Cyber Claims
Outline

- Market Overview
- Our Model & Experience
- Case Studies
- Outcomes & Learnings
CYBER INCIDENTS

• Video Major Cyber incidents 2018
• Video British Airways 2019
CYBER ATTACKS EXPLAINED

• TYPE OF ATTACK
  • MALWARE
  • RANSOMWARE
  • PHISHING
  • MAN IN THE MIDDLE
  • DENIAL OF SERVICE (DDOS)
  • ZERO DAY EXPLOITS
  • MALICIOUS SOFTWARE
  • BLACKMAIL TOOL
  • EMAILS CONTAINING MALICIOUS CODES
  • ATTACKS BETWEEN TWO COMM. USERS
  • INUNDATES SERVERS WITH TRAFFIC
  • MALWARE THROUGH VULNERABILITIES OF NEW SOFTWARE
THE ETERNAL CYCLE OF HIGH-PROFILE DATA BREACH

1. Successful data breach

2. The hacker uses the stolen data for his own personal gain

3. The data is shared by the hacker within his inner circles

4. The data is offered for sale on closed deep web or darknet platforms

5. The data shared online, either in its entirety, or partially

6. The targeted company confirms the breach

7. The now publicly-available data is used in large volumes for executing attacks

8. Hacking communities offer a processed version of the data for sale, or share it, on closed platforms
Cyber products have been around since the late 1990s
- Infancy of market, emerging needs and evolving products
- It is estimated that premiums from the global market will grow to $7.5 billion by 2022
- The cost to the global economy is more than $400 billion a year and continues to grow
ASIA market

- Buyers mainly in the Telco, Technology and Financial Centers
- SME’s buyers have yet to come to the party
- More customers buying BI extensions
- Market size of approx. $100m - 2019
- Cover led by major Reinsurers, Chubb, AIG, Munich Re
- Stand alone and add-on policies

Source: ACSC 2016 Cyber Security Survey
CLAIMS MODEL

Legal Support
Reputational Management
FNOL TPA
Forensic IT Experts
Credit Monitoring
Forensic Accountants

Sedgwick
Client

Global solutions. Local expertise.
Sedgwick Claims Experience

Global footprint & > 1000 cyber claims

UK, Asia, Australia, New Zealand

- 14+ clients
- 40FTE team
- GDPR, NDB privacy breaches
- Decryptions
- Claim Types:
  - SME
  - Enterprise
  - High Net Worth
  - Personal Lines
- Industry Awards
What do claims look like?
CLAIMS VIDEO

• BBC news – one ransomware
Cyber Claim Lifecycle

The first 48 hours are key

**FNOL**
- 24/7 hotline
- Incident manager contacts Insured
- Notify Insurer, Broker

**1st 12 Hours**
- Triage call with Insured, experts
- Containment, mitigation measures
- Review Policy coverage
- Clear Discovery Next Steps

**Next 12 Hours**
- Containment, mitigation efforts
- Engage Insurer, broker
- Stakeholder updates

**Within 48 hours**
- Clear Solution next steps emerge
- Rectification plan
- Notify regulator, legal representation?
- PR required?
- Business interruption?

- Proactive timely response to contain immediate impact and mitigate future losses
- Intense broker, insurer, insured engagement
- Ensure confidentiality and protect privilege
- Consistent and professional claims management approach
Case Study – Website Hack

Remediation/Action
- Website immediately taken offline
- External IT specialist engaged
- Call centre established to handle all queries
- Loss Adjuster and Lawyer appointed

Issues
- NDB obligations
- 3rd party IT agreement
- Ransomware – to pay or not to pay?
- PR & Media – insuring more than Cyber breach

Outcome
- Almost 3 months to restore website
- Indemnity granted – restoration and incident response costs

Event
- Website was hacked
- Threat of crypto locker – ‘Drupalgeddon 2’
- Bitcoin ransom demanded for decryption key
Case Study – Small Phish

First 48 hours translated

Monday
- **11:45am**: Malicious email received
- **12:15pm**: Insured clicks on link to the proposal

Tuesday
- Hacker has gained control of Insured’s email, downloads inbox (folders sync) and changes auto forwarding rules
- **~10am**: Hacker starts sending out phishing emails
- **2pm**: IT Vendor receives email, notifies Insured, resets password
- **3:30pm**: Notifies incident response line
- **4:30pm**: Stakeholder Call
- **6pm**: Email to all clients to ignore the email sent earlier

Wednesday
- **6pm**: Engages MS Admin to delete hidden auto forwarding rules to deleted inbox
- **8am**: IT Forensics continues – no auditing logs enable, RDS Server malware scan
- **9am**: Process begins to analyse information stored in Insured’s inbox

Thursday
- **8am**: IT Forensics continues – no auditing logs enable, RDS Server malware scan

Friday
- Insured operating normally and continues to analyse inbox
Cyber Claims – Incident Response

Case Study Learnings

- Incident response time to react – internal, external IT, objectives
- Ransoms – to pay or not to pay
- Decryption services – cost effective, worth it?
- Recoveries – vendor agreements
- Exclusions: Betterment, Social engineering, Proprietary information
Understand the revenue drivers of a business. How is revenue recognised and recorded

- Indemnity periods – move is to shorter indemnity periods, select period that coincides with operating cycle
- Excesses – time and monetary deductibles
- Extensions – contingent BI
- Exclusions – internal resources vs 3rd party, normal expenses vs additional costs, inconvenience vs actual losses
- Specific Industries – retail, online, professional services
Key Outcomes and Learnings

- Approx 10-15 years
- Evolving product
- Evolving market
- Knowledge

- Coverage v indemnity
- Continued development & knowledge sharing
- Multiple stakeholders

- Dual Insurance
- Co-insurance
- Recovery
- Claims preparation

- Policy language
- Policy limits
- Discovery v Occurrence
- Indemnity periods
- Risks

Infancy of Product
Expectation Gap
Other Aspects
Policy Response

Global solutions. Local expertise.
Q&A