

Lessons From the Front Line of the Cyber Zone

3rd May 2019

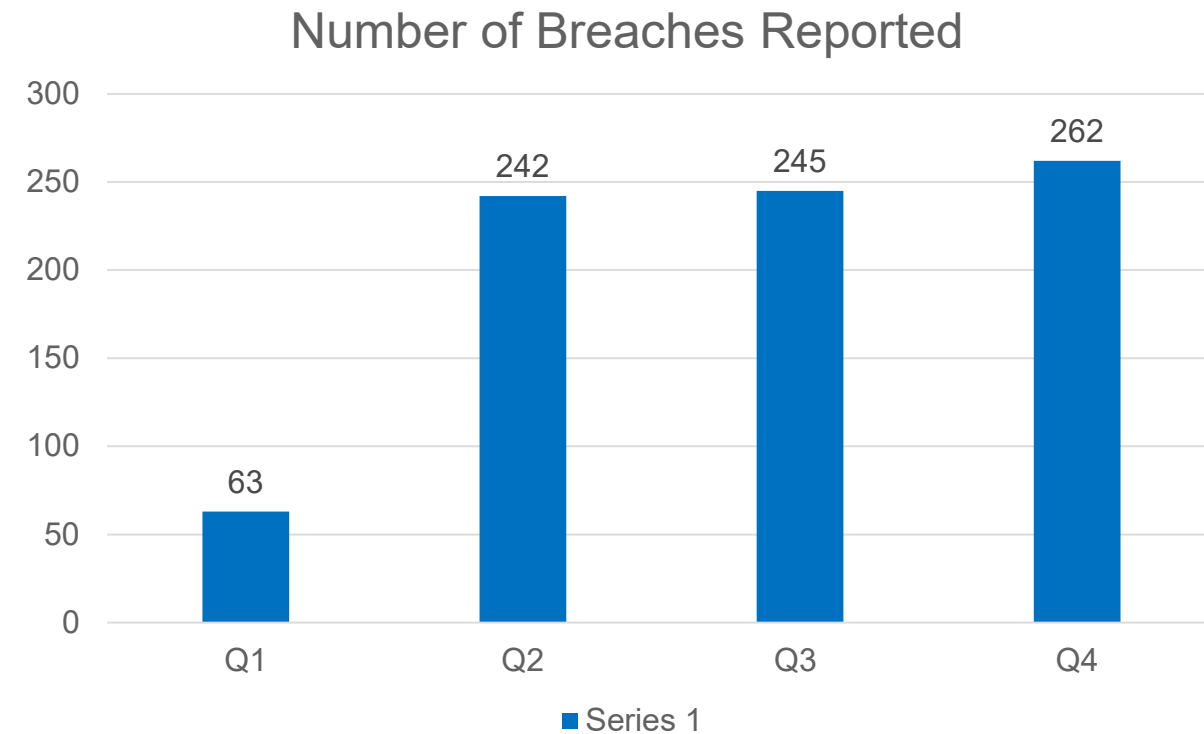


ES2 Capabilities



1 Year of NDB Legislation

OAIC have now produced four quarterly Notifiable Data Breach (NDB) reports providing almost a full year of breach data.



