Waves of Disruption
The Cyber Risk threat to the Insurance Industry
Agenda

Introducing ‘Waves of Disruption’

Cyber Risk landscape – The threat to the Insurance Industry

Cyber Risk protection – Pricing challenges of Cyber insurance products

Panel discussion
Session 1: John Kilbride
Financial services globally has been impacted by a range of forces:

- **Regulatory reform** in response to the 2008 global financial crisis
- Growing **consumer empowerment** driven by generational changes
- **Globalisation** and availability of low cost locations and labour
- **Industrialisation** of core functions and activities
More recently, new technological disruptors are emerging including:

- **Digitisation** of the core activities of financial services.
- **Big data** technologies allowing profoundly different insights into business activities.
- **Machine learning and artificial intelligence** leading to robotisation of work.
- **Blockchain** technology fundamentally challenging traditional technology platforms.
- **Internet of Things / Connected**
- **Cyber**
Over the next 10 years the cumulative effect of these forces will re-shape the Insurance industry in Ireland.
Session 2: Kelvin Garrahan
Cyber Security Landscape for the Insurance Industry
Agenda

- Impact of Cyber Incidents
- Cyber Threat & Risk Landscape
- Lens on Insurance Industry
- What Can Be done
- Lens on Cyber Insurance
- Summary
Impact of Cyber Incidents
Impact of Cyber Incidents – What we know

Cyber incidents are reported in popular media at an increasing frequency

- TalkTalk Cyber incident
- Anthem (Second Largest US Health Insurer) 80,000,000 records stolen
- Care First (US Health Insurer)

The reality is this is only the “tip of the iceberg”

- Organisations want to avoid losing face and the potential brand damage
- Limited regulation mandating publication of breaches
- Breaches going undetected

Analyst data tells us

- Incident numbers are trending upward
- Number of records breached are trending upward
- Costs associated with an incident are trending upward
Impact of Cyber Incidents – What we know

Data Source: Verizon, Ponemon
Impact of Cyber Incidents – What we know

**Data Source:** hackmageddon, Symantec

**Attack Motivation**

- Cybercrime: 68%
- Hacktivism: 15%
- Cyber Espionage: 12%
- Cyber Warfare: 5%

**Underground Economy**

- 1000 Email Addresses: €10
- Scan of Passport: €2
- Stolen Cloud Credential: €8
- Credit Card Details: €20
Cyber Threat & Risk Landscape
Cyber Threat & Risk Landscape

Threats

9 Threats form 96% of 80,000 Incidents

1. Crimeware – Ransomware
2. Cyber Espionage
3. Denial of Service
4. Insider Privilege Abuse
5. Payment Card Systems
6. Physical Thefts
7. Point of Sale Intrusions
8. Web Application Attacks
9. Phishing Attacks

Data Source: Verizon
Cyber Threat & Risk Landscape: Risks

Risk Landscape is changing

- Mobility
- BYOD
- Cloud
- Social Media, *more*..

Traditional ICT Risks still apply
- 99% of attacks analysed are against vulnerabilities with patches > 1 year old
- Zero Day vulnerabilities time to “weaponise” is reducing

Cyber threats are asymmetrical risks
- Small, highly skilled groups exact disproportionate damage
- They often have very targeted motives
- They’re spread across the globe, often beyond the reach of law enforcement
- Threat velocity is increasing
- The window to respond is shrinking
Cyber Threat & Risk Landscape: Interconnected Risk

- **Social Media**
- **Cloud**
- **Mobility**
- **Networks**
- **Regulations**
- **Technology**
- **Globalisation**
- **Customers**

### Strategic Risks
- Brand Image
- Affect reputation
- Competitive position

### Financial Risk
- Affect earnings
- Share price
- Profitability

### Operational Risk
- Impact systems
- Supply chain
- People and processes

### IT Risks
- Affect ICT systems
- Infrastructure

### Regulatory and Compliance Risk
- Affect ability to comply
- With laws, regulations

---

**Social Media**

**Cloud**

**Mobility**

**Networks**

**Regulations**

**Technology**

**Globalisation**

**Customers**
Lens On: Insurance Industry
Cyber Security Lens on: Insurance Industry

**Actor**
- Criminal
- Competition
- Government
- Terrorist

**Vulnerability**
- Flaws
- Weakness

**Motivation**
- Financial
- Political
- Publicity

**Assets**
- IP
- Risk Strategies
- Sensitive Proprietary Information
- Personal Identifiable Information (PII)
- Client Data
- Staff Data
• Cyber-criminals have started to recognize that insurers possess large amounts of personal information about their customers, which is very attractive to identity thieves and fraudsters. In some cases, insurers also possess significant amounts of customer credit card and payment data. However, there is at least one case in the insurance sector where the victims of a cyber-attack weren’t even paying customers but merely consumers who had requested a price quote.

• Cyber-criminals targeting insurers often have significant resources. This enables them to employ sophisticated attacks that combine advanced malware with other techniques such as social engineering.

• Attacks on insurance firms can result in significant, tangible damages such as fines, legal fees, lawsuits and fraud monitoring costs. However, a less obvious but no less significant impact may be loss of trust, driven by customers’ concerns about whether their information is truly safe.
Cyber Security Lens on: Insurance Industry

• Since the insurance business revolves around trust, a major breach can have a very real impact on an insurer’s brand and market value.

