Trust Re Perspectives

Recent Cyber-Attacks Cause Rise in Insurance Purchasing

Cyber-risk is expected to become the number one risk facing the non-life insurance industry over the next few years due to the increase of cyber-crime incidents, according to the Survey of Risks Facing Insurers by the Centre for the Study of Financial Innovation based in London, United Kingdom. In this article, Trust Re offers a perspective on the implications which this trend has for the insurance industry.

A cyber-attack can generally be defined as any deliberate, offensive manoeuvre directed at any computer information system, network, or infrastructure, resulting in information or identity theft, corporate, and government espionage. Businesses across a wide range of industrial sectors are exposed to potentially enormous physical losses and liabilities as a result of cyber-crime.

The potential economic fallout from cyber threats should not be underestimated. As a result, many insurance companies have developed insurance products and policies that help protect clients from damages incurred from cyber-attacks. These products are generally known as cyber insurance.

Cyber insurance coverage typically falls into two broad categories: first party and third party. First party coverage focuses on the internal costs incurred by the company, such as hiring an attorney to deal with legal ramifications, and hiring a PR firm to minimise reputational damage. Third party coverage handles the consequences caused by cyber security events that affect other companies and individuals. Typical coverage includes network maturity liability. It also covers financial harm to other individuals from a company's privacy breach, as well as the cost of post-breach regulatory investigations and fines.

Commenting on the evolving nature of the industry, Tom Regan, the cyber practice leader for Marsh, says, "The industry is continuing to change and expand, and in certain areas of the business, we see some prices going up. The insurance industry can deal with risks that grow significantly if they can be appropriately compensated for them. As long as they can get an adequate premium, they'll be OK."

According to Verizon's 2014 Data Breach Investigations Report, the majority of security incidents fall under nine classification patterns. In the Energy and Utilities sector, two patterns, web application attacks and crime-ware, accounted for 69 percent of incidents. Under financial services, 75 percent of attacks came from web app attacks, "Denial-of-Service" (DoS) attacks, and credit card skimming. In the manufacturing sector, 54 percent of attacks were a result of cyber-espionage and DoS attacks.

Governments are also facing an unprecedented level of cyber-attacks and threats with the potential to undermine national security and critical infrastructure. Businesses that store confidential customer and client information online, such as banks and financial institutions are fighting to maintain their reputations in the wake of colossal data breaches. As corporate concerns heighten, a highly receptive audience lobbying for dedicated cyber insurance policies has developed.

Over the last 15 years, the energy sector has adopted widespread use of Internet systems, which help to considerably reduce costs and increase efficiency. However, they can be quite vulnerable to attacks if they are not fully secured. The energy sector in particular has recently become the target of attacks by hackers, political activists, and criminal gangs for financial and political reasons. Andrew George, Marsh's Global Energy Practice Chairman states, "Several energy firms have already suffered attacks originating from malicious software or viruses that has disrupted production and damaged hardware. A successful attack on a computer control or emergency shutdown system even at a small refinery, petrochemicals or gas plant, could result in estimated maximum losses as a result of a fire or explosion worth hundreds of millions of dollars."

Most cyber insurance products that are currently available cover minor problems such as data losses. However, coverage does not yet extend to digitally triggered catastrophes such as explosions and other damages to facilities. The UK estimates that cyber security breaches cost local energy firms around 400 million pounds annually. Companies are now coming under tremendous pressure from governments and shareholders to introduce defenses against such breaches, which could lead to regulatory requirements aimed at protecting key infrastructure.

