Cyber security

IR Newsletter August 2017

Cyber security

Rapid technological developments have enabled companies to distribute products and services globally but also added new risks for private individuals and companies.

Accounts can be settled at the glimpse of an eye and global communication is handled at a scale hard to imagine 20 years ago when the fax machine was still an important piece of equipment in every office.

New opportunities have, however, also resulted in a new vulnerability towards new types of risks that need to be addressed. When companies rely on robots in production lines or logistics, they are exposed to errors in the software controlling these processes. If a company sells products online, it may retain sensitive credit card information that can easily be copied or distributed on the internet, potentially resulting in losses for both the individuals and the company that lost the information.

From an insurance perspective, risks associated with the technological development or cyber risk [a] is a multifaceted risk that affects companies and private individuals across traditional risk types such as Property, Business Interruption and Liability. It is, however, also a risk that goes beyond traditional insurance lines.

From being an issue for the IT department, cyber risk is growing into being one of the most important business risks and the handling of IT is becoming a matter for top management and board discussions.

"Everyone is at risk of being exposed to cyber attacks all the time."

[Marika Frederiksson, CFO, Vestas Wind Systems] [b]

Tryg has always been focused on supporting its customers by advising and covering the risks they face. It is therefore natural for us to engage in the development of insurance solutions addressing cyber risk as perhaps the most pressing emerging risk for businesses across all sectors.

Criminals are going digital

Globalisation has benefited all kinds of business and individuals. Unfortunately, criminal activities related to cyber crimes have increased sharply both in terms of numbers and amounts.

In essence, crime in the digital world is just like in the physical world. If you have valuables that can be converted into cash, criminals will try to steal it and if you are dependent on specific resources to run your business, criminals can threaten you to pay a ransom or 'protection money' to keep it from being destroyed.

Some of the most diffused types of cyber attacks are shown in the box below. Though they vary in nature and effect, they pose threats to a company potentially resulting in substantial financial losses. One of the most discussed threats recently has been ransomware. A virus that encrypts your data and then offers you to unlock it after paying a ransom. In May 2017, 300,000 computers worldwide were affected by the ransomware 'WannaCry' that exploited a bug in an outdated version of Microsoft Windows to spread and encrypt files on computers all over the world. Among the victims were several hospitals, railways and other critical industries.

Though WannaCry is perhaps the most exposed cyberattack to date, it is by no means new. In July 2001, the Code Red worm infected 350,000 servers worldwide and among other things launched a denial of service attack on the website of the White House. Cyber attacks are not a new phenomenon but the technical expertise needed to launch an

Ransomware	A programme that encrypts the victim's files and offers to release the data against payment of a ransom
Malware	General term for malicious software
DDOS	Distributed Denial Of Service. A coordinated attack on the victims' webpage resulting in it not being able to function
Advanced persistent threats	A type of hacking that focuses on not being detected, thereby enabling the perpetrator to tap the victims' data over an extended period of time
Phishing	Sending emails with the intent of luring the receiver to inadvertently install a malicious software
Spear fishing	A scam based on emails to specific individuals e.g. the CFO requesting a money transfer or a confirmation of password

a) There are several definitions of cyber risk. Here the term is used to describe any risk emerging from the use of information and communication technology (ICT) that compromise the confidentiality, availability or integrity of data.
b) Source: www.borsen.dk

attack has reduced dramatically. It is now possible to order a tailor-made cyber attack on the so-called 'Dark Web' including ransom note and a control screen to monitor how the proceeds come in.

"Cyber attacks have become a major challenge for everyone and the consequences of being hacked can be severe. We are very much aware of that."

[Mads Nipper, CEO, Grundfos] a)

Email threats

Whether it is ransomware or other threats, the most common way for a criminal to enter the victim's IT systems is through an email which includes a link or an attached file. Disguised as attractive offers for cheap designer clothes or important messages from a supplier, the employee receiving the mail is fooled into clicking the link or opening the file, thereby opening the door to the company's internal drives. More than 90% of cyber attacks starts with an email. Thus, education of the staff and implementing an awareness culture is an important preventive measure.

a) Source: www.borsen.dk

The number of people connected to the Internet has grown from approximately 700m in 2000 to 3.2bn in 2015 according to the International Telecommunication Union that is a seven-fold increase that brought Internet penetration from 7% to 43% of the global population. Internet communication is vital in the digital world and the threat from cyber criminals is quickly taking an important place in executives boardrooms around the world.

