



Cyber Insurance as one element of the Cyber risk management strategy

Stéphane Hurtaud
Partner
Governance, Risk
& Compliance
Deloitte Luxembourg

Thierry Flamand
Partner
Insurance Leader
Deloitte Luxembourg

Laurent de la Vaissière
Director
Governance, Risk
& Compliance
Deloitte Luxembourg

Afaf Hounka
Senior Manager
Actuary Services
Deloitte Luxembourg

With the steady increase in cyber crime, many organisations across a variety of industries are susceptible to cyber attacks. Recent cyber attacks indicate that breaches are inevitable and can be extremely harmful. Cyber breaches can lead to tangible costs, brand degradation and changes in consumer behaviour.

In this context, many organisations have come to the realisation that a cyber attack is inevitable - it's not a question of 'whether' it will happen, but 'when'. Although it is impossible to be 100% secure, by developing a sound cyber risk management approach, organisations can implement a number of risk treatment measures for prevention, detection and response activities to keep cyber risks at an acceptable level. Furthermore, the ever-evolving cyber risk landscape is driving interest in cyber insurance as one complementary element of the cyber risk management approach, which allows organisations to transfer some of the risks associated with cyber incidents to their insurance provider.

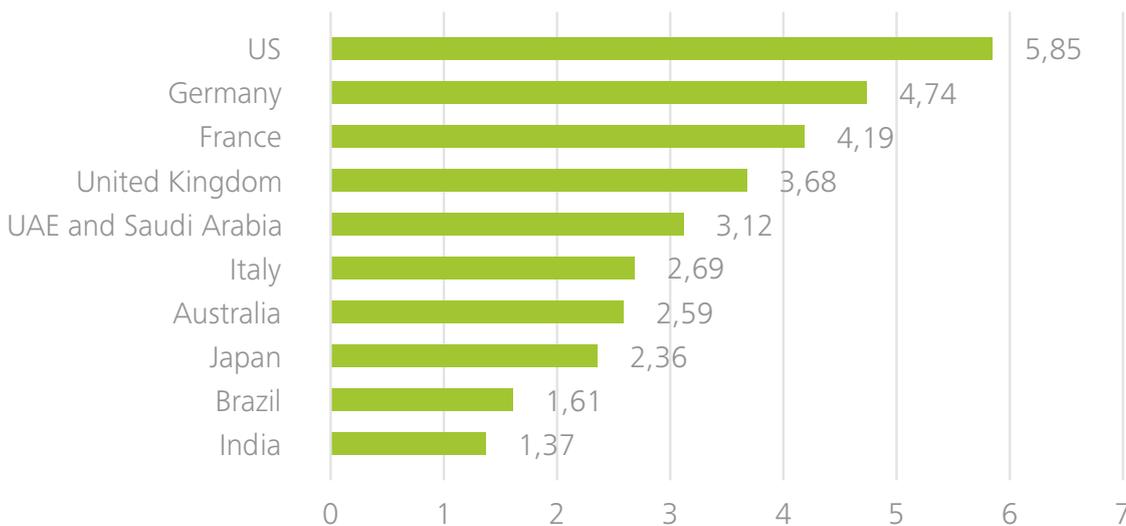
The cost of cyber crime

The largest data breaches in the last decade have cost each of the affected companies hundreds of millions of dollars.

- In 2014, the cost of a data breach ranged between US\$1.37 million and US\$5.85 million (depending on the country) (Fig. 1)
- Based on multiple analyst reports, the average cost per compromised record is anywhere from US\$78 to US\$277

The costs are attributable to investigation of the breach, remediation activities, notification of customers, credit monitoring, reputation management, legal fees and settlements, and regulatory fines.

Figure 1: Average total organisation cost data breach (measured in millions US\$)



Source: 2014 Cost of Data Breach Study: Global Analysis, Ponemon Institute

Today's cyber insurance market

Cyber insurance can complement an organisation's active security measures by providing insurance coverage in three broad areas:

- Liability for a data breach or loss
- Remediation costs (e.g. for investigating the breach, notifying affected parties, etc.)
- Regulatory fines/penalties and settlement costs

The demand for cyber insurance, along with the number of insurance providers, has been increasing as the use of technology has become so prevalent.

