exfiltration Over Alternative Protocol	Endpoint Denial of Service ≡
Search Victim-Owned Websites			Inter-Process Communication ≡	Create Account ≡	Abuse Elevation Control Mechanism ≡	Credentials from Password Stores ≡	Network Share Discovery		Man in the Browser	Data Encoding ≡	Transfer Data to Cloud Account	System Shutdown/Reboot
			Container Administration Command	Browser Extensions	Domain Policy Modification ≡	Steal or Forge Kerberos Tickets ≡	Password Policy Discovery		Data from Information Repositories ≡	Remote Access Software		Account Access Removal
			Deploy Container	Traffic Signaling ≡	Escape to Host	Forced Authentication	Browser Bookmark Discovery		Man-in-the-Middle ≡	Dynamic Resolution ≡		Disk Wipe ≡
				BITS Jobs	Exploitation for Privilege Escalation	Steal Application Access Token	Virtualization/Sandbox Evasion ≡		Archive Collected Data ≡	Non-Standard Port		Data Manipulation ≡
				Server Software Component ≡		Man-in-the-Middle ≡	Cloud Service Dashboard		Data from Network Shared Drive	Protocol Tunneling		
				Pre-OS Boot ≡		Forge Web Credentials ≡	Software Discovery ≡		Data from Cloud Storage Object	Encrypted Channel ≡		
				Compromise Client Software Binary			Query Registry		Data from Configuration Repository ≡	Non-Application Layer Protocol		
				Implant Container Image			Remote System Discovery					
				Modify Authentication Process ≡			Network Service Scanning					
							Process Discovery					
							System Information Discovery					
							Account Discovery ≡					
							System Time Discovery					
							Domain Trust Discovery					
							Cloud Service Discovery					
							Container and Resource Discovery					
							Cloud Infrastructure Discovery					
							System Location Discovery					
						Indicator Removal on Host ≡						
						Modify Registry						
						Trusted Developer Utilities Proxy Execution ≡						
						Traffic Signaling ≡						
						Signed Script Proxy Execution ≡						
						Rogue Domain Controller						
						Indirect Command Execution						
						BITS Jobs						
						XSL Script Processing						
						Template Injection						
						File and Directory Permissions Modification ≡						
						Virtualization/Sandbox Evasion ≡						
						Unused/Unsupported Cloud Regions						
						Use Alternate Authentication Material ≡						
						Impair Defenses ≡						
						Hide Artifacts ≡						
						Masquerading ≡						
						Deobfuscate/Decode Files or Information						
						Signed Binary Proxy Execution ≡						
						Exploitation for Defense Evasion						
						Execution Guardrails ≡						
						Modify Cloud Compute Infrastructure ≡						
						Pre-OS Boot ≡						
						Subvert Trust Controls ≡						
						Build Image on Host						
						Deploy Container						
						Modify System Image ≡						
						Network Boundary Bridging ≡						
						Weaken Encryption ≡						

≡ Has sub-techniques

MITRE ATT&CK®
Enterprise Framework

attack.mitre.org

MITRE ATT&CK® - Trickbot

Technology Supply Chain Management

The House Loses: Caesar's Entertainment paid a ransom after being cyberattacked. GETTY

Within weeks, two of the world's largest casino-hotel companies—MGM Resorts and Caesars—were hit with ransomware attacks. One met the hackers' demands, while the other is resisting.

ALPHV reportedly bragged that it took 10 minutes to infiltrate MGM's system after identifying an MGM tech employee on LinkedIn and then calling the company's support desk.

Scattered Spider gained entry to Caesars' system by deceiving an employee at a third-party vendor.

