Actuaries Summit

Think Differently

Actuaries Institute

21-23 May 2017 • Grand Hyatt Melbourne

Actuaries Summit
Think Differently

21-23 May 2017 • Grand Hyatt Melbourne

Actuaries Institute

Strategic decision making in a rapidly evolving cyber risk environment

Dave Millar & Robert Menzies

Agenda

- Current cyber threat landscape
- Responses of businesses, insurers, governments and others
- Current cyber insurance landscape
- Cyber risk modelling for insurers as a target
- Cyber risk modelling for insurers as risk aggregators
- Supporting strategic decisions

High profile cyber threats

- **Talk Talk** – DDoS diversion + SQLIA
- **Target / Home Depot** – Malware @ POS + compromised employee credentials
- **Sony Entertainment / Yahoo** – Malware
- **Russian, Israeli, German, Bangladeshi banks** – Malware, "Spear- Phishing"
- **Aussie Travel Cover** – Database hacks
- **Ashley Madison** – VPN attack using compromised passwords
- **NSA, CIA, Twitter, Reddit, DNC** – Leaks, DDoS, Database hacks
- **Allianz Worldwide Care, NIB, ARCBS** – Disclosure breaches
- **Kansas Heart Hospital, NHS, FedEx** – Ransomware

Cyber threat landscape

Who's behind the breaches?

75% perpetrated by outsiders.

25% involved internal actors.

18% conducted by state-affiliated actors.

3% featured multiple parties.

2% involved partners.

51% involved organized criminal groups.

Who are the victims?

24% of breaches affected financial organizations.

15% of breaches involved healthcare organizations.

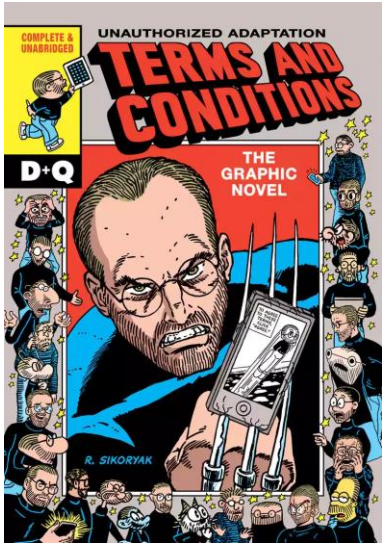
12% Public sector entities were the third most prevalent breach victim at 12%.

15% Retail and Accommodation combined to account for 15% of breaches.

