

Cyber Threats and Insurance



Zainab Khatib
Aqaba Conference 2019



Agenda

Cyber Threats

- ▶ Key Concepts
- ▶ Threat Actors & Attributes
- ▶ Types of Breaches
- ▶ Cyber Trends of 2018
- ▶ Cyber Threat Outlook 2019

Cyber Insurance

- ▶ Cyber: New to Insurance?
- ▶ Why is Cyber Insurance Important?
- ▶ Global Cyber Market
- ▶ Insurance Opportunity with Increasing Regulation
- ▶ Common Misconceptions
- ▶ What are Insured Cyber Risks?
- ▶ Challenges for Cyber Insurance Market
- ▶ Insurance Outlook 2019

Cyber Threats



Key Concepts

- ▶ Emergence of **Industry 4.0**
- ▶ Dependency on **data & networks**
- ▶ **Enterprise** technology vs. **Operational** Technology
- ▶ **Essential Security Capabilities:**
 - *Availability*
 - *Integrity*
 - *Confidentiality*

Threat Actors & Attributes

- ▶ **Political** – *nation-state/terrorism, APT groups*
- ▶ **Criminal**
- ▶ **Hacktivist**
- ▶ **Script Kiddies**
- ▶ **Human Error**

Types of Breaches

▶ Hacking or Malware:

- *Unauthorised third party access/malware*
- *Ransomware*
- *Social Engineering/Phishing*
- *DDOS*
- *Vendor Hack*
- *Credential Stuffing*
- *Money Theft*

▶ Unintended Disclosure:

- *Online*
- *Mailing/Emailing Error*
- *Incorrect Disposal*
- *Incorrectly Shared with Vendor/Third Party*
- *Vendor*

▶ Insider

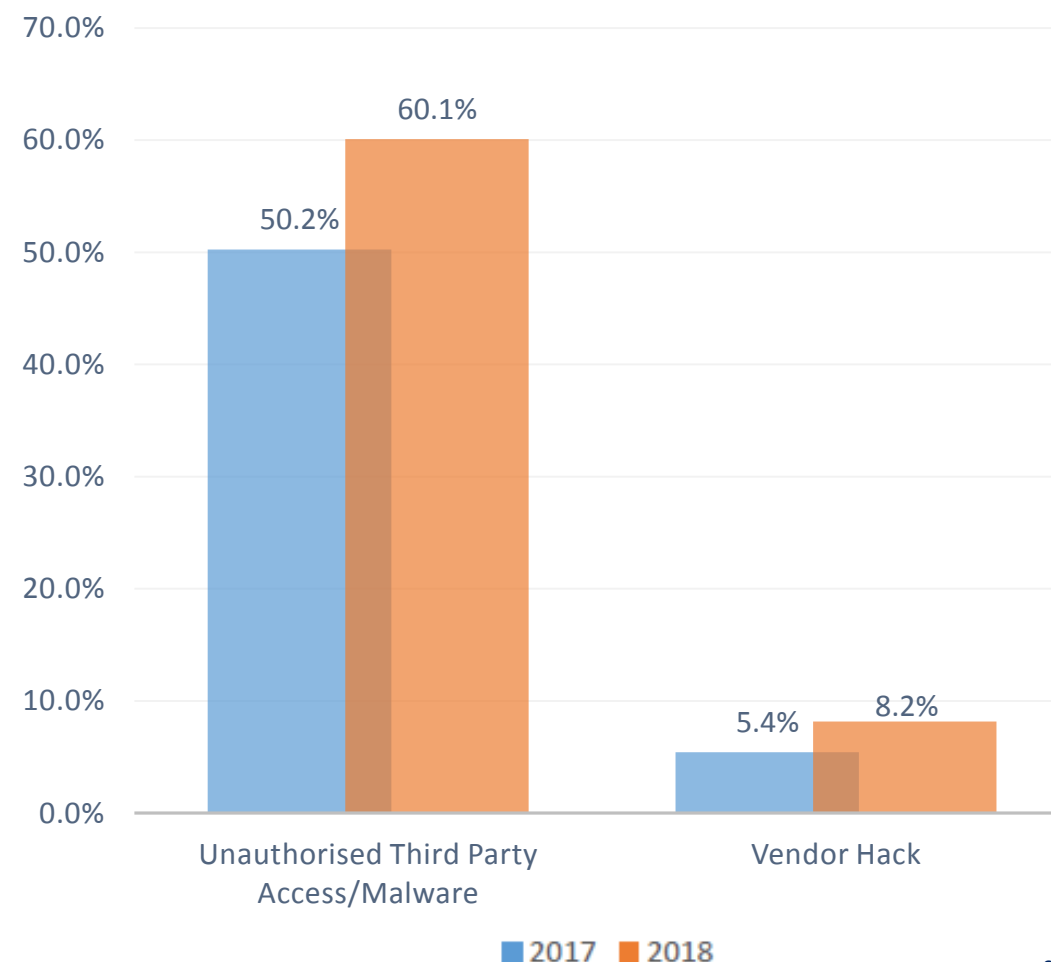
- ▶ *Portable Device*
- ▶ *Physical Device*

