8th AIDA Europe Conference, Lisbon, 4 October 2019

Insurers' own Exposure to Cyber Risks

Peggy Sharon, Adv.
Levitan, Sharon & Co., Israel
Cybersecurity in the Insurance Sector

• Insurance companies hold substantial volumes of sensitive and confidential personal data, public savings and pensions of insureds → a target for cyber threats

• Growing importance of cybersecurity in the Insurance sector in view of GDPR and privacy laws → exposure to heavy fines

• Insurer’s own cyber security as means of protection of Insurer’s Stability → Protection of the Insureds
• **Sensitivity of Data**
  → Insureds’ duty of disclosure
  (Especially due to personalized insurances)

• Sole event – catastrophic results
• Increased digitization – increased vulnerability
• Cloud storage – improvements on the one hand, greater risk on the other
EU Regulation

Insurance regulation:

Solvency II Directive 2009 $\rightarrow$ Article 45: ORSA

Own Risk and Solvency Assessment
Risk based capital regime

Israel – Required by The Commissioner of Insurance's Directive 2017-1-9 of June 2017, yet full implementation is due in 2024
Own Risk and Solvency Assessment

- Own risk assessment includes external risks.
- **Cyber crime** - key scenario under Insurers’ risk and solvency assessment.
- Risk management of operational, emerging and potential cyber risks

- Israeli Supervisor of Insurance - directives on handling external risks, such as money laundering and **cyber risks**.
The Israeli Commissioner identified the following threats:

- A negligent employee
- Attempts to insert malware via email
- Attack by a guest
- Attack by employee or supplier with remote access
- Attack by a broker
Insurers’ connection with external bodies

- Lawyers
- Health providers
- Loss adjusters

Targeted by hackers

Biggest threat: leakage of sensitive data
Cybersecurity Regulation in the Israeli Insurance Industry

- The Capital Market Authority’s “Cyber Risk Handling Circular” (2016) – plan for cyber emergency event

- “Business Continuity Circular” (2013) - maintaining continuity and setting recovery plan

- “Outsourcing circular” (2018) - material activity of the insurer’s core business should be protected and complying with regulator’s circulars when transferred to outside businesses
On May 2019, Israel’s Capital Market Authority concluded cyber exercise against supervised bodies.

Overall readiness is satisfactory.

However, comments were given on specific weaknesses to specific companies. e.g.:

- Lack of updated work procedures for business continuity
- Absent of emergency teams
- Declaration by management of a cyber emergency event
Worldwide Cyber Simulations by Regulators

- **ABS Singapore** - large-scale, industry wide cyber attack simulation on financial sector to test business continuity (2017)

- **Bank of England**– CBEST cyber resilience testing for financial sector continuity (2014)

- **Hong Kong Monetary Authority** requires participation in simulations under iCAST framework (2017)

Cybersecurity Incidents in the Insurance Industry

- **Anthem** (2nd largest US Healthcare Insurer) and **Premera** attacked in 2014-2015. Exposed personal information and credit card data of up to 91M policyholders.

- Cybercriminal group **DD4BC** attacks financial institutions worldwide, threatening denial of service in consideration for bitcoins. Attacked two German insurers in 2015.

- **Defense Health** - Australian health insurer for military personnel hacked in 2019. Impersonation as staff member, requesting unauthorized payments.
Another Regulated System…

- Not only insurers are regulated – the dark web is regulated and structured
- Objective: trade hackers’ skills and other illegal activity for profits
• Less human involvement in insurance underwriting and claims. Use of automatic algorithms, AI and machine learning.

• Need to adapt to new technologies – be one step ahead to successfully block intruders.

• Data protection – a big issue to be aware of.

• Insurers – top-sensitive bodies, growing target for cyber attacks.
Who will provide cyber insurance to insurers?

Muito Obrigada!