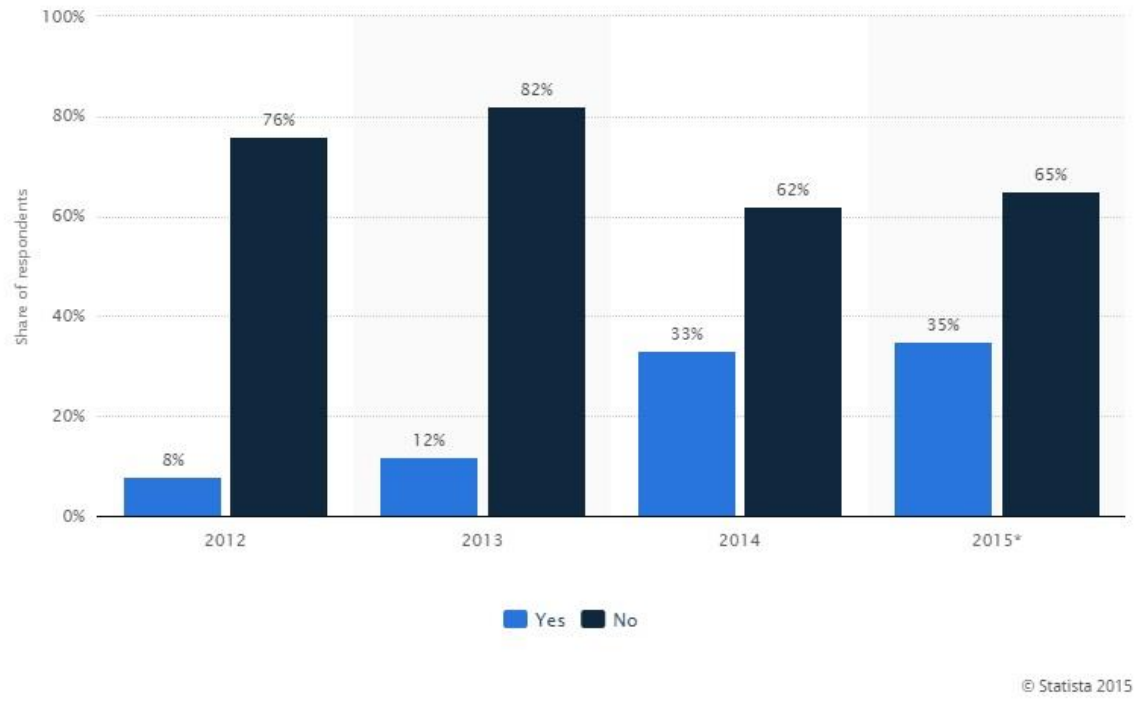
Targets of recent attacks include well-known corporations and establishments such as eBay, Target, the University of Maryland, NATO, JPMorgan Chase, Adobe, Aramco and RasGas, amongst many others. Approximately 145 million users were affected when eBay was targeted in early 2014. Although earnings were not as low as expected, the site did see a decline in user activity.

David Lacey, futurologist and security researcher with IOActive – a provider of specialist information security services, stated, "Large scale breaches always result in financial losses

because of the cost to respond and repair the damage… Lost future sales are a more variable impact, as it depends on factors such as brand value, competition, and customer confidence."

French TV channel TV5 Monde had to suspend broadcasting for 24 hours on April 8th, 2015 when it was it targeted. Messages by hackers were published on their website and Facebook page. The incident highlighted Europe's vulnerability to high-tech cyber-crime.

The graph below represents the share of companies that bought cyber insurance in Europe between the years 2012 and 2015. According to this, the amount of organisations that own cyber insurance increased from 8% in 2012 to 35% in 2015.



Source: Statista – *Does your organization purchase cyber liability insurance?*

According to another statistic from Statista, a statistic database company based in Hamburg, the average cost of cyber-crime amounted to 12.69 million U.S. dollars in 2014. 54 percent of global companies were insured against the loss of income, due to data breaches, while more than half of companies (which were not insured) were considering purchasing it. Only 3.8 percent of companies with revenues lower than 2.5 million U.S. dollars owned cyber insurance. Among companies with revenues exceeding five billion U.S. dollars, this number was equal to 25.9 percent.

A survey by the Ponemon Institute conveyed the average cost of cyber-crime for U.S. retail stores more than doubled from 2013 to an annual average of $8.6 per company in 2014. The

cyber insurance liability in Europe is growing at the rapid pace of 50-100% annually, according to statistical data gathered by Marsh & McLennan Companies. Early evidence from 2015 suggests increased acceleration in clients seeking financial protection through insurance, buying coverage from data breaches and business outages. Yet despite the large number of reported breaches, the actual number of breaches and exposed records is without a doubt much higher as many, if not most, attacks go unreported.

Though the bulk of business growth for cyber insurance has mostly been based in the United States, the European market is also rapidly growing. Many large telecommunications corporations, financial institutions and retailers have been studying recent events in the US and have realised they should be protecting themselves as well. This has caused a dramatic rise in the demand for cyber insurance throughout Europe. Although the European market for cyber insurance is still several years behind the US, awareness and demand are increasingly significantly.

October 2015

© Trust Re