Cyber Trends in 2018

- ▶ **Public attribution of attack activity by governments** – *US, UK etc.*
- ▶ **Regulation** – *GDPR, California Consumer Privacy Act*
- ▶ **Software sector increased frequency of breaches** – *attackers following data*
- ▶ **The commoditization of cyber criminal tools** – *Ransomware-as-a-Service, Malware-as-a-Service and DDoS-for-Hire, have made the tools for global extortion and business disruption campaigns accessible to the less experienced.*
- ▶ **Proliferations of crypto-currencies** – *methods to anonymize their users are also fueling the spread of cyber crime.*

Cyber Trends in 2018: LSM Internal Analysis

- ▶ Widely reported increase in **Vendor** hacks since 2017
 - 23% of companies in Middle East and Africa manage more than 21 vendors (Cisco 2018 Security Capabilities Benchmark Study)
- ▶ Fewer breaches in the **Financial** sector vs. greater breaches in **Healthcare** potentially due to continued lag in cyber security investment
- ▶ Increase in **unintended disclosure** breaches – greater emphasis on reporting requirements
- ▶ Increase in **reported** breaches in MENA region



Cyber Trends in 2018: Middle East

- ▶ APT 39 – *cyber espionage threat*
- ▶ Triton malware – *watershed SIS cyber attack*
- ▶ Hidden phishing risks during M&A
- ▶ Growing cybercrime marketplace

58% of organisations in Middle East/Africa have suffered public scrutiny due to a breach

48% of attacks in the Middle East and Africa resulted in damage over \$500,000.



MEDIAN DWELL TIME

175

DAYS IN 2017

177

DAYS IN 2018

Cyber Threat Outlook 2019:

AI-Powered
Malware

Previously unknown
threat vector in
systems/cloud
environments *i.e.*
*Spectre/Meltdown of
2019*

Industrial
Control
System Hack

Cyber Insurance



Cyber: New to Insurance?

- ▶ First cyber policy – mid/late 90's in the **dotcom boom**
 - *Regulation as a driver*
 - *Shift in coverage demands following **WannaCry** & **NotPetya** attacks*

- ▶ Definition of cyber – **affirmative** vs. **non-affirmative** cyber risk
 - *Different proximate causes in different classes of business*