1 Year of NDB Legislation

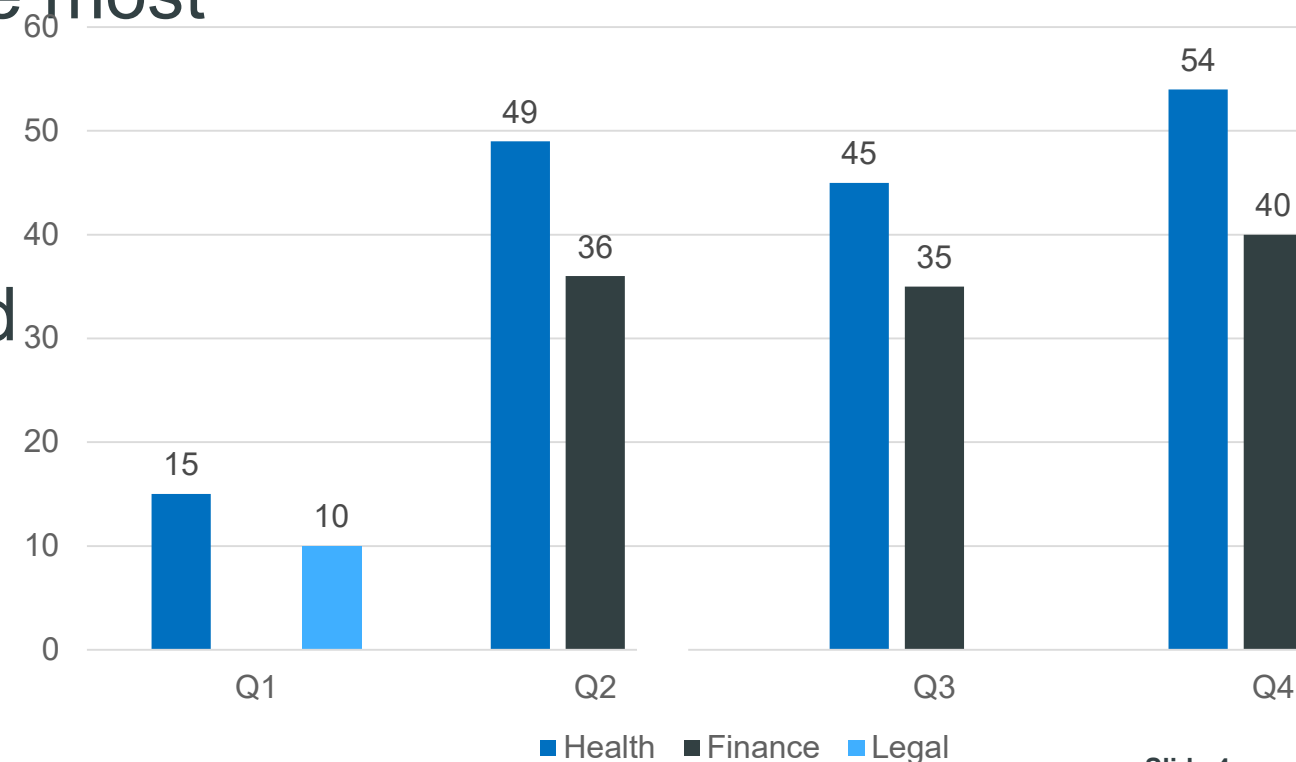
With the exception of the first (incomplete) quarter.

The Health sector (H) has had the most notifiable breaches.

