Study Tour USA:

Cyber Insurance – Europe in Footsteps of USA

Introduction

In 1995 only 1% of the Europeans had access to a computer at home. By 2011 that number had increased to 73%. In 2010 36% of the EU citizens banked online. Connected devices is said to amount to 9 billion worldwide and the number will increase to 24 billion by 2020.[1] The internet is everywhere and numbers will continue to grow; it has by far proved to be not only a passing fad as the Swedish minister of Communications uttered in 1996.

Along with growing numbers and increased activities over the internet, cyber security has become ever so topical. As more and more sensitive data is stored on computer systems all over the world every element of society including government, industry, commerce, health care, education and individual citizens is progressively at risk.

The average frequency cost of data breaches increased in 2010/2011 to USD 7.2 million in the US, USD 3.4 million in Germany and USD 2.6 million in the UK, whilst the number of catastrophe claims reached new levels. Recently Sony was forced to shut down its PlayStation Network (PSN) following a security breach that may have exposed the credit card details of up to 77 million customers at a cleanup cost of approximately USD 178 million.[2]

The first breach notification law was passed 2003 in California. To date a majority of US states have enacted laws for notification obligations on organizations.[3] In Europe winds are blowing in the same direction as the European Commission in early 2012 proposed reforms for the European data protection legislation.

Data breach regulations has been a major driver for cyber insurance in the USA, where 90 % of the cyber budget is spent, and now Europe seems to be next.[4]

Understanding Regulatory Differences between USA and Europe

USA

Although there is not (yet) any single federal statute on data protection in the USA, a total of 46 states have passed individual laws on mandatory notification obligations on organizations that discover a breach of security involving personal information.

All state laws are based on the Californian law, which made it mandatory to notify security breaches involving unauthorized acquisition of computerized data including

[1] Strategic Risk, "Guide to: Cyber risk management", 2012
[2] Schwartz, Matthew J., 2011
[3] Practical Law Company, "Data Protection", 2012/13
[4] Nyman, Francesca., 2012-08-16. Hill, Patrick.

certain types of personal information relating to individuals residing in California. Notifications must be made soonest possible but the law does not apply to any public authorities.

The California law was recently altered commanding a notice to the California Attorney General if more than 500 Californians are affected by a breach. Most state laws require notifications when certain personal information were, or are reasonably believed to have been, acquired by an unauthorized person. Some states however do not require a notification if the security breach is not likely to cause harm (for example identity theft). Another 14 states have adopted the Californian amendment and require notification to a state authority, however without the threshold trigger.[5]

The different state laws might be faced with a harmonization as a Data Breach Act was introduced in the US Senate in June 2012. If enacted, organizations collecting and maintaining personal information would have to secure this information and to provide notice to individuals affected by a security breach involving personal information "as expeditiously as practicable and without reasonable delay". The act would preempt State laws and be effected a year after enactment.[6]

Europe

Though the European Parliament and Council Directive 95/46/EC regulates the processing of personal data within the European Union, there is no general breach notification requirement applying to the EU states. So far many European countries have passed their own national laws on mandatory notification obligations with the main purpose to enable authorities to exercise their regulatory oversight functions, such as identifying security problems and deal with them.

In January 2012 the European Commission proposed a comprehensive reform with several changes to the data protection rules. The changes are meant to simultaneously simplify and toughen the rules in the 27 different EU countries to guarantee privacy rights in the future. The proposal contains two legislative proposals: a Regulation setting out a general EU framework for data protection and a Directive on protecting personal data processed for the purposes of prevention, investigation or prosecution of criminal offences and related judicial activities.[7]

Among rules for stricter sanctions and the right to fine violations, the proposal includes a much-debated requirement for companies operating in Europe to disclose data breaches as soon as possible and if feasible within 24 hours. Should a company break the 24-hour rule it could face penalties of up to EUR 1m or up to 2% of the annual global turnover. Companies based outside the EU would also be affected by the rules if they are active in the EU market and offer their services to EU citizens.[8]

