CYBER CRIME: THE ACHILLES HEEL OF THE BUSINESS WORLD

Businesses are increasingly the victims of cyber attacks. These crimes are not only costly for the companies, but can also put their very existence at risk and may provoke significant externalities for third parties. The fact that businesses are becoming more and more tech-dependent and interconnected adds to an increased cyber crime presence. The pace of innovation is escalating rapidly among threat sources, helped by an acceleration in the global proliferation of cyber expertise. Sharing information is a solution. What about insurance? The market is growing - fast - but faster grow the risks!

The World Federation of Exchanges reported in July 2013 that half of the 46 exchanges it surveyed had been victims of cyber attacks in the previous year. In a 2013 Financial Times article, the Depository Trust and Clearing Corporation, which processes large securities transactions for U.S. capital markets, described cyber crime “as arguably the top systemic threat facing global financial markets and associated infrastructure.”

Cyber attacks are not limited to the financial sector. A multitude of companies of different sizes and across sectors incur losses as a result of this crime. According to the IdentityTheftResourceCenter, a nonprofit research and education group that aids cyber-crime victims, at least 441 U.S. companies, government agencies, and other institutions reported material breaches to their computer networks during the first three quarters of 2013. This figure likely underestimates the real magnitude of the crime. As Michael Levy, chief of computer crimes at the U.S. Attorney’s Office for the Eastern District of Pennsylvania, notes, “Companies often don’t know that they have been victims of cyber attacks, and if they do know it, they are reluctant to disclose such

intrusions” because they fear this might damage their reputations or cause them to lose their shareholders’ confidence.

The fact that businesses are becoming more and more tech-dependent and interconnected adds to an increased cyber crime presence. Based on the 2012 “Cost of Cyber Crime Study” published by the Ponemon Institute — a research center dedicated to privacy, data protection, and information security policy — U.S. organizations experience an average of 102 successful cyber attacks per week, more than double the total for 2010. Costs linked to cyber crime rose by nearly 40% compared to 2010 and reached an average annual cost of US$8.9 million for the U.S. organizations that are part of the sample benchmark. The same report points out that 78% of these costs are caused by malicious code, denial of service, stolen or hijacked devices, and malevolent insiders. PA Consulting, a consultancy specializing in management, technology and innovation, estimated in a March 2012 blog post, published in the Future of Business, that “roughly 80% of the value of a typical company is exposed in cyberspace” and that “a typical advanced attack costs the victim in excess of US$150 million, with an average of 12% wiped off the market cap of a company in the immediate public aftermath.”

Source: Office of the Attorney General State of Mississippi

In addition, cyber criminals are more sophisticated than ever as the cost of equipment has fallen significantly in recent years, hence allowing a new generation of cyber criminals — often based in emerging countries — to develop elaborate attacks that circumvent cutting-edge cyber-security systems. Matt Hartley, senior director at the cyber-security consultancy firm iSIGHT Partners, notes that “cyber attackers are increasingly sophisticated. The pace of innovation is escalating rapidly among threat sources, helped by an acceleration in the global proliferation of cyber expertise.” As examples of the transfer of more sophisticated approaches, he cites not only the Stuxnet worm, but also recent attacks that targeted the oil and gas industry, such as the data-destruction attack against Saudi Arabian oil company Saudi Aramco in 2012. In this attack, considered to be one of the most destructive against a single company, a group of hackers calling themselves the “Cutting Sword of Justice” managed to shut down 30,000 Aramco computer workstations and to delete all of their data.

Cyber warfare damages for a company can go beyond business interruptions and the destruction of strategic data. They include cyber espionage, intellectual property loss, identity, and sensitive data theft, as well as the losses that affect third parties such as customers. What will be the real consequences of the security breach e-commerce startup LivingSocial experienced in April 2013, which involved the data of more than 50 million customers? Businesses can suffer not only from direct losses, but also from indirect losses such as brand and reputation damage. Depending on their jurisdiction, “companies may also be responsible for negative externalities they may have not directly caused and for the lack of compliance to an increasingly stringent regulation in the event of cyber incidents involving third parties,” notes Bradley Gow, a cyber insurance pioneer from specialty insurance provider Endurance.

