Aon Cyber Solutions Group

Ransomware Info Session

Our Community

March 2024

Today’s Agenda

1. Introduction (CSG)
2. Cyber Risk Landscape
3. Major types of cyber attacks
4. Un-packing Ransomware
5. Risk Mitigation & Risk Transfer
6. Claim Scenario Mapping
7. Q&A

Introduction - CSG

Salman Khokhar

Client Manager, Cyber Solutions Group

Over 10 years' experience in Financial Lines Insurance including Cyber, Tech E&O, PI, and D&O.

Cyber Solutions Group

Part of Financial Specialties Group assisting with broking and placement of cyber programs for Aon’s Global and Corporate and Financial Services Group clients.

Consulting arm provides cyber risk consulting services Limit Adequacy and Loss Quantification.

Cyber Risk Landscape

Evolving at rapid pace

Attack Trends & Predictions

- **Ransomware continues to be no. 1 threat;** data exfiltration is at an all-time high.
- **Business Email Compromise** increasing in severity
- Uplift in software **supply chains attacks,** cloud and OS events
- **Australia Trends** – Optus, Medibank, Latitude, and HWLE breaches demonstrating increased frequency & reputational harm risk. New gov. offensive operation ASD & AFP

Regulatory Reform

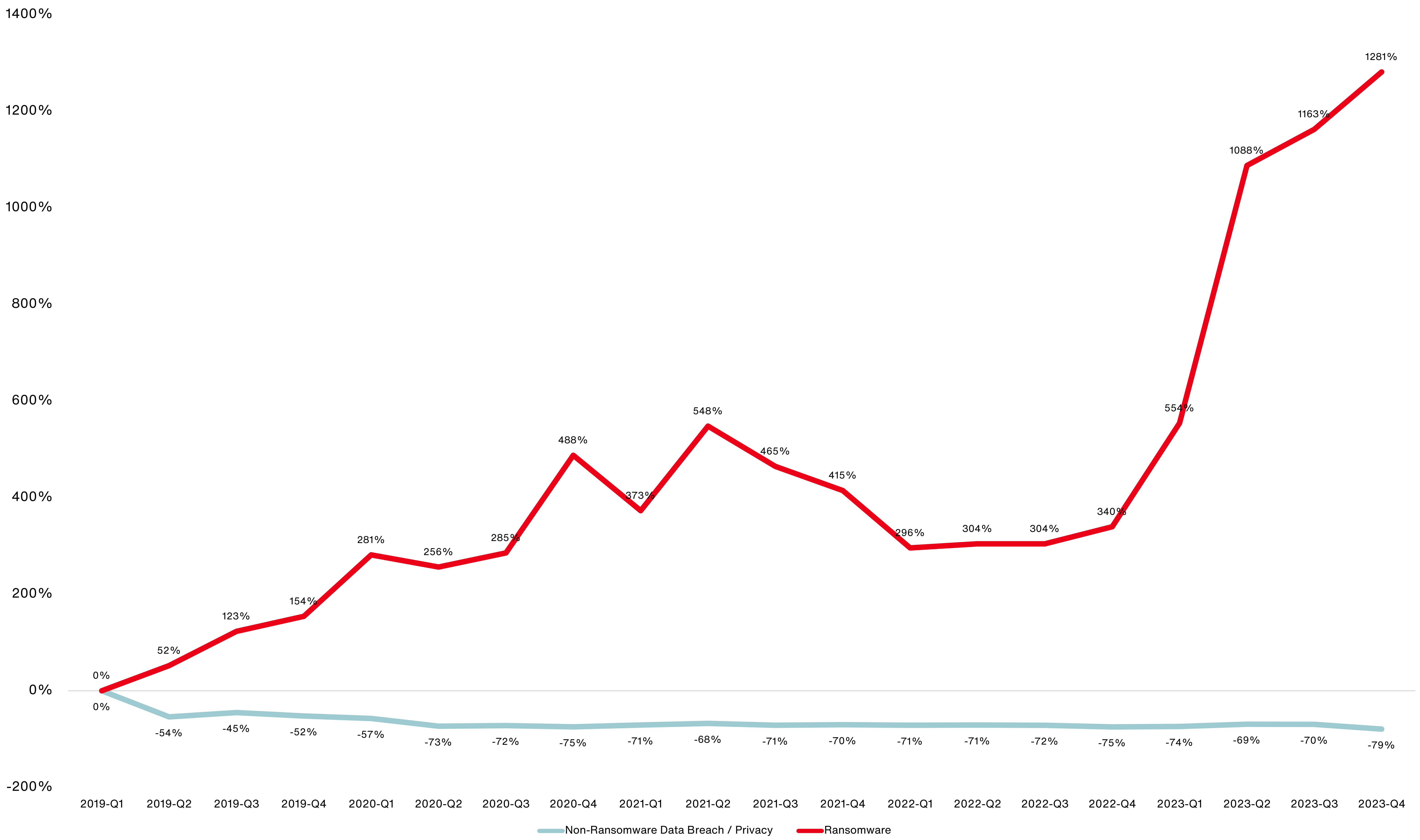
- Review of the **Privacy Act,** including **increased penalties** for serious or repeated breaches
- Increase in **OAIC** investigations and **new powers** to request information
- **Ransomware Action Plan,** plus review if paying will be illegal
- Increased scope of sectors for **Critical Infrastructure Act**