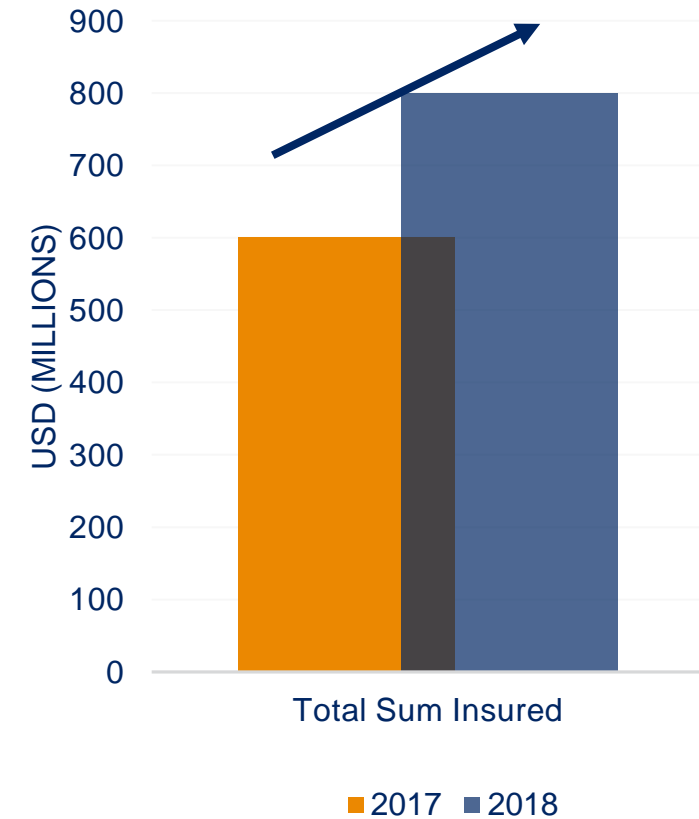
Why is Cyber Insurance important?

- ▶ Threat is **real** and **significant** to businesses
- ▶ Businesses in **varying stages** of cyber risk mitigation **maturity**
- ▶ Changing value **of data/assets** reliant on technology
- ▶ **Catastrophic** nature
- ▶ C-suite level management more **accountable**