[5] Ibid.
[6] Weiss, Marie-Andree., 2012-07-06
[7] European Commission Press Release, IP/12/46, 2012-01-25
[8] Rashid, Fahmida Y., 2012-01-24

Cyber Insurance

Prior to the end of the 1990's there was hardly any policy language that expressly included or excluded coverage for cyber risk. When a growing number of companies began to rely on their information infrastructure they began to file claims towards property policies for first-party data loss and software damages originating from advertisers (trademarks, copyright). Claims were then either paid because of vague policy language or litigated essentially to establish whether property was tangible (covered under property insurance) or non-tangible (not covered).

Since 2000 it has been more or less accepted in courts and insurance industry that standard property and liability insurance programs are not designed to cover typical cyber claims, which has been reinforced through explicit cyber exclusions in the wordings.

As a consequence insurers began developing a product designed to cover the financial loss that might arise out of a data breach, mainly to target big "dotcom" companies like Yahoo, eBay, Google etc. that pioneered e-commerce and online retailing. The new type of insurance was called "cyber insurance". [9]

Cyber insurance proved slow to take off, partly because the introduction coincided with insurance buyers attempts to decrease insurance costs and partly because the need for the coverage was not fully clear. The first policies included liability (claim expenses and liability arising out of a security breach of the insured's computer systems) as well as property (business interruption and data asset loss/damage arising out of a data breach) components.

Shortly after the passage of the California breach notification law big breaches lead to class action lawsuits. Along with organized crime effecting the frequency and magnitude of breaches cyber threats became financial rationale and insurance cover developed into covering the direct costs related to breaches.[10]

Cyber Threats

The very nature of computer networks is such that they allow authorized users to send and receive information. While there may be "guards" watching the inflow and outflow of information they can be tricked to allow information to head in either direction.

The lion part of data breaches occur because of human errors or bugs in the system. Errors like these often occur due to organizations failure to observe basic security procedures and to encrypt sensitive information; laptops can be stolen or altered, e-mails with sensitive data can be sent in error etc.

[9] Navetta, David., 2012-02-01
[10] Schoenberger, Steve.

The number of individuals as well as organized criminal gangs stealing personal data for personal gain has increased significantly. Theft can be achieved through the use of computer viruses or malware that in the end gives the criminal access to sensitive data.

Spear phishers send e-mails alleging to come from a trustworthy source in order to acquire personal information such as bank details, passwords or user names which can enable fraudsters to gain access to individuals' bank accounts, credit or store cards.

A new trend in hacking is to hack into an organization's computer system in order to protest or promote a political viewpoint or simply for the sake of challenge. Usually this type of hacking is not aimed to gain personal profit but to take an ideological stand through website hijacking, conducting e-mail campaigns or anonymously blogging, all of which can damage a business' reputation.

Denial of Service (DoS) attacks occur when a site is hit by a large number of visitors at the same time making the system overload and crash before it is taken offline. The DoS attacks can cause major disruptions to the businesses, damage consumer trust, harm the brand reputation and in the end affect the company's brand and share price in a negative manner.

Hackers may threaten to carry out a Denial of Services attack, to disclose valuable information (such as trade secrets) or to introduce a Trojan virus in exchange for a ransom. In order to keep share price intact and reduce the risk of copycat attacks cases of cyber extortion are often kept in the dark.

Cloud computing, meaning the outsourcing of data storage, in order to access cheaper, up-to-date systems and meet the need for flexible and home working can mean risky business. The responsibility for the company data is transmitted to a third party whose servers or internet locations are often not located in the same country and jurisdiction as the client. As a result difficulties occur as regards to establish whether the company is compliant with relevant local legislation. The outsourced firm is also often strictly limiting its liability, leaving the risk with the outsourcing company.[11]

Cyber Insurance Coverage

Though the core cyber coverage is impartially consistent among the insurers, the names used are far from it. Similar products are named cyber liability, network security liability, data breach liability, security and privacy liability, privacy breach coverage etc. The covers available can broadly be divided in two parts; damage to a company's own system (first-party loss) and third party liability (third-party loss).