Macro-environment

- Increased media reporting locally
- **Hostile cyber activity**, escalated by Ukraine / Russia conflict
- Growing **digitalisation** increasing the attack surface
- **Hybrid / remote working**
- **Proliferation of emerging tech** (adoption of cloud, IoT, automatic, AI, quantum computing, blockchain)

AON

Cyber Incident Rates Indexed to Q1 2019



Source: Risk Based Security, analysis by Aon. Data as of 1/1/2024; Claim count development may cause these percentages to change over time

Proprietary & Confidential: The content, analysis and commentary included herein are understood to be the intellectual property of Aon. Further distribution, photocopying or any form of third-party transmission of this document in part or in whole, is not permitted without the express, written permission of Aon.

Key Observations:

- Ransomware activity has continued to **accelerate through Q4 2023**
- **Ransomware Events are up 1,281%** from Q1 2019 to Q4 2023
- Compared to Q3 2023:
  - Ransomware Events are up 9%
  - Non-Ransomware Data Breach/Privacy Events are down 32%
- The most commonly impacted industries by Ransomware in Q4 2023 were:
  - Business Professional Services
  - Manufacturing
  - Healthcare
  - Real Estate / Construction
  - Education
  - Public Entities

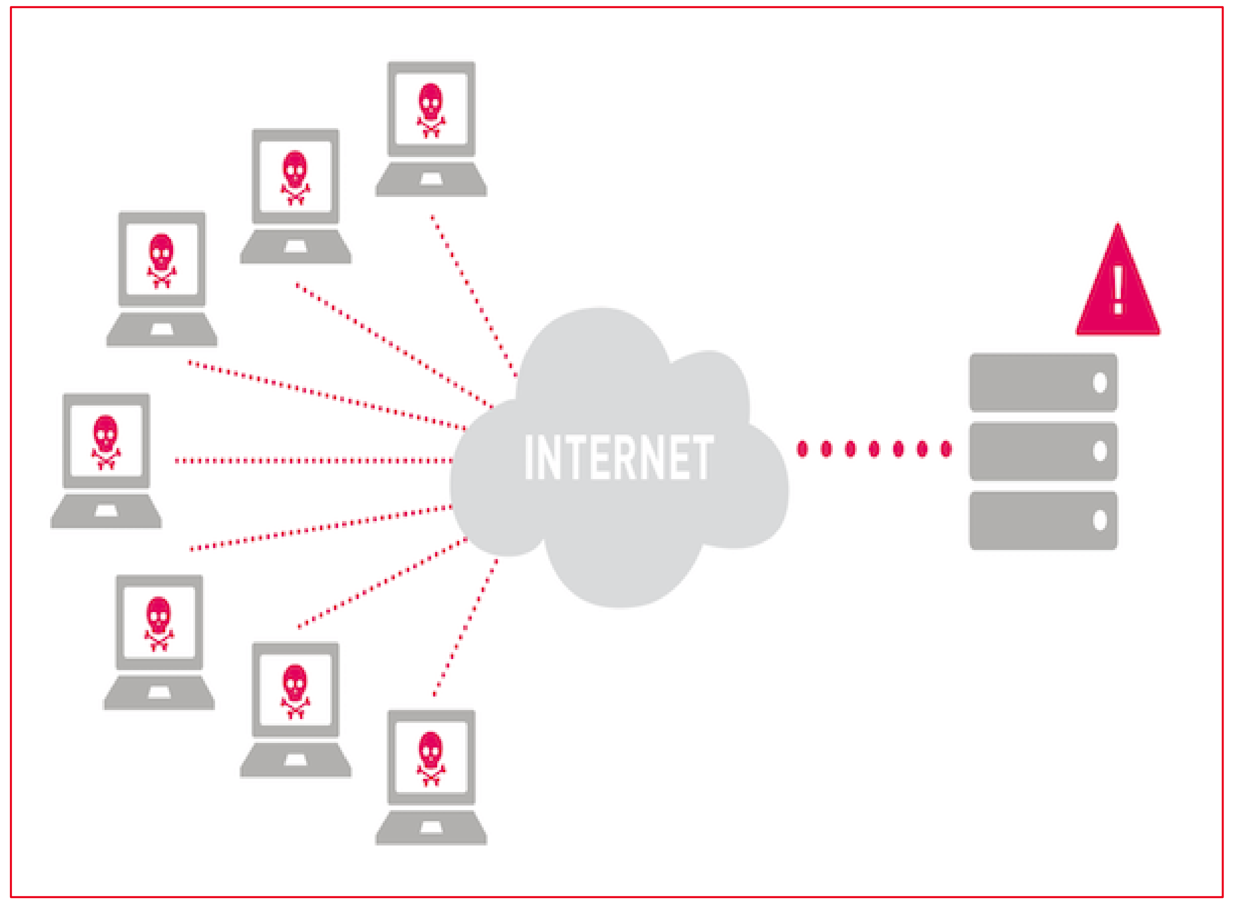
4 Major Types of Cyber Attacks

1. Ransomware/Malware: Ransomware is a common and dangerous type of **malware.** It works by locking up or encrypting your files so you can no longer access them, and the hacker demands you to pay a Ransom.