The insurance market for cyber risk

Corporations around the world have been forced to include cyber risk into their risk management practice including ways to control and mitigate this through the purchase of insurance.

Especially the risk of loss of data has been an important driver of the development. In 2003, the first regulation concerning data breach was introduced in California, requiring a company which had lost data on individuals to disclose the loss and to notify the affected. Since then all but a few American states have introduced similar regulation. Costs associated with a data breach will not be covered by the traditional insurance products, and with the dramatic development in the amount of data stored and the reputational risk connected with a data breach, this has been a main driver for the development of cyber insurance in the US.

By 2018, the EU regulation named the General Data Protection Regulation will implement similar conditions in the European market to those in the US. Together with the increasing focus in recent years' on cyber-related risks, it is expected that also Europe will experience a development similar to the one seen in the US.

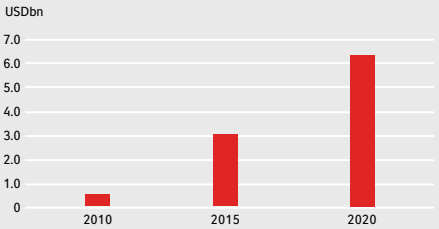
As mentioned, cyber risk transcends traditional insurance lines that typically focus on either first party loss, i.e. loss to the insured's own assets (e.g. fire) or third party losses, i.e. loss incurred by a third party, but where the insured carries the risk (e.g. liability or workers' compensation). Looking at the standalone cyber insurance cover, it usually includes both first and third party losses and is as such a hybrid between the traditional insurance coverages. First party losses include restoration of data, business interruption with no physical damage e.g. in case of a virus attack, IT forensics and costs associated with finding and notifying individuals whose data has been lost.

In Scandinavia, the largest corporations have been purchasing cyber insurance through the international insurance markets for some years, but the demand in the SME market has been limited. Over the last year, however, the awareness of cyber risk as an important risk for companies of all sizes has increased together with the demand for cyber insurance.

Market development

Since the first cyber risk covers were introduced in the 90s, the US has been forerunner in the development. Especially the data breach regulations mentioned earlier have resulted in an increase in

Market development in the US



Business interruption

Car maker Renault was hit by the WannaCry virus in May 2017. In the effort to clean the computer systems, production had to be shut down in many factories around the world.

Worst hit was the plant in Douai in Northern France which was out of production for more than 24 hours.

In June 2017, the Danish shipping giant Maersk was hit by a virus that interrupted operations for several days. The attack was announced on 27 June and not until six days later, the company could announce that all major IT systems were back in operation.

These examples highlight the fact that business interruption is a major part of cyber risk.

the demand for insurance. After 2011, the growth has been high starting from a level of around USD 0.5bn reaching approximately USD 3.0bn in 2016 (PWC estimates). Europe including Scandinavia, has lacked behind the US in this development and Tryg estimates the Scandinavian market at less than USD 50m in 2016.

Recently A.P Moller-Maersk, an integrated transport and logistics company, which is also a global leader in container shipping, was hit by a cyber attack. On June 27, a malware, later known as NotPetya, distributed through an Ukrainian accounting software used to file tax returns in Ukraine, hit many global companies. Maersk has disclosed in its Q2 report that the associated cost of this attack is in the region of USD 200-300m of which the majority relates to lost revenue in July. Incidents like this are likely to increase attention to the cyber risk topic and therefore impact the overall importance of the product.

"The Maersk attack left a big impression [on our view on cyber attacks] ... We have subsequently reviewed our own systems, but there is no guarantee that we will not be exposed to similar attacks in future."