• It’s worth noting that most of the breaches publicly reported by insurance companies to date have been characterized as short term attacks, with cyber-criminals compromising a system, stealing specific information and then quickly moving on. In fact, our research did not uncover any documented cases of long-term infiltration and cyber-crime in the insurance sector. However, we believe the number of long-term attacks may be silently growing as attackers quietly slip in undetected and establish a persistent, ongoing presence in critical IT environments.

• Over the years, many insurance organizations have invested a lot of money in security tools and processes that may be providing a false sense of security. As attackers learn to leverage encryption and other advanced attack techniques, traditional tools such as firewalls, antivirus software, intrusion detection systems (IDS) and intrusion prevention systems (IPS) are becoming less and less effective.
Cyber Security Lens on: Insurance Industry - Compliance

NIAC
Principles for Effective Cybersecurity Insurance Regulatory Guidance

CBI
Increasing Focus on Cyber Security Threat

Germany Cyber Law
Critical Infrastructure Protection, fines up to 100,000 Euro

European Cyber Law
NIS directive identifying operators of essential services, including Financial Industry

APRA
Will check extent of Insurance Industry preparedness to Cyber attack in 2016
Cyber Security: What Can be Done?
Cyber Security: What can be done

Understand cyber security posture, both current and desired state
- Measured against peers
- Alignment to frameworks
- Establish Metrics and KPIs, KPIs

Integrating Threat Intelligence into tactical and strategic cyber security planning

Embrace Automation where possible to
- Reduce the cyber security workload
- Improve responsiveness

Analyst data tells us
- Cyber Incident Response Plan
- Game days & Testing
Lens On: Cyber Insurance
Cyber Insurance: Underwriting Technical Challenges

Historical data on cyber incidents is alone is not sufficient to predict future events.

Threats evolve over time:
- Vulnerability discovery
- Weaponziation and utilisation by Attackers
- Motivations of attacks and their skill levels, behaviour and association

Speed of Threat evolution is getting faster.

Analyst data tells us:
- Technique can be used to gain perspective into risk across
  - Market Sectors
  - Individual Organisations
Cyber attacks are on the increase, as are the costs of a data breach, these trends are set to continue for the foreseeable future.

The Insurance Industry is a significant target and this has been recognised by financial regulators globally. This has resulted in increased regulatory oversight with the expectation for this to scale up as the regulators develop cyber skills.
Session 3: Sinéad Kiernan
Cyber Risk Insurance
## Cyber Risk Insurance: Introduction

- Immature and evolving area
- Risks are unique & rapidly changing
- Significant market potential...
- ...but considerable challenges
- Underwriting considerations
- Effective risk mitigation is critical
Cyber Risk Insurance: Market Potential

Estimated annual cost of cyber crime to the global economy*

$445bn

Total global economic losses from natural and man-made catastrophes**

$110bn

* Allianz Risk Barometer
** Swiss Re
Cyber Risk Insurance: Market Potential

Global Cyber Risk Premium ($bn)
Cyber Risk Insurance: Opportunities

Growing market

- Develop standards
- Diversify portfolio
- Limited, but growing, capacity
- Become early market leader
- Niche line of business
- Develop expertise
- Enhance reputation as innovator
Cyber Risk Insurance: Challenges

- Limited past data
- Reliant on data from industry
- Non-traditional expertise required
- Policy wording needs to be precise
- Level of risk is ever evolving
- Aggregation/clash risk

Cyber Risk Challenges
Cyber Risk Insurance: Underwriting – The Cyber Risk Landscape*  

Cyber Risk Landscape

<table>
<thead>
<tr>
<th>Security Standard</th>
<th>Potential Loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lower</td>
<td>Lower</td>
</tr>
<tr>
<td></td>
<td>Food &amp; Beverage</td>
</tr>
<tr>
<td></td>
<td>Manufacturing</td>
</tr>
<tr>
<td></td>
<td>Construction</td>
</tr>
<tr>
<td>Higher</td>
<td>Higher</td>
</tr>
<tr>
<td>Technology</td>
<td>Banking</td>
</tr>
<tr>
<td>Aviation</td>
<td>Telecoms</td>
</tr>
<tr>
<td>Insurance</td>
<td>Health</td>
</tr>
<tr>
<td>Legal Profession</td>
<td>Retail</td>
</tr>
</tbody>
</table>

* Illustrative only
Cyber Risk Insurance: Underwriting Considerations

- Some clients a “no-go”
- Rating factors
- Service offering
- Pricing
- Policy terms
- Target specific industries
- Expertise needed
- Exposure monitoring procedures
- Risk appetite
- Profit/Expense loadings
Cyber Risk Insurance: Risk Management

- Partner with reinsurer / others for expertise & data
- Exposure and aggregation monitoring
- Review effectiveness of policy wording
- Monitor insureds’ cyber risk mitigation processes
- Post-loss mitigation
- Continually update knowledge and skills
- Cover for catastrophes / accumulations
- Limits on reinsurance capacity
- Alternative mitigation tools e.g. ILS / CAT bonds

Cyber Risk Mitigation
Conclusion

The scale of global cyber risk offers an opportunity for insurers. However, it is essential to understand the challenges unique to cyber risk. Underwriting and risk management strategy need to be aligned with the organisation’s risk appetite and evolve in tandem with developments in the cyber risk landscape.