 Companies that are more aware of the increasing threat of cyber warfare, especially global brands and players in the banking and energy sectors, are increasing their annual budgets for cyber security and defense. The trend is to move from a reactive to a proactive approach and to adopt “intelligent security” strategies. Cyber security is about understanding the cyber threats to a company and acting upon them. However, even in these best-in-class companies, cyber security often remains isolated and is rarely integrated into the company’s other strategic areas. According to Hartley, “Companies must move from a mostly-isolated and technology-centered security operation to a unified security organization, tying technology, security and intelligence on threats together. Those [people] leading security and technology teams should be connected and in constant communication with those [who are] heading operations, marketing, finance, and strategy, all the way up to and including the CEO and board.”

Sharing information

A higher degree of cyber security discourages opportunist attacks, but does not offset the risk of being the victim of a targeted attack. Different strategies are being adopted to minimize the risk of such attacks in terms of frequency and impact. Large banks have created the Financial Services-Information Sharing and AnalysisCenter (FS-ISAC) to share information about attacks and how they managed to repair the breaches in their systems in order to prevent similar attacks from happening to other members of the organization. Despite being initially reluctant to share sensitive information, large financial institutions understand that such practices will benefit all of them in the medium to long term by reducing the frequency of their losses. Institutionalizing ways to reduce damages from cyber attacks implicitly recognizes that all companies’ IT

platforms are vulnerable, no matter what their cyber security policy's level of sophistication is.

Hartley points out another way in which companies are currently preventing damage, especially in the tech industry. Facebook has a white-hat system that encourages cyber experts — so-called "cyber researchers" — to disclose security gaps discovered in its technology. They are paid a minimum of US$500 for each critical gap reported, and there is no cap to such compensation. In this way, Facebook gathers data on its platform's shortfalls before they can be exploited by malicious intent. However, paying the researchers is effective only if their impetus is money, which is not always the case. Money would unlikely have stopped Julian Assange from creating Wikileaks and Edward Snowden from leaking top-secret government information. Also, as the provenance of cyber attacks suggests — a considerable number of attacks originate in China, the Middle East, and the Commonwealth of Independent States — political motives are becoming increasingly common.

Because even those companies that invest the most in cyber security are vulnerable, it would be reasonable to expect an approach to cyber risk similar to what companies apply with respect to other risks they face: insurance. This is not the case. While virtually all American businesses are insured against natural disasters and terroristic attacks — the latter being covered by the Terrorism Insurance Act of 2002 — only a few businesses cover their risk within their insurance package. As Levy notes, "If a company does not appreciate that there is a risk, it does not address it." Nevertheless, the economic damage resulting from cyber attacks can be as great as that of a natural disaster, and the impotence of businesses in the face of cyber criminals is similar to what they experience in the face of terrorists.

According to Gow, "cyber insurance products were commercialized at first in the 1990s when dotcom companies started going public and had to justify in their IPO prospectus how they were mitigating their

exposure to hacker threats and viruses." New regulations on privacy supported an initial expansion phase of cyber insurance, which companies used as protection against the potential lack of compliance with legal requirements in the event of personal data loss. Nonetheless, as pointed out at a November 2012 U.S. Department of Homeland Security workshop focused on cyber insurance by Tyler Moore, professor of computer science and engineering at Southern Methodist University, "the cyber security insurance market today is small and has underperformed expectations." Because businesses are often unaware of the cyber risks they are exposed to, they are reluctant to pay a premium to cover such risks. However, justifying the underdevelopment of the cyber insurance market with a lack of demand is simplistic. Had the insurance industry found the business opportunity linked to cyber insurance attractive, it would have pushed cyber insurance products by educating its client base more convincingly and creating a need for cyber risk coverage.

