

Australian
Cyber Conference
2021



Cyber Insurance: The Existential Battle for Its Future

Dr John Selby



Australian Cyber Conference 2021



About us

Privcore's team with 40 years' combined experience helps business and government **make privacy core business** so they can deliver services with the trust and confidence of customers and citizens.

Privacy impact assessments	Data breach prevention and recovery
Audit and privacy health checks	Privacy by design
Privacy management frameworks	Algorithmic impact assessments
Privacy maturity models	Research, training & presentations
Privacy advice and research	Cookie policies & Cookiebot



Making privacy core business



Overview

- Cyber-Attacks & Cyber-Risks from an Insurance Perspective
- How Cyber-Insurance Differs from other Insurance Products
- NotPetya Attack
- Aftermath and Legal Disputes for Five NotPetya Victims
- Acts of War in Cyber-Insurance
- Attribution of Cyber-Attackers
- Silent Cyber Insurance Risk
- Analysis



Making privacy core business



Australian Cyber Conference 2021



Cyber Attacks Cause Insurers To Lose Sleep

- 2010: Stuxnet on Iranian Nuclear Enrichment Facilities
- 2014: German Steel Mill
- 2015: Ukraine's Power Grid
- 2016: SWIFT inter-bank message system heists
- 2017: Wannacry ransomware
- 2017: NotPetya wiperware
- 2018: Triton – industrial safety controls
- 2019: LockerGaga & MegaCortex ransomware hit organisations
- 2019: Airbus supply chain
- 2020: SolarWinds Orion
- 2021: MS-Exchange Email Servers



Making privacy core business



What are Cyber-Risks?

Cyber-Risk: the risk of any financial loss, disruption or negative reputational impact because of a failure in IT systems, whether through people, processes or technology, including risks emanating from:

- Use of electronic data and its transmission;
- Physical damage;
- Fraud committed by mis-use of data;
- Liability arising from data use, storage or transfer; and
- Availability, integrity and confidentiality of electronic information





Cyber-Insurance Compared to Other Insurance Products

Issue	Other Insurance Products	Cyber-Insurance
Specificity	Broader	Narrower
Intention of Insurer/Underwriter	Non-cyber focused, but may cover some cyber losses ("silent cyber")	Focused specifically on cyber losses
Volume of Historical Data	Large	Very small
Confidence in Accuracy of Actuarial Modelling	High	Lower
Confidence that Aggregation Risks are being Managed	Higher	Very Low
Potential to Create Solvency Risk for Insurers	Low-Medium	Higher
Industry Coverage	Broad	Narrowing
Acts of War & Terrorism	Typically Excluded	Excluded, but may have Carveback for Cyber-Terrorism
Maximum \$ coverage	Typically higher (up to \$Billions)	Typically lower (rarely above \$100m)



Making privacy core business



Australian Cyber Conference 2021



Questions

operations@privcore.com

www.privcore.com



Making privacy core business