Legal challenges are shaping cyber insurance discussions

The latest EY Global Information Security Survey¹ reveals that only 65% of organizations believe they have cyber insurance that meets their needs. Two recent, significant legal actions indicate that as cyber threats and their associated risks increase, even the remaining 35% of organizations may not be adequately covered by insurance. The two cases, briefly described below, raise a number of questions about the direction of cyber insurance.

Exclusionary clauses – denial of coverage

A lawsuit claiming $100 million in damages was filed in the State of Illinois, US, alleging wrongful denial of insurance coverage. The complainant, a victim of a NotPetya attack², claimed the business was covered by a property insurance policy³ (not cyber insurance, specifically) providing insurance for:

- All risks of physical loss or damage to property
- Physical loss or damage to electronic data, programs or software, including physical loss or damage caused by the malicious introduction of a machine code or instruction
- Time-element coverage for actual loss sustained and extra expense incurred by the insured during the period of interruption directly resulting from failure of the insured’s electronic data-processing equipment or media to operate, resulting from malicious cyber damage

The complainant claimed losses as a result of property damage, commercial supply and distribution disruptions,

² In June 2017, a global cyber attack called Petya (also known as Petrwrap, NotPetya, Petna and GoldenEye) impacted organizations across a wide range of sectors, including financial services, power and utilities, media, telecom, life sciences, transportation and government agencies. It was speculated to be a nation-state cyber attack.
³ Usually commercial general liability and property insurance policies exclude cyber risks, which has led to cybersecurity insurance as a different line of coverage.
unfulfilled customer orders and reduced margins. The complainant asserted the cybersecurity breach caused damage to hardware and operational software systems, and rendered 1,700 servers and 24,000 laptops permanently dysfunctional. The complainant also alleged the insurance company denied coverage under the above policy based on a policy exclusion, which reads as follows:

“B. This Policy excludes loss or damage directly or indirectly caused by or resulting from any of the following regardless of any other cause or event, whether or not insured under this Policy, contributing concurrently or in any other sequence to the loss:

- hostile or warlike action in time of peace or war, including action in hindering, combating or defending against an actual, impending or expected attack by any:
  - government or sovereign power (de jure or de facto);
  - military, naval, or air force;
  - agent or authority of any party specified in i or ii above.”

According to the complainant, the denial of coverage placing reliance on the “hostile or warlike action” exclusion in the property insurance policy is improper. The case is still pending before the court.

Shareholder action against the board

A court in California recently approved a $29 million settlement in a data-breach-related derivative lawsuit filed against the board of directors and senior executives of a company that suffered several data breaches. Shareholders can use derivative lawsuits to act on behalf of the company against its directors and officers to redress harm done to the company. The allegations in the complaint included a breach of fiduciary duties, failure to implement safety mechanisms to prevent attacks, and failure to investigate and remediate breaches after they occurred.

The settlement amount will be paid by the insurance carriers. However, there was no admission of fault, nor was there a concession of liability on the part of the defendants.

Questions

1. As some cyber attacks are alleged to be motivated by nation-state-driven agendas, should the exclusion for warlike situations in insurance policies be renegotiated?

Similar to the first case cited here on denial of coverage, damages related to cyber crime may be covered by other insurance policies, such as property insurance. Traditionally, such insurance policies contain exclusions for warlike situations. Regardless of the outcome, the case is a reminder that discussions should be initiated between the insurer and the insured to better understand the scope and limits of coverage under the “hostile or warlike action” exclusion of the insurance contract. Such exclusionary clauses may need to be modernized through amendments or clarifications to take into account increasing cyber threats motivated by nation-state agendas.

2. Are insurance policies providing sufficient coverage for shareholder lawsuits that may follow a cyber breach?

Large monetary damages in data-breach-related derivative lawsuits are rare, but the settlement in the shareholder action discussed above will encourage future actions. This latent threat of shareholder action for cybersecurity breaches would in turn lead to an increase in the demand for adequate coverage under directors and officers liability (D&O) insurance policies. As a condition for increased coverage, insurance companies may demand adequate oversight of a cyber-risk management program from the board of directors. The oversight and appropriate actions taken by the board would also contribute toward a robust defense in the case of legal action by shareholders.

3. It seems like insurance premiums will rise as cybersecurity risks increase. What can be done to reduce costs?

Companies’ initiatives that mitigate risk and contribute toward better cyber hygiene could determine the risk categorization by the insurance company (high, medium, low) – i.e., the lower the risk, the lower the premium. Insurance companies may demand information related to the maturity of a cyber-risk program to determine the premium. A maturity evaluation may include an assessment of a company’s level of compliance with industry standards, set out in legislation or by regulators. It could also entail an audit of monitoring and incident-response programs performed by third parties.

Evolution in cyber insurance

Securing cyber insurance does not mean investing less in processes and controls that will lead to better cyber hygiene. Digitization and connectivity have increased exposure to cyber risk; as a result, cyber insurance premiums are also increasing, with the large retail and health care sectors seeing the highest increases. Partnerships between the insurer and the insured to strengthen cybersecurity practices could lead to lower premiums, broader coverage and less exclusions. This would benefit both the insured and insurer as the former can benefit from lower fees and increased coverage and the latter would face lower claims, which would increase profitability.
EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

EY member firms do not provide advice on US law.

© 2019 EYGM Limited.
All Rights Reserved.

EY no. 001576-19Gbl
BMC Agency
GA 1010249
ED None

In line with EY’s commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.

ey.com

Contacts

Author

Manu Mohan
EY Law, Lawyer
+32 2 774 9990
manu.mohan@be.ey.com

Contacts

Peter Katko
Ernst & Young Law GmbH
Partner, EY Global Digital Law Leader
+49 89 14331 25951
peter.katko@de.ey.com

Fabrice Naftalski
Ernst & Young Société d’Avocats
Partner, EY Global Head of Data Protection Law Services
+33 1 55 61 10 05
fabrice.naftalski@ey-avocats.com

Douwe Mik
Ernst & Young Advisory LLP
Associate Partner, EY Advisory Risk, Cyber Leader Netherlands
+31 88 40 74978
douwe.mik@nl.ey.com

Michael Payne
Ernst & Young Advisory LLP
Senior Manager, EY Advisory, Cybersecurity
+31 6 55 44 24 32
michael.payne@nl.ey.com