Cyber insurance, Ransomware and Regulation – where do we go from here?

29 June 2021
Dr Jan Lemnitzer
JML Cyber Policy Consulting and
Department of Digitalization,
Copenhagen Business School
The ransomware crisis and cyber insurance

• The escalating ransomware problem has put a strong focus on existing issues in the cyber insurance sector:
• 1) Has the possibility of claiming ransom payments on cyber insurance policies contributed to the current problem, and should ransoms be banned?
• 2) Are the ways the insurance industry measures the cyber risk of companies still appropriate for the current threat environment?
• 3) Could cyber insurance help protect SMEs and fix their notoriously low IT security standards?
Current trends

• Storm clouds are gathering over the cyber insurance industry:

• Until very recently, it was a highly profitable niche sector that kept growing every year, driven by customer demand. Now, ransomware has developed from a problem to an existential threat.

• Insurers raise premiums, lower coverage limits, experiment with ransomware exclusions, and shrink their portfolios.

• Munich Re CEO recently wondered whether ransomware damage might become uninsurable in the near future.
GAO cyber insurance market report, May 2021

• Customer demand for cyber insurance is rising, and they demand higher cyber specific coverage limits.
• Insurers are moving in the opposite direction and raising premiums.
• Some have begun to move out of specific sectors, such as healthcare and education.

• Structural issues:
• Clients struggle to understand their policies as coverage and conditions are confusing and key terms left undefined.
• Insurers complain about a lack of historical data on cyberattack-related costs. Together with the difficulty of measuring company cyber risk, this makes product pricing and development a challenge.
Based on a two-year research project funded by the UK NCSC and others, this report offers 60 pages of analysis of the issues and challenges facing the cyber insurance market, with a focus on the UK.

- It makes 14 recommendations, ranging from proposals for premium incentives for SMEs to ideas for improved data sharing to compulsory cyber insurance for companies seeking government contracts.

- Very happy to discuss them during Q&A, especially since I disagree with most of them.
1) Ransoms and cyber insurance

• Insurers say they don’t encourage ransoms but:
• Incident Response professionals insist this is happening.
• There are people making a living negotiating ransoms that work with insurers.
• Some Ransomware gangs claim they target insurers and work off their lists of insureds as payment is quick and unproblematic.
• **Economic incentive:** paying ransoms is cheaper than covering a full rebuild of the IT system.
• The Association of British Insurers has publicly defended the practice of offering insurance cover for ransoms.
So should ransoms be banned?

• While a comprehensive ban of ransoms as discussed in New York would seriously undermine the criminal’s business model there are concerns:

• It might drive businesses and negotiators handling payments underground, creating a new criminal sector offshore.

• There would have to be exceptions for certain cases where ethical or humanitarian concerns prevail. Criminals might then target those.

• **Instead, we should:**

• regulate and control the cryptocurrency exchanges (KYC rules).

• Ban insurance coverage of ransom payments.
2) Measuring cyber risk

• One constant complain of insurers is that they would like more cyber claims and loss data, but data sharing remains difficult.

• Question: to what extent can historic data guide pricing decisions in the current cyber threat environment? Should the focus instead be on threat analysis and company risk assessment?

• There are established ways of measuring company cyber risk through intensive audits and site visits. Problem: that’s expensive.

• As cyber insurance coverage is brought to more and more companies, how can cyber risk assessment be scaled or automated?
Why not just rely on the Bitsight score?

• When cyber security risk rating companies like Bitsight and Security Scorecard set up ten years ago, insurers were their first customers.

• Combining vulnerability scans, network monitoring and various streams of data, they let their algorithms create a score.

• As experiences have been mixed, key questions remain: how reliable are these scores, especially when compared with claims data?

• Can business decisions like granting coverage to a smaller company be made just based on a scan and online report?
What if we all relied on the BitSight score?

- None of these concerns has restrained the expansion of these companies: they attract huge amounts of venture capital and are expanding their business and customer base.
- The technology is currently winning over companies seeking to improve their cyber security third party risk management.
- Companies already get offered supplier contracts that automatically fall void if the BitSight score falls under 700.
- Thinking ahead, are we walking into a world where IT security budgets are allocated to maintain a rating rather than keeping the company secure?
- Might this shift resources away from everything that cannot be observed online from the outside?
But could regulation of third-party cyber security risk management save insurers?

• The increasing focus on supply chain cyber security is prompting regulation, particularly for providers of critical infrastructure.

• The EU’s upcoming NIS 2.0 regulation draft includes a requirement to conduct ‘state of the art’ third party risk management for cyber risk.

• What does ‘state of the art’ mean? If it’s more than BitSight scores, large companies will routinely audit their suppliers and suppliers will seek ways to demonstrate their trustworthiness.

• This could be a great opportunity for insurers to benefit from all these ratings and perhaps shape the policy process on ratings and certifications.
What could this look like in practice?

• Some member states have attempted to anticipate the new NIS requirements by setting up their own rating systems:
  • KSV1870 in Austria (nationwide rating system for suppliers of critical infrastructure run by NimbuSec, launched January 2021).
  • Pinakes in Spain (nationwide rating system for financial services industry, launched by LEET Security in February 2021).

• Both argue their platform solutions are more reliable than scores without audits while offering much greater efficiency than companies conducting their own audits. Both are untested in practice though...
3) Can Cyber insurance help protect SMEs?

- Report after report has confirmed that IT security standards at many SMEs remain shockingly low.
- The ENISA report on SMEs published yesterday confirmed a picture of low preparedness and a continuing belief cyber attacks happen to other, larger companies.
- New insights:
  - Shadow IT problem exacerbated by Corona, without the control measures used in larger companies. This means they pose an even larger supply chain risk than before.
  - IT security standards usually designed for more mature companies.
So why aren’t SMEs buying cyber insurance?

• Signing up for cyber insurance costs time, money and effort, especially if the insurer suggests replacing outdated IT.

• Mistaken belief they will not be targeted (research shows recent experience of a cyberattack is a key motive for taking up insurance).

• Definitions and coverage options in the various policies are confusing – even brokers and large companies are struggling.

• Doubts whether insurers will pay out in the end – this is linked to the absence of universally accepted IT security standards.

• The insurance industry essentially ignores them – good money could be earned offering bespoke services to large companies.
How could compulsory cyber insurance work?

• Insurers would become the enforcers of a universal minimum IT security standard – this should be set externally.
• This should be condition for coverage – premium incentives will not work.
• Low premiums due to large market size.
• Coverage, support and access to incident response services for companies that so far refused to pay for cyber insurance.
• Insurers and companies would need between three and five years to prepare (similar to GDPR).
• Universal coverage will require a backstop mechanism to protect reinsurers from cluster or aggregate risk.