Deployment/Attack Vector: Malware is short for malicious software and is typically deployed via Phishing, however other attack vectors are also exploited e.g. known vulnerabilities in a software, stolen credentials, brute force, and physical access etc.

Examples: NotPetya, WannaCry, CryptoLocker, Emotet Trojan, Clop ransomware etc

2. Distributed Denial of Service (DDoS): A cyber-attack in which the hackers overwhelms a machine or network resource to a point that it becomes unavailable to its intended users either temporarily or indefinitely.



Deployment/Attack Vector: Large volume of Malicious traffic is directed to intended machine/server/network – often this traffic is generated via a network of malware infected botnets, and thus can be remotely controlled by the hacker.

Examples: 2020 AWS DDoS, 2018 Github DDoS, 2016 Dyn DDoS

4 Major Types of Cyber Attacks

2. Business Email Compromise: Email account credentials are stolen resulting in malicious use of this access to cause financial loss or retrieve more information/data via Social Engineering.

Deployment/Attack Vector: BEC attacks are typically conducted through Phishing emails using Social Engineering techniques.

Example: A legitimate looking email from Microsoft to reset your password where the intention is for the user to enter their existing credentials which are then fed back to the hacker without user realising they are hacked.

4. Network/Data Breach: A Hacker gains un-authorised access to a network or computer to steal or damage confidential or sensitive data retained by an individual or an organisation.

Deployment/Attack Vector: Exploiting existing vulnerabilities, malware (via Phishing), Stolen credentials (via Phishing or Dark Web), Unprotected servers or Databases, un protected open ports etc.