The U.S. cyber insurance market accounts for approximately 90% of the global market¹, with annual gross written premiums estimated in the region of US\$2 billion for 2014, up from US\$1.3 billion in 2013². It is important to highlight that many early adopters were financial services companies, retailers and healthcare organisations with large amounts of personally identifiable information (PII).

The cyber security insurance market has developed far more quickly in the United States than in the EU because of the former's mandatory data breach notification laws. However, the European market can be expected to catch up over the medium/long term, as the coming EU General Data Protection Regulation (GDPR) will likely require prompt notification of personal data breaches to supervisory authorities.

Cyber insurance is only one element of risk management and it will never be able to remove cyber risk entirely

Despite the increase in cyber incidents, cyber insurance adoption among organisations remains at a low level: according to the 'Chubb 2012 Public Company Risk Survey', 65% of the publicly-traded companies surveyed do not purchase cyber insurance, yet 63% of decision-makers are concerned about cyber risk. This is primarily due to:

- **Lack of awareness** - many executives underestimate the costs associated with cyber incidents and/or inaccurately believe they are already insured under the firm's general liability policy
- **Underwriting complexity** - the increasing number of data breaches has led several insurers to become more cautious, and prospective cyber insurance buyers might be daunted by the complexity associated with the underwriting process (e.g. level of detail of risk surveys, potential use of third-party risk assessments, etc.)
- **The challenge of aligning insurance coverage with risk exposure** - broad expertise in IT and risk management is required to have a proper understanding of the total cost of cyber risk to an organisation and to determine whether the proposed terms and policies satisfy the organisation's needs

Overall, the cyber insurance market remains immature, with room for improvement:

- A wide range of coverage is on offer, and policies vary significantly from one provider to another
- There is limited actuarial data available for insurers to adjust premiums based on what security controls and products are most effective
- Coverage is inadequate in some areas, e.g. cyber insurance does not do a good job at covering intellectual property theft or reputational damage, and the downturn in business that may result

² Gartner Inc.

³ The Betterley Report: Cyber/Privacy Insurance Market Survey 2014, Betterley Risk Consultants

Coverage provided by cyber insurance

Although traditional insurance policies may offer the option to cover some specific areas related to cyber risk, they are not designed to fully cover all the potential costs and losses.

Figure 2: Comparison between traditional insurance and cyber policies

	General liability 	Property 	E&O/D&O 	Crime 	Cyber 	
Network security	+	+	+	+	✓	
Privacy breach	+	+	+	+	✓	
Media liability	+		+		✓	
Professional services	+		+	+	✓	
Virus transmission	+	+	+	+	✓	
Damage to data	+	+	+	+	✓	
Breach notification	+		+	+	✓	
Regulatory investigation	+		+	+	✓	
Extortion	+		+	+	✓	
Virus/hacker attack	+	+	+	+	✓	
Denial of service attack	+	+	+	+	✓	+
Business interruption loss		+	+		✓	✓

+ Possible
✓ Coverage

Cyber insurance policies provide a variety of coverage options and pre-conditions that need to be considered when purchasing cyber insurance:

- First party coverage protects against losses incurred directly by the company in response to a cyber incident (direct expenses), and typically includes theft and fraud, forensic investigation, business interruption, extortion, and computer data loss and restoration
- Third party coverage: protects against losses incurred by third parties in response to a cyber incident, and typically includes litigation, dealings with regulators, notification costs, crisis management and credit monitoring

Cyber insurance is written and priced to suit individual customers. As such, cyber insurance policies may stipulate exclusions, impose limits, or add clauses to protect the insurer from higher risks

(e.g. non-performance of a cloud-computing provider, unencrypted devices that contain personal or other sensitive data, computer software malfunctions due to programming errors.)