2017 Data Breach Investigations Report - Verizon

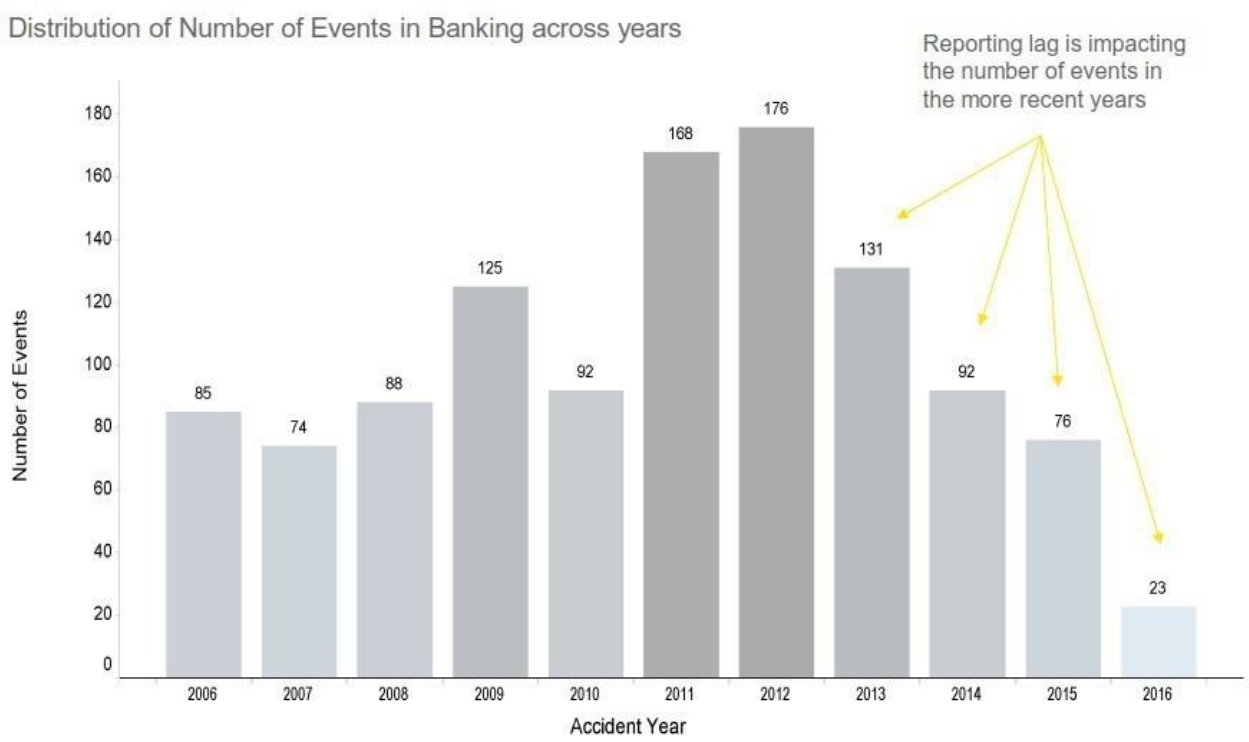
Collective responses

- Management stood down
- Share prices collapsed / depressed / increase in volatility
- Sales volumes fall
- Class actions undertaken
- Media outcry
- Political gesturing
- Regulatory enforcement / penalties
- Consultants engaged
- Insurance claims paid



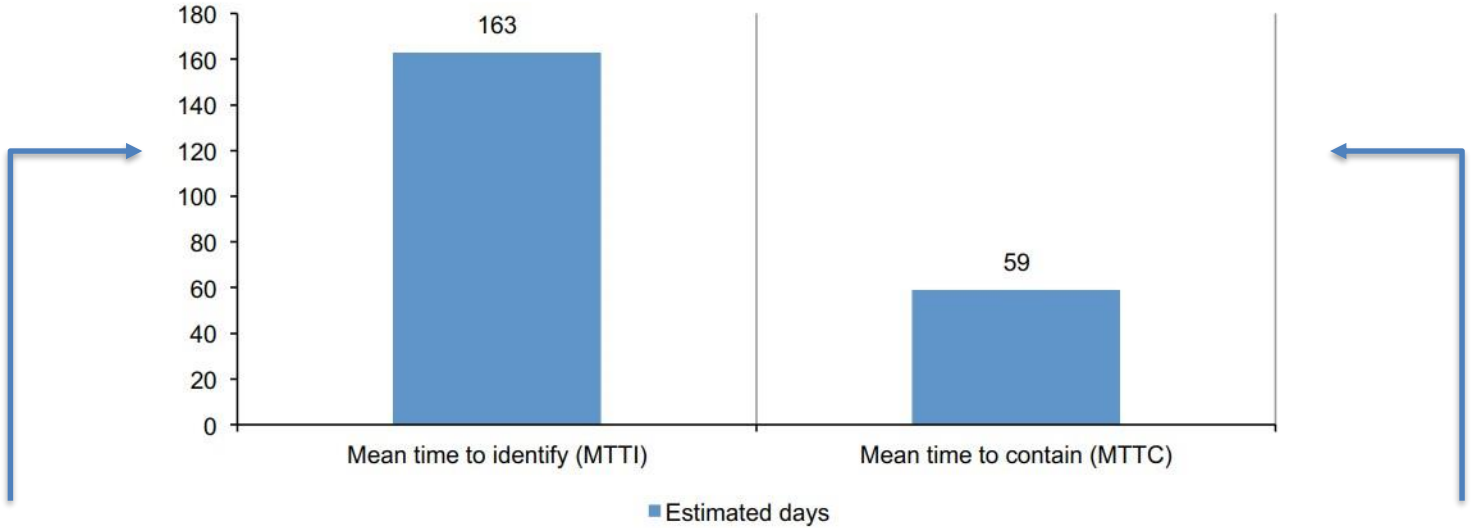
Insights from the USA

Insights from the USA



Data breach insights

Figure 16. Mean time to identify (MTTI) and mean time to contain (MTTC)