Example: Optus, Medibank, Latitude Financial etc.

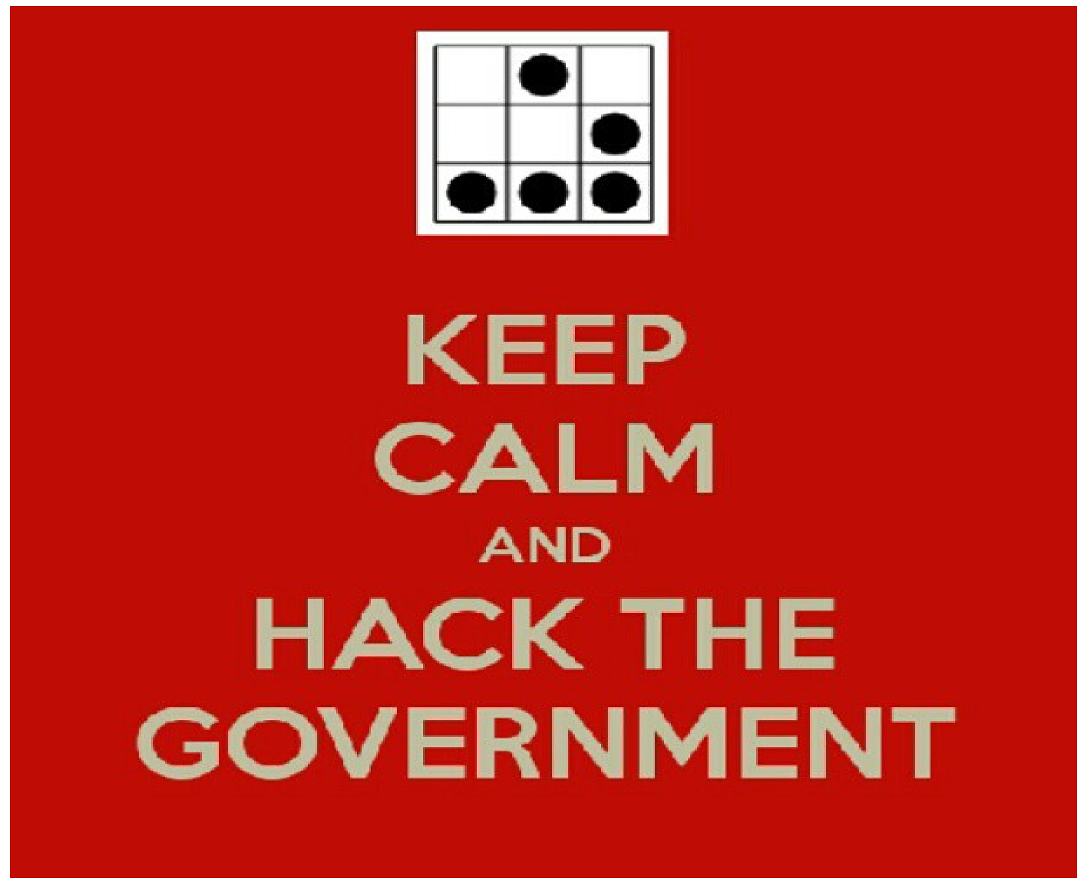
Un-packing Ransomware/Cyber Extortion

Ransomware/Malware:

Ransomware is a common and dangerous type of **malware.** It works by locking up or encrypting your files so you can no longer access them, and the hacker demands you to pay a Ransom.

RANSOMWARE ATTACK MOTIVATIONS

- It can be a matter of opportunity for a hacker e.g. an organisation that is easier to penetrate and holds large PII records
  - PII: Personally Identifiable Information e.g. Date of birth, License number, Financial/health info
- Some organisations make the Hacker's hit list due to their ability or the likelihood of paying a ransom e.g. Government organisation, Law firms etc, to ensure secrecy around their data being compromised.
- **NOTE:** Ransomware spreads automatically and indiscriminately across the internet, and more often than not it is an un-targeted campaign.