Global Cyber Market

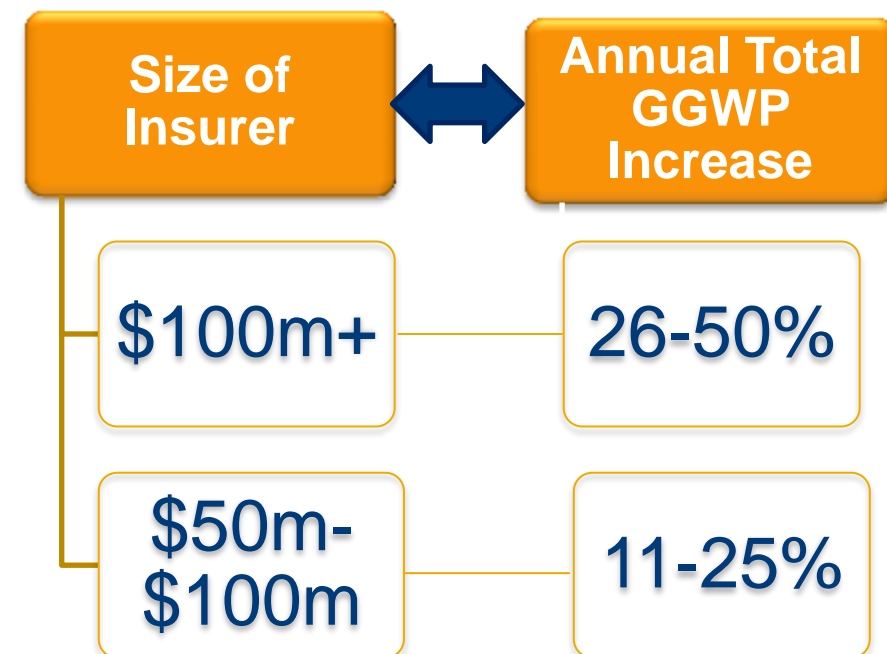
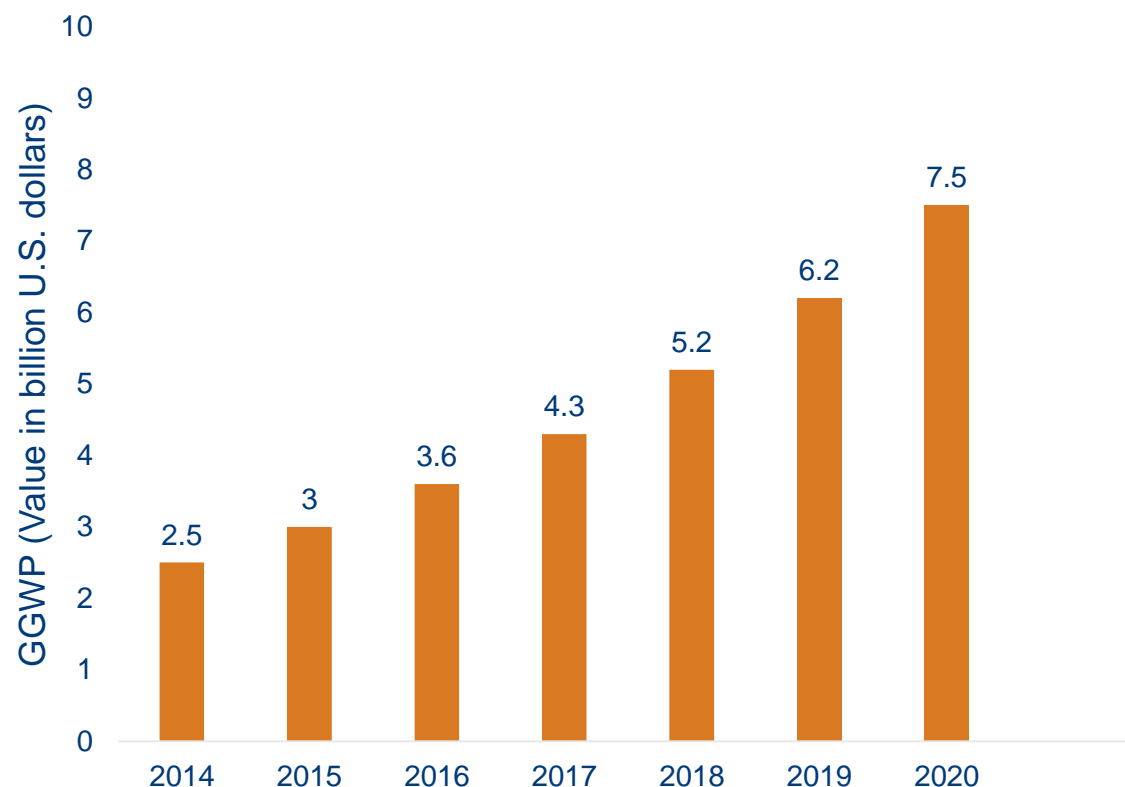
- ▶ **\$725 million capacity** in cyber insurance market
 - C. 50% is US capacity, \$312m London capacity & remainder in Bermuda.
- ▶ As overall towers are growing, **\$1 billion** should soon become commercially viable.
- ▶ **Average policy limits increased** by 100% to roughly \$6 million (2017), compared with \$3 million, as of October 2016 (CIAB Report, 2017).
- ▶ **Average largest cyber policy limit** placed by survey respondents increased by roughly 66% from \$61 million in October 2016, to a reported \$101 million (CIAB Report, 2017).
- ▶ Growth in the global cyber insurance market reflects companies' **increasing awareness** of their cyber, and an appetite to transfer this exposure.

Largest Cyber Insurance Towers



Global Cyber Market

Value of cyber insurance premiums written worldwide (Statista, 2016)



Source: The Betterley Report (2018)

- ▶ Most premium likely to be from **new insureds** – with some **increased limit buyers**.

Insurance Opportunity with Increasing Regulations






Common Misconceptions



What are Insured Cyber Risks?

► First Party:

- Loss or damage to digital assets
- Non-physical business interruption and extra expense
- Cyber extortion and cyber terrorism
- Reputational Harm

- 
- 1) *Computer crime and computer attacks by third parties*
 - 2) *Accidental damage or destruction of hardware*
 - 3) *Administrative or operational mistakes by employees and third party providers.*

What are Insured Cyber Risks?