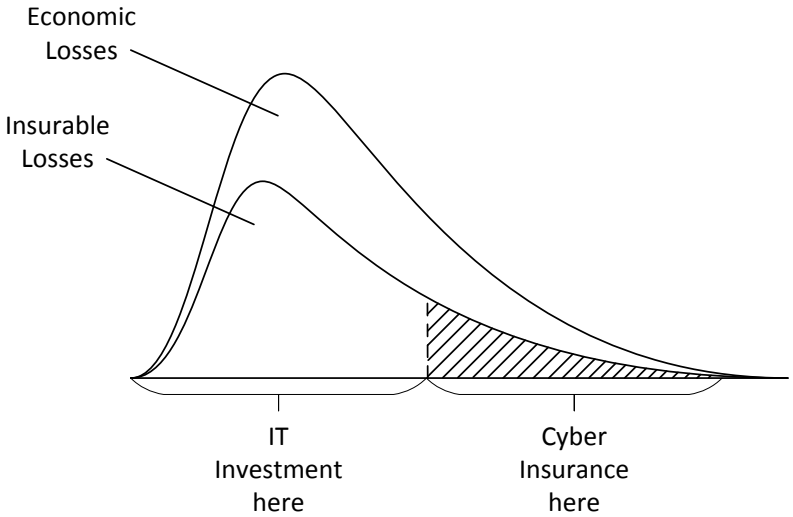
> 100 days TTI = +65% to costs

> 30 days TTC = + 30% costs

Current cyber insurance landscape

- Historical development and initial losses by early providers
- Evolution of products and client purchasing requirements
  - increasing demand from new regions and new sectors
  - Global partnerships forming to price cyber risks
  - Cross over with other insurance coverages
- Cyber is near the top of insurers' strategy, as they embrace all things "digital"
- Customer complexity and understanding of cyber insurance products is evolving

Insurance strategy ahead of the curve?



Challenges of cyber modelling

Data Collection

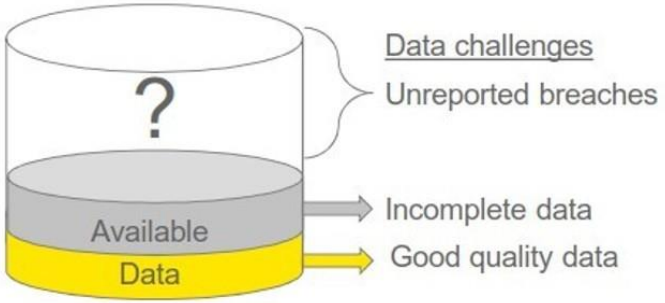
- Lack of cohesive data sources
- Inconsistent and fragmented
- Unreported breaches
- Scant details (companies not wanting to disclose)

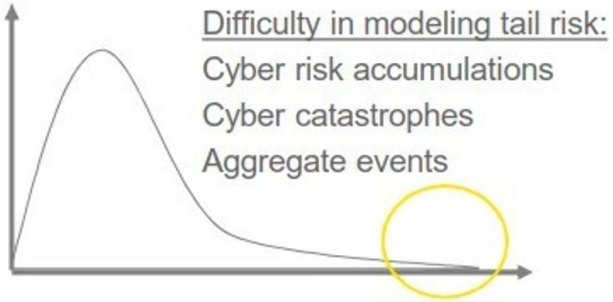
Modelling Challenge

- Dynamic regulatory and threat landscape continues to evolve
- Hence, probability and severity constantly change
- Tail-risk is difficult to capture

People Challenge

- Human element to cyber threats, increases modelling difficulty
- Need to account for both technology and people/process
- Needs a holistic, data-driven approach





Scenario-based approach

Cyber risk workshop

Recommended Attendees:

- CISO/CIO
- Information Security and IT Executives / Managers

Discuss and agree set of top cyber risk scenarios

Review of risk scenarios

High Impact Scenario

High Impact Scenario

High Impact Scenario

Scenario workshop

Recommended Attendees:

- Operational risk representatives

Develop scenario narrative

Identify critical assets

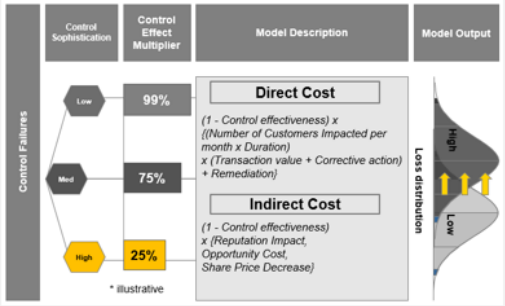
Identify primary risk drivers

Identify key mitigating controls

Identify primary loss drivers

Financial impact assessment

Example: Phishing campaign by criminal syndicate targets bank employees and delivers malware onto bank's network, enabling criminals to steal customer information



1 Cyber risk identification

2 Scenarios deep dives

3 Financial impact assessment

Example scenario

It’s not just your cyber defence plan

- There are a number of threats and attack vectors that will indirectly impact insurers:
  - Vulnerable supply chains
  - Insured businesses
  - Parent companies & subsidiaries

- Cyber resilience increases if management is able to make informed decisions about prioritising spend between:
  - Protective measures
  - Monitoring programs
  - Containment and remediation
  - [Re]Insurance

Strategic focus is needed by insurers

- Develop robust cybersecurity strategies
- Eliminate vulnerabilities in legacy IT systems
- Build in evaluation of cyber risks into vendor due diligence
- Target cyber resilience in operational risk stress scenarios
- Establish and evolve incident response teams
- Create compelling cyber protection products
- Clarify exclusions on existing policies
- Get close to your clients
- Evaluate concentration risk – consider reinsurance policies

Questions?