Finance sector (F) is close behind

Then Legal (L), then Education

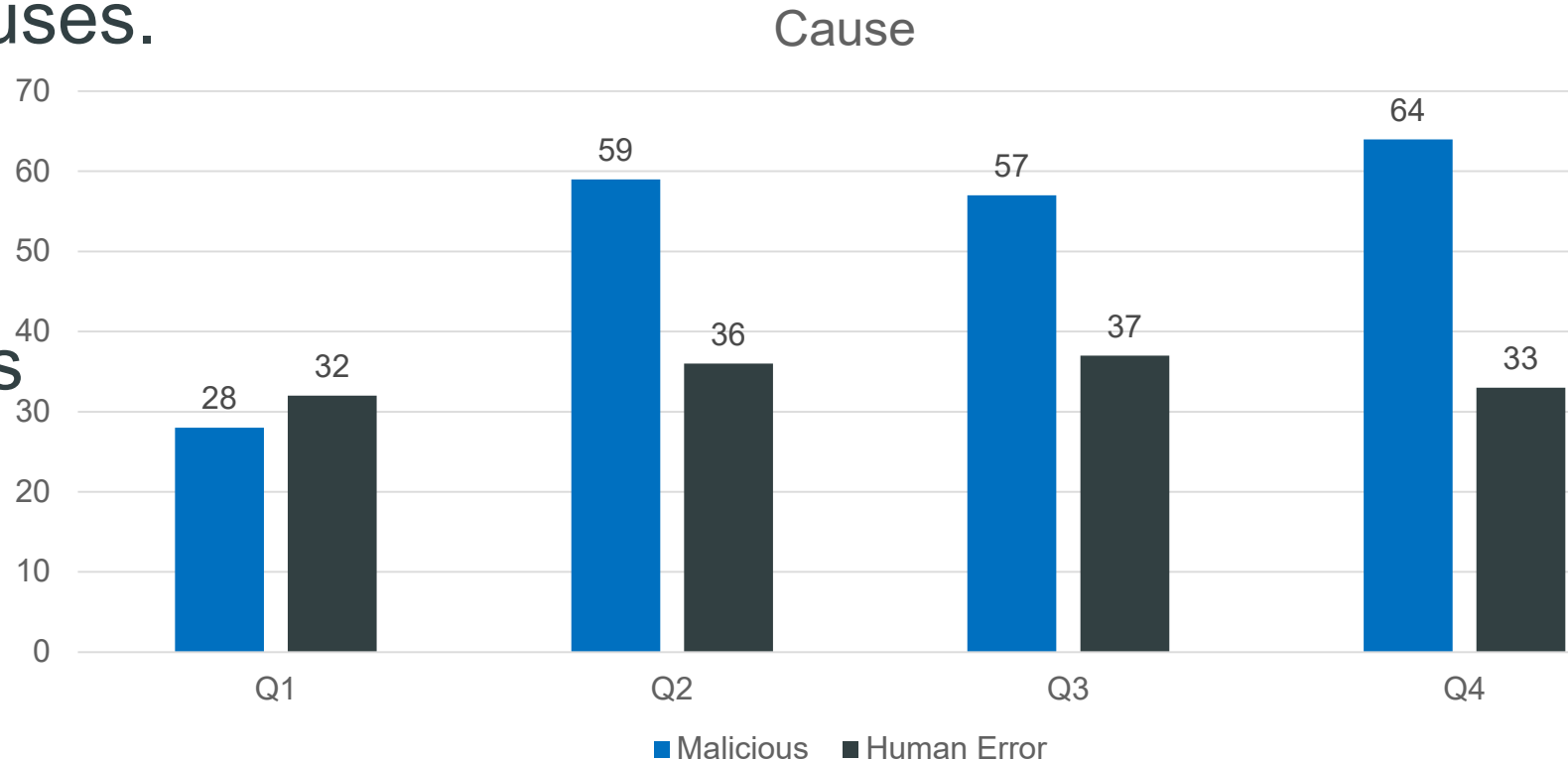
Breaches by Industry Sector



1 Year of NDB Legislation

Across all quarters Malicious attacks (M) and Human Error (E) make up the largest percentage of breach causes.

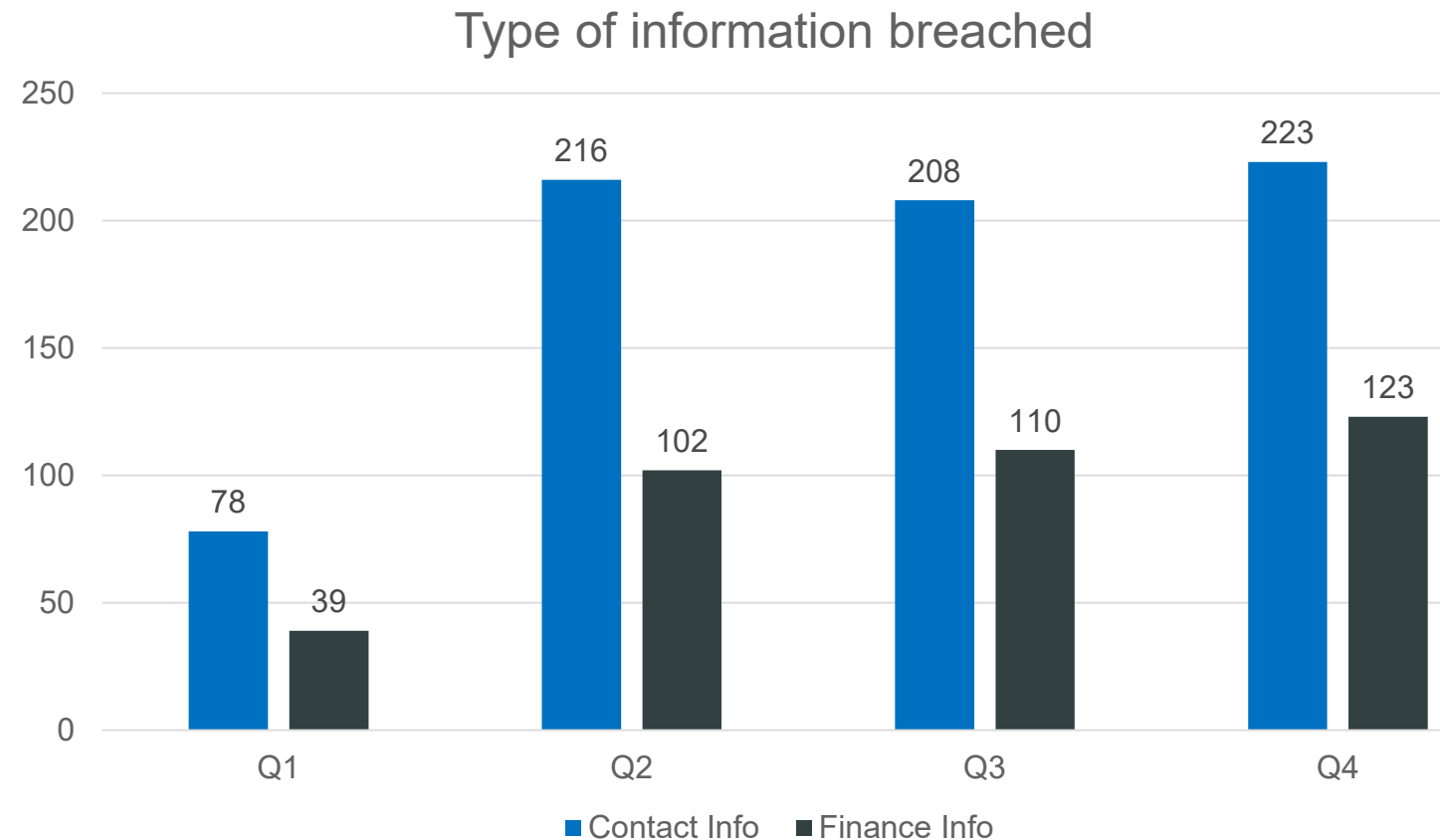
The highest percentage attributed to system faults is only 6%.