[11] Lockton., February 2012

Typically first-party loss includes damage, loss or corruption of data and software arising out of non-tangible events such as virus, hack power surge or programming error. Insurance is to provide for costs to research, reconstruct or recreate the lost or damaged data. Insurance coverage is also accessible for loss of income arising from the preceding damage, not only generated by online sales but also subsequent offline business loss. First-party cyber loss also includes additional operating expense and expenses due to cyber extortion.[12]

Third-party loss usually includes injury arising out of content or information made available on a website or distributed through email. Typical infringement claims through website content include libel, defamation and trademark or copyright infringement. One of the greatest sources of cyber liability is the unauthorized access of confidential information such as client data, trade secrets, personal health records or financial information. Most organizations are in the possession of information that if released could lead to third party claims but obvious examples are health care and banking businesses. Insurance would cover attorney fees, forensic investigation expenses, printing and mailing costs, credit monitoring expenses, call center expenses.[13]

Cover under Alternative Insurances

Property policies are traditionally constructed to cover damage to tangible property perils as fire, flood and earthquake. Usually property damage is also required before the business interruption or extra expenses cover kicks in. Insurers usually hedges against the risk of paying damage to non-tangible assets by excluding damage to data information stored in electronic format (if not caused by fire, flood etc.). Some insurers might be up for extending cover to include malicious damage and destruction of data to a certain sub-limit.[14]

Crime policies often exclude the theft of information such as trade secrets but can be extended with coverage for Computer Sabotage, DoS and Virus contamination to certain limits and conditions.

General liability (GL) programs are mainly designed to cover liability due to property damage or bodily injury. Additionally the GL policies often include a narrow scope of coverage for “advertising and personal injury”.

Errors and Omissions (E&O) or Professional liability programs can partially be custom-made and thereby, explicitly or implicitly, provide coverage for third-party liabilities to a certain extent. Since the E&O insurance usually is activity specific it

[12] Schoenberger, Steve.
[13] Ibid.
[14] Green, Paula., September 2012

may not correspond to claims arising out of a network unrelated to the delivery of a product or service such as the spread of a virus to an affiliate or supplier.

As kidnaps, extortions and hijacks are increasingly prevalent globally, Kidnap and Ransom (K&R) insurances are becoming more important. A traditional K&R insurance could provide adequate cover for cyber extortion events.

Intellectual Property (IP) insurance protects businesses against claims based on alleged infringement of IP (defensive cover) as well as covers expenses for pursuit due to alleged infringement of the company's IP rights (offensive cover). A specialized IP insurance could cover elements that are covered under a cyber insurance policy.[15]

Thoughts on the Need for Cyber Insurance and its Future in Europe

Insurers often point out that there is no comprehensive cover for cyber risks offered under any other insurance form than the cyber risk insurance. They seem to be correct in terms of a comprehensive cover; however, certain elements of the risks can be covered under alternative insurances. As cyber insurances usually are dividable, businesses could save premiums and avoid double insurance situations by taking an extra look at their current insurance cover. Inadequate cover under property insurances and the current absence of mandatory breach notification laws makes at least the first-party coverage attractive to European businesses today – business interruption and damage to a company's brand can be crucial. Insurers' fingers are however crossed whilst they hope for increased demand for third-party cover.

Since compulsory breach notification was a key factor when cyber risk insurance grew in USA, the introduction of stringent cyber security regulations in the EU reform is expected to boost the cyber insurance market in Europe. Even though the draft EU data breach notification regulation might be altered and possibly linger a couple of years before it is in place the proposal seem to have changed the game.

Kristina Strandberg

[15] Ibid.