Difficulties quantifying risk

Jean Lemaire, a professor of insurance and actuarial science at Wharton, explains from an outsider's perspective why cyber insurance may not be seen as a lucrative segment for traditional insurers: "Unlike natural disaster risks, cyber risks are not independent, and [they] evolve rapidly. These two peculiarities, coupled with the lack of data, make it difficult for insurance companies to quantify the risk and the size of damages, which are necessary to calculate premiums." In addition, potential losses following a cyber attack vary from company to company depending on the industry and the company's business model, its positioning and reputation, and its association with certain causes and values.

Moore notes that, after a first development phase along with the Internet bubble, cyber insurance growth slowed down following the Y2K fears and the 9/11 attacks, the magnitude of which insurance companies had not anticipated. Hence, premiums increased, and insurers began to remove cyber risk coverage from their general policies. In addition,

“policies are typically capped at $1 million to $50 million and contain unpopular exclusions.”

Gow adds that insurance providers typically limit their exposure to any single cyber account to US$10-US$20 million. Although companies often purchase policies from different providers, such a strategy reduces their cyber-risk exposure only marginally. Moreover, companies were unsuccessful in their attempts to file claims under their commercial general-liability insurance policies, which often exclude explicitly cyber-related incidents. Gow recalls the legal dispute between Zurich Insurance and Sony, which was decided in favor of the insurer in 2011.

“Cyber insurance is today a specialist market, underwritten separately, which accounts for approximately $1.3 billion in premiums,” notes Gow. “Despite being relatively small compared to its potential, the market is among the fastest growing segments of the insurance industry and is highly correlated to regulation, for example on privacy.” Government can, in fact, play a major role both in the fight against cyber crime and in the spread of cyber insurance. The U.K. government took the lead on cyber security in 2011 by setting aside nearly US$1 billion to boost the country’s cyber defenses. This has already resulted in the creation of a cyber crime investigation unit and a hub to promote information-sharing across organizations. Currently, tax incentives and new regulations promoting cyber insurance are being debated in the U.K.’s public arena. In fact, the development of cyber insurance would not only diminish the exposure of companies to cyber risk, but also increase the protection of virtually all citizens from cyber crime. This insurance could result in virtuous circles leading to companies that are better protected against opportunistic attacks. As Gow points out, “minimum security policies are required by an insurer before the latter is willing to take on the risk,” and insurance companies are likely to discount their premiums for companies exceeding these minimum requirements.

The U.S. government is also increasingly seeing cyber security as a major threat that requires its intervention. While closely monitoring the level of cyber protection for critical infrastructure, President Barack Obama in February 2013 signed an executive order expanding private sector access to government cyber threat information and instructing agencies to create a set of standards. Levy believes that the U.S. government may also consider “the creation of an agency gathering cybercrime information, and self-sustained via a minimum registration fee” — in other words, the extension of the FS-ISAC system beyond the financial services industry. “This agency would analyze malware and share the analysis and proposed mitigation strategy with subscribers, while at the same time keeping anonymous the company that provided the information,” adds Levy. The actuarial data collected in this way would also be a key resource for insurance companies in their attempt to quantify cyber risk and could ultimately result in a more dynamic offering of cyber-insurance products.

As a complement to such a data-gathering effort, establishing a federal re-insurance entity would further fuel the cyber insurance market by protecting insurance companies from large-impact, low-frequency risks — or the so called “cyber hurricanes.” The U.S. government did assume the role of insurer of last resort for terrorist events in the aftermath of 9/11, but public opinion is already considering whether this role should be extended beyond its planned December 31, 2014, expiration date. Thus, the battle for a new government-funded cyber re-insurance vehicle may not arise in the near future.

Source : http://www.paristechreview.com/2014/02/20/cyber-crime-business/