1 Year of NDB Legislation

The information that is most often breached is:

- Contact Information (C)
- Financial Information (F)



ES2 Incident Response Services



1800 373 732
(1800 ES2 SEC)



24x7 Incident
Response Hotline

Open discussions
to establish
situation

Incident analysed

Logs and
malware
analysed

Remediation
recommendations

Post-incident
Reporting

Incident Response Types

- Advisory (CxO)
- Onsite Response
- Forensic Analysis
 - Malware Analysis
 - File Analysis
 - Log Analysis
- System Backups / Restorations
- Technology Remediation (Policy / Controls)
- Technology Implementation (SIEM / NGFW / EDR / AI)

Threat Intelligence: Indicators and TTPs

Indicator: A set of cyber observables combined with contextual information intended to represent artefacts and/or behaviours of interest within a cyber security context. Commonly referred to as indicators of compromise (IOCs)

TTP: Commonly referred to as **Tactics, Techniques and Procedures** are the representations of the behaviour or modus operandi of cyber adversaries. It is a term taken from the traditional military sphere and is used to characterise what an adversary does and how they do it in increasing levels of detail.

“patterns of activities or methods associated with a specific threat actor or group of threat actors”

Example Indicators

- Unusual Outbound Network Traffic
- Anomalies In Privileged User Account Activity
- Geographical Irregularities
- Other Log-In Red Flags
- Swells In Database Read Volume
- HTML Response Sizes
- Large Numbers Of Requests For The Same File
- Mismatched Port-Application Traffic
- Suspicious Registry Or System File Changes
- DNS Request Anomalies

Tactics (Tools)

- Phishing Attacks
- SQL Injection Attacks (SQLi)
- Cross-Site Scripting (XSS)
- Man-in-the-Middle (MITM)
- Malware
- Denial-of-Service
- Spear Phishing
- Whaling Phishing
- Brute-Force and Dictionary

Techniques

- Espionage and foreign interference
- Theft or Loss of Devices
- PII Breach
- Data Breach
- DDoS (Distributed Denial of Service)
- Ransom / Extortion
- Financial Fraud
- Unauthorised Access

Procedures

- Reconnaissance
- Enumerating exposed systems
- Gather contact details
- Third Party Compromise
- Email Account Takeover
- Identify Vulnerabilities
- Social Data Mining
- Obtain Exploits & Zero Days
- Malware Execution
- Detect and evade sandbox or heuristic analysis
- Deploy persistence
- C&C Communications

Incident

A large Western Australia-based organisation was subject to a cyber security breach followed by an extortion attempt.

Response

Engaged as the first responder to assist the in house IT team as advisors and to conduct the forensic collection of log data and system data.

Data Breach and Extortion

Tactics, Techniques and Procedures



Post-Incident

SIEM Implementation, Multi-Factor Authentication, Dark Web monitoring, 24/7 Monitoring

Incident

A skilled hacker in Asia stole sensitive security details and building plans from a WA organisation after breaking into its computer systems.

Response

ES2 were engaged as a Second responder to assist the IT team as advisors and to conduct the forensic collection of log data and system data.