Risk Mitigation

Human Element:

"82% of breaches involve the human element". (Verizon DBIR Report 2022)

COMMONLY USED ATTACK VECTORS FOR INITIAL ACCESS

1. PHISHING

- **Training, Training, and more Training for staff awareness**

2. SYSTEM VULNERABILITIES

- **Keep systems up to date via Patching – reduce attack surface**

3. PRIVILEGED ESCALATION

- **Multi-factor Authentication across Privileged Access and Remote Access**

4. UNAUTHORISED MALICIOUS APPLICATIONS/WEBSITES

- **Web application firewall, Anti-virus, Application Whitelisting**

RANSOMWARE RESILIENCY

- Staff awareness training
- Good Backup controls i.e. Offline backups, more than one copy, and malware testing
- Ransomware table top exercises and restoration from Backups

Key Controls

Ransomware Mitigation

- Multi-Factor Authentication (MFA)
- Endpoint Detection and Response (EDR)
- Phishing Exercise/ Cyber Awareness Training
- Vulnerability Scanning & Patch Management
- Secure RDP/VPN
- Incident Response Plan/ Ransomware Exercise
- Access Control/ Service Accounts
- Disaster Recovery/Backups
- Email Filtering & Security (DMARC / DKIM)
- Zero Day Vulnerabilities and Supply Chain Risks
- Network Segmentation/ Network Monitoring
- M&A DD and Integration

AON

Risk Transfer

Key Pillars of a Cyber Insurance Policy

Prevention

- Pre-breach assessments
- Access to pre-vetted vendors
- Cybersecurity information

Assistance

- Forensic investigators
- Legal services
- Notification
- Credit Monitoring
- Call Center Services
- Crisis Management/ Public Relations

Operations

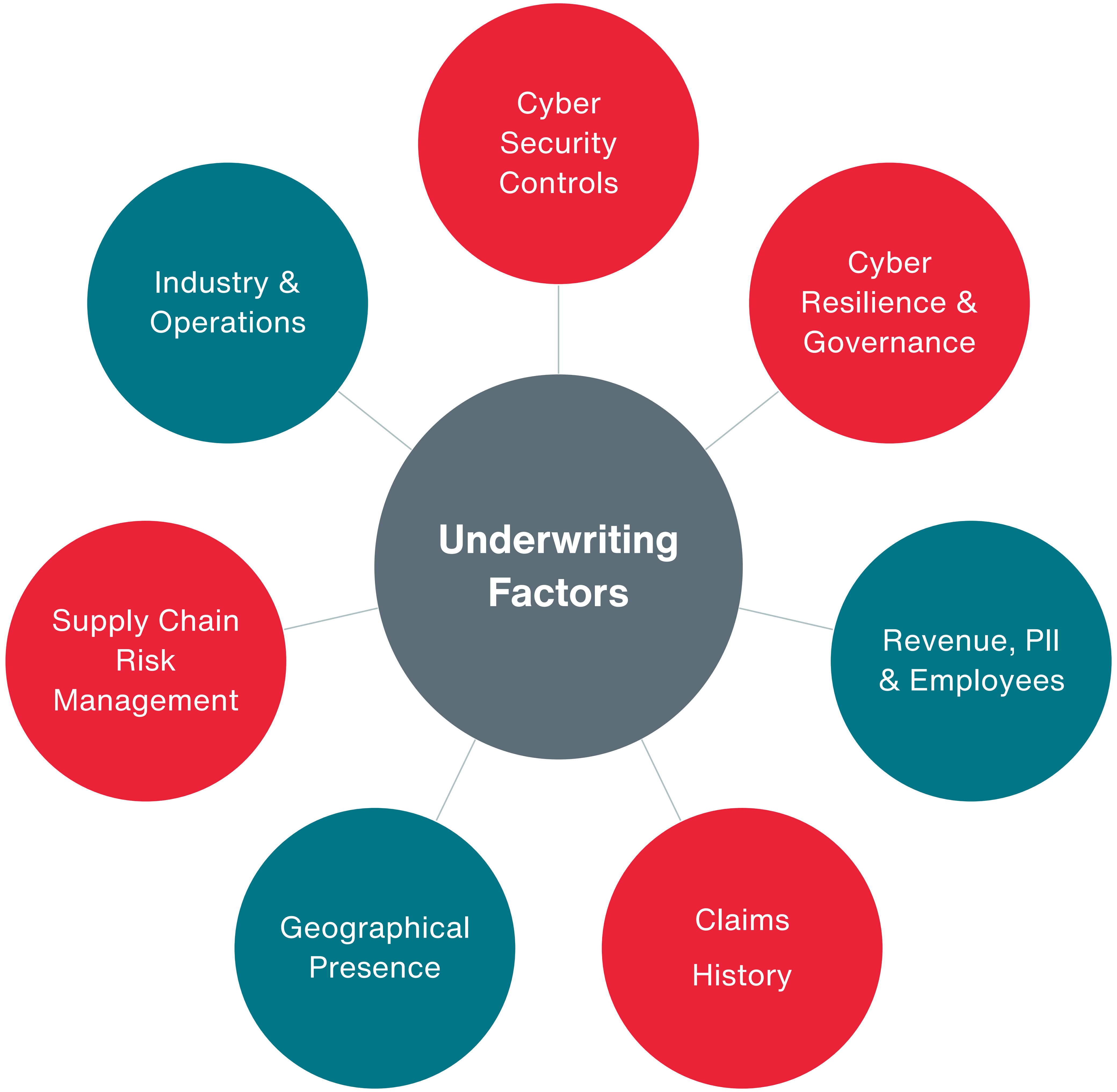
- Costs incurred to keep or return the business to operational
- Loss of revenue, income, turnover
- Costs incurred to recreate/restore data and information