► Third Party:

Security and privacy liability and defence costs

- Network security breaches
- Transmission of malicious code
- Damage, alter, corrupt, distort, copy, delete, steal, misuse, or destroy Third Party Digital Assets
- Breach of third party or employee privacy rights or wrongful disposal of data
- Causing DDoS attack on third party
- Phishing or Pharming confidentiality

Privacy regulation defence, fines and penalties

- PCI fines extensions available

Customer care & reputational expenses

- Notification expenses
- Credit monitoring
- PR expenses



Other Types of Insured Cyber Risks

- ▶ **'Infrastructure' losses/ Failure to supply** – *result in business interruption or third party liability*
- ▶ **Dependent business income loss** – *optional and sub-limited*
- ▶ **Insured's cost to purchase replacement power on the spot market**
- ▶ **Defined terms for SCADA energy management systems & critical infrastructure assets** – *clarify intent of policy for non-privacy related breaches*
- ▶ **Property Damage**
- ▶ **Hull/Loss of Lease**
- ▶ **Manufacturing, on-shore and off-shore energy, commercial property and ports and terminals**

Challenges for Cyber Insurance Market

- ▶ **Constantly evolving class**
- ▶ **No wording the same; various subtleties to coverage.** *Aon Survey 2016 – nearly 95% of companies state clear policy wording as the most important issue in the cyber risk market at this point.*
- ▶ **Lack of publicly available data** relating to frequency and severity of claims.
- ▶ **Companies not keen to disclose data breaches** or the full cost to the company of such attacks (implementation of GDPR will change this in Europe)
- ▶ **Difficult to benchmark** – *sophistication of cyber security practices can vary significantly even amongst companies from same industry sector with similar revenues.*
- ▶ **PartnerRe and Advisen, 2018 Survey of Cyber Insurance Market Trends** – *30% of brokers answered that cyber pricing was still very disjointed across the market.*
- ▶ **Lack of historic claims** – *limited precedents for application of policy terms and conditions.*
- ▶ **Claims support services in flux/development; generally increased competition**
- ▶ **Systemic Exposures**
- ▶ **Absence of Talent to underwrite and broker the class of business**

Insurance Outlook 2019:

- ▶ **Rate volatility** looks to be set to continue
- ▶ **Further product innovation** – power/energy – marine/hull/loss of lease
- ▶ **Some areas flooded with new capital** – e.g. European/UK business
- ▶ **Smarter buyers**; analyse exposures, buyer cat not dollar-swapping
- ▶ **Technological advances**; chip-and-pin effect?
- ▶ **Political instability**
- ▶ **Challenges with automation** – cars etc. – cyber or not

Q&A



Liberty
Specialty Markets

Appendix

Cyber Claims Example 1

▶ Situation:

- *On or around July 2015 a hacker group instigated what seems to be a coordinated attack against a number of banks in the UAE. Our client suffered a breach and some client data was compromised. The breach was apparently identified within a few days and the malware isolated and removed. The Bank has represented that it has suffered no business interruption loss, neither has there been any claims or complaints brought by customers. They did not claim notification expenses either.*

▶ Covered Costs

- *Forensic review: \$96,000*
- *Overtime: \$26,000*

▶ Lessons Learned

- *Extortion and BI exposure*

Cyber Claims Example 2

▶ Situation:

- *The insured, a large UK retailer, were targeted by what initially appeared to have been a DDOS attack. Subsequently, over a busy shopping weekend, the insured's websites suffered multiple outages. Technical advisers were appointed to investigate the cause, and concluded that the cause of the outages was due to a technical issue with the Insured's data management system.*

▶ Covered Costs

- *Business Interruption GBP2.25m; Overtime/Legal/forensics: GBP 300,000; Monitoring/Coverage council GBP 150,000*

▶ Lessons Learned

- *First party losses can be caused by external attacks*
- *Business interruption may arise out of the failure of network security, including unauthorized access and use of corporate systems*
- *Proper architecture and configuration for high volumes key*