In general, cyber insurance cannot provide:

- Protection from reputational risk - while a monetary claim can be awarded for an information security breach, the damage done to an organisation’s brand cannot be repaired as easily or transferred to an insurance carrier
- The removal of risk - insurance, whether cyber or otherwise, provides the organisation with the opportunity to transfer, not remove, risk
- A replacement for an information security programme - strong security controls and a comprehensive information security programme are prerequisites for purchasing cyber insurance

Figure 3: Typical premiums for cyber insurance

Size of Company (Based on Revenue)	Small Companies (Less than \$100 Million)	Midsized Companies (\$100 Million - \$1 Billion)	Large Companies (More than \$1 Billion)
Coverage	\$1 – 5 million	\$5 – 20 million	\$15 – 25+ million
Yearly Premium (Cost for Coverage)	\$7,000 – \$15,000 per million in coverage	\$10,000 - \$30,000 per million in coverage	\$20,000 - \$50,000 per million in coverage
Typical Coverage Sublimits (Restrictions on Payout)			
Sub-limits can restrict payouts on a single aspect of coverage from 10 – 50% of the total coverage			
Notification Cost	\$100,000 - \$500,000 limit	\$500,000 - \$2 million limit	\$1.5 - \$2.5 million limit
Crisis Management Cost	\$250,000 - \$1.25 million limit	\$1.25 - \$5 million limit	\$3.75 - \$6.25 million limit
Legal and Regulatory Defense Expense	\$500,000 - \$2.5 million limit	\$2.5 million - \$10 million limit	\$7.5 - \$12.5+ million limit

Source: Deloitte research on insurance provider Web sites

As an example, consider a large credit card processor that purchased a cyber insurance policy with coverage of US\$30 million against a cyber incident. Unfortunately, a data breach involving several million credit cards resulted in the company paying over US\$145 million in compensation for fraudulent payments. In this situation, the insured party had to pay out US\$115 million and was not adequately covered.

In order to gauge the cyber coverage organisations need more effectively, insurers have started to implement a more rigorous procedure for underwriting cyber insurance policies.

This procedure includes a number of well-defined steps:

- **Initiate** - the cyber insurance broker/provider asks the customer to complete a self-assessment form on its information technology (IT) and security environment
- **Assess** - the cyber insurance provider reviews the assessment, then arranges an onsite assessment of the customer. For higher risk customers, the cyber insurance provider requests a third-party risk assessment to be performed on the customer, with the cost charged to the customer
- **Review** - the third-party risk assessment partner provides the results to the cyber insurance provider based on baseline IT and leading security practices
- **Report** - the cyber insurance provider uses the third-party risk partner's recommendations to produce its own assessment report
- **Underwrite** - the cyber insurance provider finalises the coverage and any exclusions, and calculates the premiums based on its assessment report

Key considerations for selecting cyber insurance

When selecting a cyber insurance policy, we recommend paying attention to the following considerations:

Understand your organisation's risk exposure

- Evaluate your current cyber risk exposure to understand the type and amount of cyber insurance coverage required
- Coverage may not be required in areas where controls are well established and routinely tested

Understand policy complexities

- There are a wide variety of insurance policies available, often requiring a rigorous underwriting process - spend time upfront understanding the pre-conditions that need to be met in order to obtain insurance
- It is also important to understand any policy exclusions to make sure that you are able to take advantage of the coverage you will be paying for

Balance the cost of premiums and of implementing controls

- While insurance policies may assist in transferring risk, organisations should conduct a cost-benefit analysis to determine the appropriateness of investing in cyber insurance coverage
- Make sure you are buying cyber insurance to cover the risks that cannot be addressed in-house

Understand the claims process

- Not all cyber claims are treated equally - know what will be needed to file a claim and make sure you can satisfy these requirements before purchasing insurance
- When an incident happens, insurers often require organisations to execute a formal incident response process - including saving logs, emails, forensic scans and other evidence - using methods that preserve the integrity of the evidence

Cyber insurance products are no replacement for a robust information security programme.

Cyber insurance is only one element of risk management (i.e. risk transfer), and it will never be able to remove cyber risk entirely. Organisations should first develop mature information security programmes and an understanding of the total cost of their cyber risk before seriously considering cyber insurance.