Liability

- Legal costs and damages from claims alleging privacy breach or network security failure

Cyber Insurance

Underwriting Factors



Underwriting Factors

Cyber Security Controls

Cyber Resilience & Governance

Revenue, PII & Employees

Claims History

Geographical Presence

Supply Chain Risk Management

Industry & Operations

Claim Scenario

Ransomware Attack

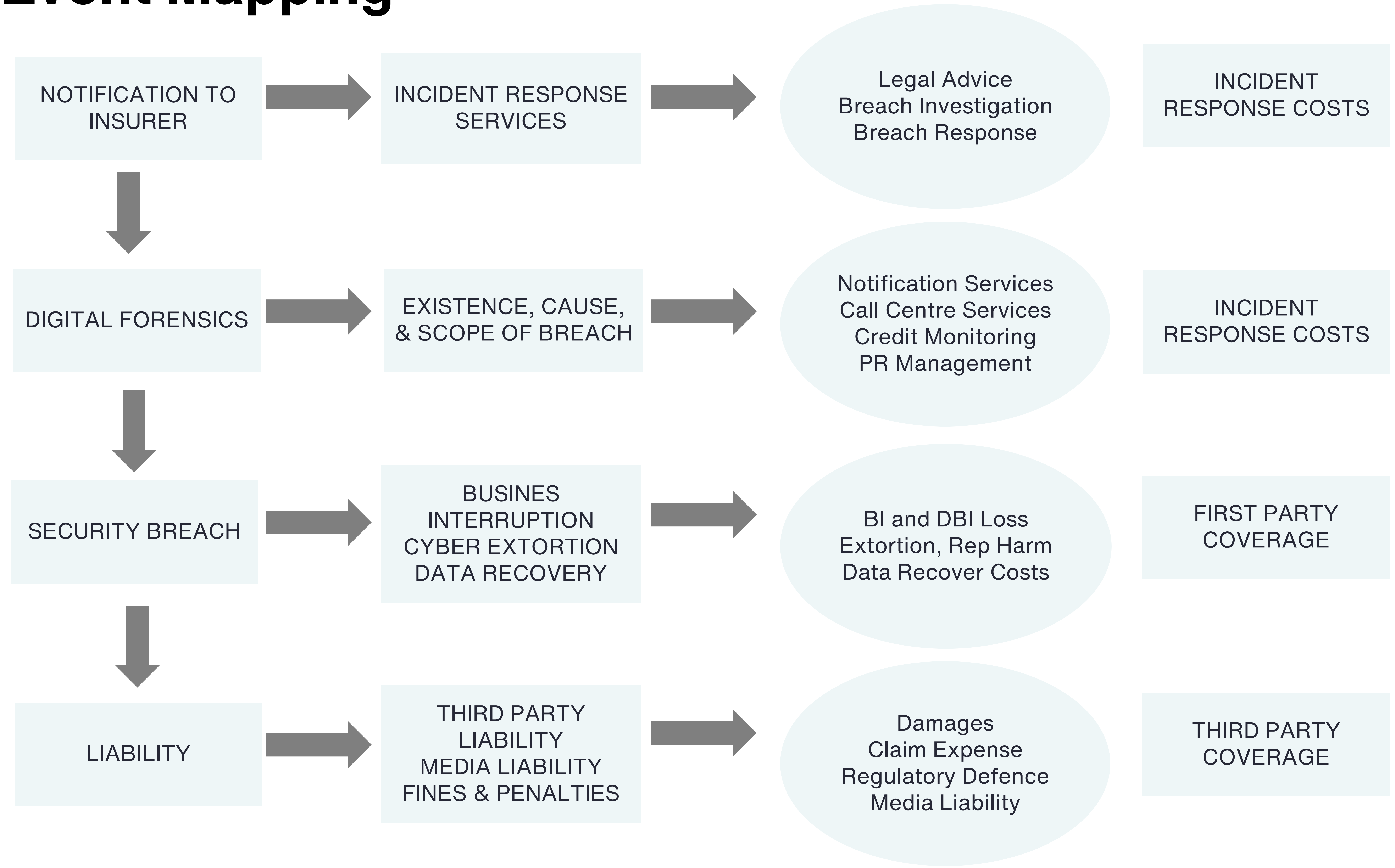
A SME organisation’s employee opened an email which appeared to be from a familiar business containing a link referring to as ‘Click here to view Payment Invoice’.

- The staff opened the LINK which led to a malicious website running malicious code (malware) and subsequently the malware was downloaded on the computer system being used and spread across the entire organisation’s network.

- The Hackers subsequently made a demand for a ransom to be paid to unlock the network & files within.

- The SME refused to pay the ransom and began working with their IT provider to restore the network and files back to normal, however, they were unable to recover from their backups, and had to hire external vendors (like DFIR experts, ransomware negotiators, and Lawyers) to help them manage the situation which ended up costing a significant amount of money.