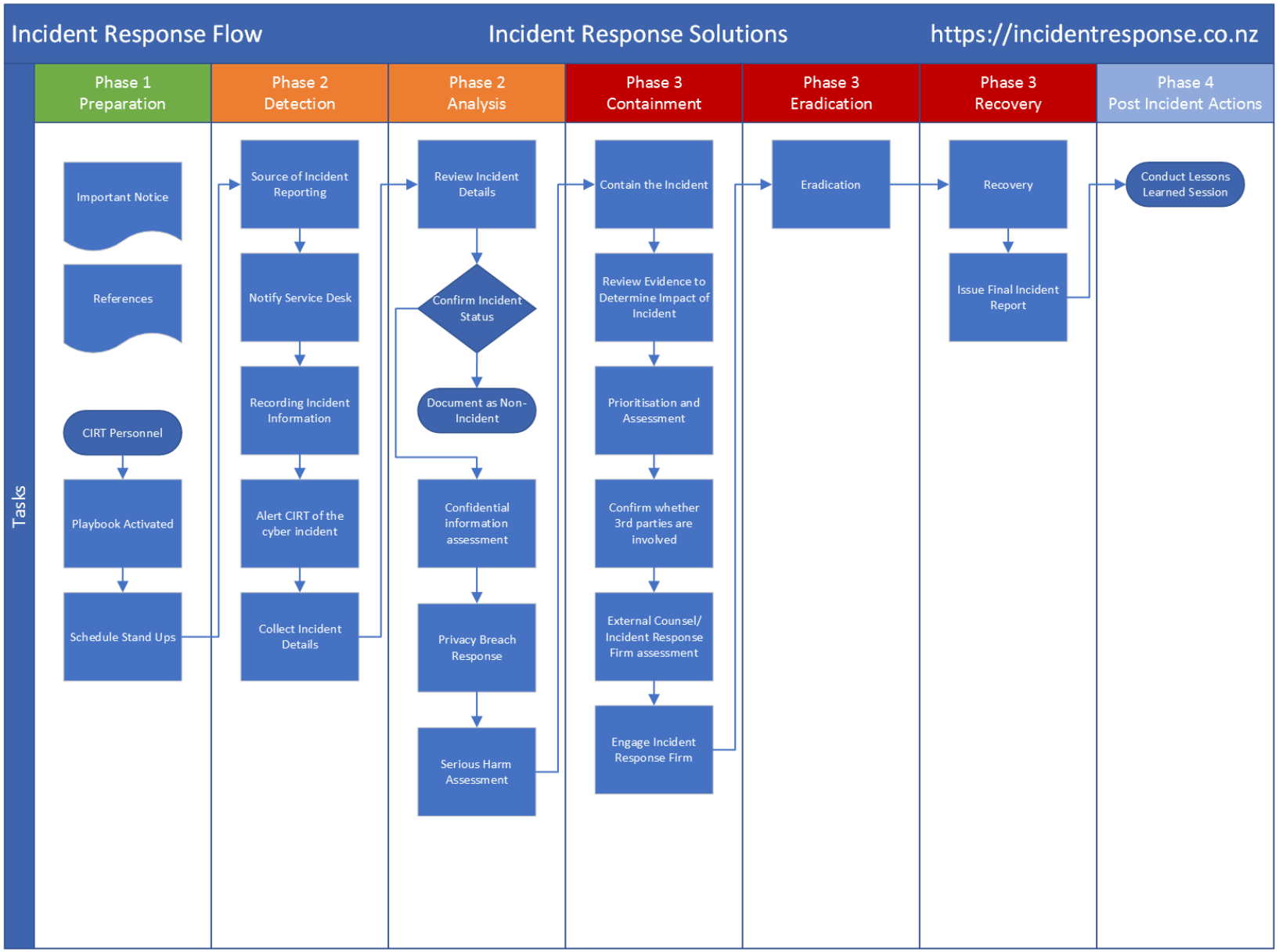
Cyber Governance and Risk Management - Controls

Cyber Risk Management – Security Awareness and Skills Training

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		●	●

Incident Response Plans and Simulations



What services our IT / MSP clients are engaging in

- Cyber Governance
- Cyber IR plans and testing
- Breach response
  - Incident controller
  - Data Breach assessment (DART)
  - Communications
  - Ransomware response
  - Dark web and data leak monitoring
- Forensic technology
- Hosting / eDiscovery / GPT “ASK”

Thank you

Campbell McKenzie

0800 WITNESS or 021 779 310
campbell@incidentresponse.co.nz

incidentresponse.co.nz
whistleblowers.co.nz

https://incidentresponse.co.nz/demos
Password: *Bulletin*

Incident Response
FORENSIC & CYBER