[Cees 't Hart, CEO, Carlsberg] [a)]

Assuming the introduction of the general Data protection Regulation, supported by the increased focus on cyber risk and also based on the recent Maersk experience, Tryg expects this to result in significant growth rates in the European and Scandinavian markets for cyber insurance.

Risk management

As goes for all risks, insurance is not intended to replace careful behaviour, robust IT governance and good risk management. Insurance is a safety net that can help to reduce the risk and consequences in the event an organisation is faced with a cyber threat or intrusion.

Experience tells us that even the most resilient IT setup cannot guarantee against cyber risk in future. A cyber insurance can assist in dealing with the aftermath of network security incident. Organisations will have varying levels of IT sophistication and capabilities to handle an incident on their own, and this will reflect their needs when it comes to coverages and how an insurer should respond. No matter the size and complexity of the company there is a need for a quick response to any event to cease an attack and restore daily operations as quickly as possible.

Assisting after a cyber attack is a complex task which includes many things and not only related to IT. Making sure that the network and operations is restored is merely the first step followed by handling of suppliers and clients affected by the breach, restoring credibility and addressing a possible legal liability exposure or compliance issues. Finally, there is also the importance of effectively communicating with the public and the market as steps in protecting the client's brand, restoring trust and mitigating a potential reputational damage following a breach and where sensitive data may have been compromised.

Tryg's approach

Tryg's Cyber insurance has been launched across Denmark, Norway and Sweden with a unified solution for claims-handling addressing all of these needs. The product offers client access to an incident hotline with 24/7 availability and first party coverage with incident response and remediation costs covered.

Clients get access to experts that keep up to date with threats and specialise in dealing with network security breaches and will be able to provide valuable insights and assistance to any company faced with a threat of and attack or actual breach.

In order to ensure access to the relevant expertise within this field, Tryg has teamed up with external partners both in terms of assessing the risk as well as claims handling. The cooperation ensures that the handling of claims gives our clients access to an international network of not only IT forensics and on site field service, where necessary, but also a network of providers of a wide range of services from law firms and PR agencies specialising in data breach and personal data legislation.

From a portfolio perspective, one of the important features of cyber risk is the risk of accumulation, i.e. the simultaneous occurrence of a large number of claims due to the same underlying cause. In this respect cyber risk is comparable to other perils like windstorm, flood and earthquake. Tryg is highly dependent to the reinsurance market for cyber insurance especially for claims related to business interruption. It is important to note that this market is only gradually developing as the sums insured, so far, have been relatively small.

The typical cyber risk claim will involve assistance in data restoration and getting the IT systems up and running, which is a process that is substantially shorter than the rebuilding of a house damaged by flood. For the individual company, the claims prevention for cyber risk is very much aligned with the ordinary operations as it involves ensuring back up of data and systems, up to date virus protection etc., all of them precautions that are gradually becoming natural for most companies.

Besides offering a relevant product to the clients, it is therefore also important for Tryg to keep control of the risk taken on board in writing cyber insurance. This is partly done through restricting the sums insured as well as reinsuring a large part of the risks.

Tryg offers cyber insurance coverage in the Danish market both for our SME and our corporate customers. In the SME segment, we cover the costs related to re-starting IT systems after a cyber incident. Business interruption coverage is sold as an add-on. Commercial Denmark has been selling cyber insurance for approximately six months and around 5% of our Danish customers have currently bought that coverage.

a) Source: www.borsen.dk

In the Corporate segment, Tryg covers data restoration, business interruption and media liability. The product is currently 90% re-insured as this is a new segment where claims patterns are little known. Tryg works together with Charles Taylor, an international loss adjuster, as many of our customers have international operations hence it is important to have a global partner. Currently around 3% of our Danish Corporate customers have bought this coverage.

Summary

Cyber risk is definitely the most rapidly developing risk type and it is important for the insurance sector to follow this both in terms of developing products relevant for the clients and in terms of assessing and controlling the risk.

Tryg sees a large potential in the market for cyber insurance in Scandinavia. With the GDPR entering into force and increasing awareness of the cyber threat on most boards' agendas, the selling of cyber insurance will inevitably see a steady increase in future years with Tryg establishing a strong footprint in the market.