Event Mapping



NOTIFICATION TO INSURER → INCIDENT RESPONSE SERVICES → Legal Advice
Breach Investigation
Breach Response — INCIDENT RESPONSE COSTS

DIGITAL FORENSICS → EXISTENCE, CAUSE, & SCOPE OF BREACH → Notification Services
Call Centre Services
Credit Monitoring
PR Management — INCIDENT RESPONSE COSTS

SECURITY BREACH → BUSINES INTERRUPTION
CYBER EXTORTION
DATA RECOVERY → BI and DBI Loss
Extortion, Rep Harm
Data Recover Costs — FIRST PARTY COVERAGE

LIABILITY → THIRD PARTY LIABILITY
MEDIA LIABILITY
FINES & PENALTIES → Damages
Claim Expense
Regulatory Defence
Media Liability — THIRD PARTY COVERAGE

LOSSES

□ **Incident Response**

□ **Ransomware Costs**

□ **Business Interruption**

- Subsequent to the IT forensic investigation, it was determined that no PII stored on the SMEs Information systems was exfiltrated or compromised.
- The total cost incurred towards legal costs and full IT restoration was $250,000 including ransom amount of 2 Bitcoins (approx. $200,000).
- This investigation & restoration of the IT Systems was undertaken over a period of three weeks. A loss of revenue of $25,000 due to Business Interruption.
- The total cost/loss incurred in relation to this matter was $275,000.

Questions?