Tactics, Techniques and Procedures



Post-Incident

SIEM Implementation, Network Segmentation, Application Whitelisting, Privilege Access Management, Multi-Factor Authentication, 24/7 Monitoring, Improved third party processes

Incident

Team of cybercriminals launched multiple malware attacks on a Perth based resources company before completing a sophisticated Network Breach, using a combination of Ransomware, Malware and Data Extraction.

Response

ES2 were engaged as a First responder to assist the IT team with advisory, and implementation/ remediation of Technical Controls

Data Breach & Ransomware

Tactics, Techniques and Procedures



Post-Incident

Network Segmentation, Application Whitelisting, Privilege Access Management, Multi-Factor Authentication, Privileged Access control, Authentication, system restoration in the cloud, data restoration from old back

Incident

NFP organisations Executive spotted unusual email activity on his account and identified spurious purchases being made using corporate credit card.

Response

ES2 were engaged as a First responder to assist the IT team with advisory and forensic collection of log data and system data.

Tactics, Techniques and Procedures



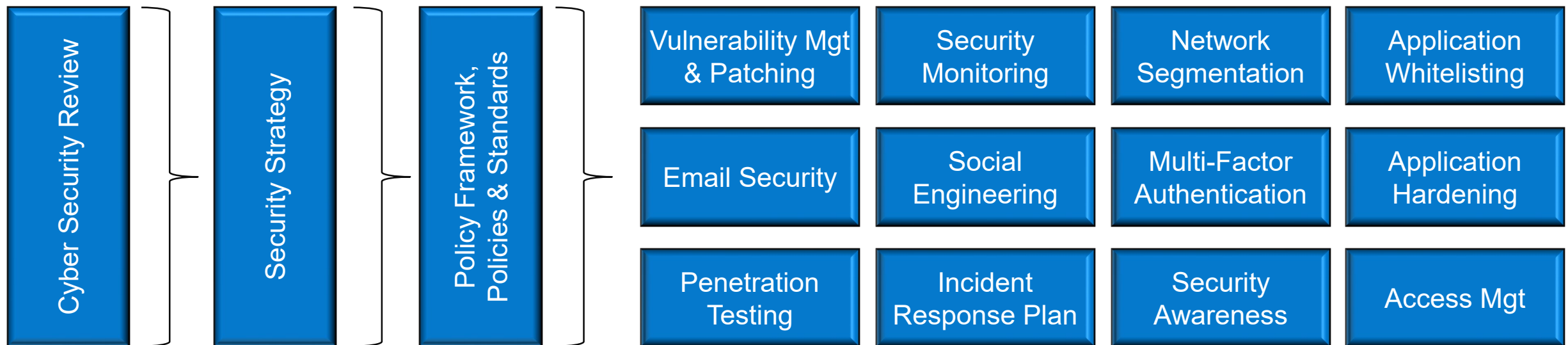
Post-Incident


Multi-Factor Authentication, Improved auditing and logging, Improved password procedures

- 1) Email Account Takeover → Financial Impact
- 2) Ransomware → Data Loss
- 3) Data Breach → Brand Damage
- 4) Malware Attack → Downtime
- 5) DDoS → Brand Damage / Downtime

- Maintaining a minimum of 90 days worth of resilient System and/or **Data Backups** will reduce the impact of a Cyber Attack.
- **Implementing Multi-Factor Authentication** to avoid Account takeovers and Impersonation attacks.
- Enable **Centralised Logging and Alarms** to prevent tampering and assist in investigations
- **Restricting Outbound Internet Access** from Privilege Users and Business Servers makes it harder for Threat Actors to exfiltrate data and download additional tools.
- Start **monitoring the Dark Web** for exposed Corporate Accounts and company data to provide faster response times.

ES2 Recommended Roadmap



[Home](#)[Notify me](#)[Domain search](#)[Who's been pwned](#)[Passwords](#)[API](#)[About](#)[Donate](#) 

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

By Kids For Kids

ES2 Kids is a Not-for-Profit Foundation that assists in bridging the gap of Cyber Security Awareness for K-12 kids.



ES2 Kids focus is to facilitate Cyber Security Awareness from the Private and Government sectors to K-12 kids (and their parents ...)





By Kids For Kids

ES2 Kids Q+A

Steve Simpson & Heidi Drouin

Thank you

Fred@ES2.com.au

Steve@ES2.com.au

Info@ES2kids.com.au