HOLBORN™
Our Independence. Your Advantage.

ViewPoint

Analyzing Industry Issues from an Independent Perspective

Cyber Liability

As the world has become more interconnected by the "internet of things," businesses and households regularly rely on technology to conduct daily activities. While in recent years the reliance on technology has increased exponentially, cyber exposures are nothing new. Companies have been exposed to cyber risks for the last several decades dating back to the dotcom era of internet growth, followed by the Y2K scare, and HIPAA compliance rules.

Not just a large company problem

Recently, there have been headline-grabbing stories of data breaches at large retail companies, financial institutions, and private websites exposing millions of personal records. Publicity of such attacks has become more and more frequent, from the 2014 Home Depot and Target data breaches, to the early 2015 attack on Sony, to the most recent attack on the Ashley Madison website. In a precedent setting case, a July ruling by a U.S. Court of Appeals decided that retailer Neiman Marcus must now defend a class action suit claiming that it failed to protect customers, after having the case originally thrown out by a Chica-

...small businesses account for 90% of data breaches.

go district court. Rulings like this make it even more difficult for hacked companies to avoid costly and reputation-damaging lawsuits.

In addition to these large corporations, there are countless cyber-attacks targeting less sophisticated, more vulnerable security systems, not covered by the media. According to a report by First Data, small businesses account for 90% of data breaches. *The New York Times* reports that last year alone over half of American adults had their information exposed. These breaches are comprised of not only faceless hackers at home and abroad, but also thieves who steal laptops, documents, and the now ubiquitous smartphone. The costs of these data breaches are higher than one may think. Any company that stores or uses data is exposed to risks associated with data breaches, including:

- Business Interruption
- Network / Hardware
- Fines
- Credit Monitoring
- Reputational Risk
- Personal / Business Data Theft
- Breach Response

According to the National Small Business Association, a focus group reported that 44% of respondents had been victims of at least one cyber-attack in 2013, at an average cost of nearly $8,700 per breach. In many states, private and governmental organizations are required to notify potential victims of a breach. To protect their reputations, firms need to be proactive by replacing credit/debit cards, deploying credit monitoring services, and upgrading point-of-sale systems.

In response to the increasing threat to businesses, companies are implementing cyber risk controls as part of their Enterprise Risk Management initiatives. Boards and senior leadership are placing cyber risks at the top of the list of corporate concerns, and are seeking a cyber-insurance solution. A May 2015 Lloyd's report, *Business Blackout; The insurance implications of a cyber-attack on the US power grid* stated that "Cyber risk is already an embedded feature of the global risk landscape, and insurance has the potential to greatly enhance cyber risk management and resilience for a wide range of organizations and individuals who are exposed to its impacts." In fact, one of the largest growth areas in the insurance industry is Cyber Security Liability.

...insurance has the potential to greatly enhance cyber risk management...

According to a new report from Allianz Global Corporate Security Specialty (AGCS), the cyber insurance market is expected to grow to more than $20B in gross written premiums over the next decade. AGCS estimates that cyber crime costs the global economy $445B annually, yet the current global cyber insurance market only stands at about $2B in premiums.

Cyber liability: The new frontier

Cyber exposure and insurance coverage continues to evolve as fast as technology advances, hackers innovate and adapt, and legal precedents and case laws are set. Insurance coverages must adapt as well. While coverages by carrier vary, cyber-specific policies and endorsements generally cover:

- Loss of digital assets
- Non-physical business interruption and extra expense
- Cyber extortion threat
- Security event costs
- Network security and privacy liability coverage
- Employee privacy liability coverage
- Electronic media liability coverage
- Cyber terrorism coverage

Cyber exposures and the corresponding insurance coverages have grown significantly over the last several years. Despite this, many businesses and organizations remain uncertain of the value and/or protections provided by cyber coverage. Some risk managers argue that internal controls, not only technology based, but also managerial and personnel, eschew much of the need for an insurance solution. One senior technology

consultant in the insurance industry argued, "The largest risk for a cyber-attack comes from one source, us – people." Mishandling of e-mail, misplacing a USB drive, or the unintentional downloading of a virus can cause damage to a firm. A strong culture of safety, awareness, and protection, from all employees, can be the strongest defense against cyber loss. In addition, state-of-art firewall protection and consistently updated technology may be seen as an adequate measure for controlling cyber risk loss exposures. But is it enough?

Insurance carrier options

Insurance carriers should evaluate their options, as the potential frequency and costs of a cyber-attack can mount. Several Lloyd's cyber underwriters surveyed estimate the cost per record stolen/lost as high as $30 per piece of data; even a relatively small company with 2,000 lost customer records could face costs as high as $60,000 or more. In January 2007, a data breach at TJX Companies, a Massachusetts-based retail firm, cost the company $9.75 million to settle claims with victims across the country, showing just how costly fixing a cyber-attack can be.

Cyber: The new Black Swan?

SCENARIO	DESCRIPTION	ESTIMATED INSURED LOSS
Large Scale Attack on Power Grid (Summer)	Computer hack on several power stations in the summer, cutting power to several key economic urban centers in the US, causing business interruption, liability, and property losses, brought about by civil unrest.	**$71.1B***
Large Scale Attack on Power Grid (Winter)	Computer hack on several power stations in the winter, cutting power to several key economic urban centers, and residential areas in the US, causing business interruption, liability, and property losses, as well as widespread cold weather related damages. Civil and political unrest.	**$50B - $75B**
Cyber-attack on oil refinery / mining / production	Hack into a major energy or heavy industrial exposure, causing environmental disaster, business interruption, and sickening those exposed.	**$10B - $25B**
Cyber-attack on a large dam or water supply	Hack into control center for major water source, diversion site, or power damming site, causing physical damage due to flooding, loss from contaminated water, affecting farming industry and local residents.	**$10B - $15B**
Large scale hack of US banking institutions	Exposure of millions of customer data, as well as active hacks enacted to move monies and assets outside of the country.	**$15B - $20B**

** Lloyd's Report*

Cyber coverage, as it stands, is primarily focused on breach and breach response coverage. Forms and coverage language are still being refined, with pricing somewhat subjective. Underwriting guidelines and coverage costs are primarily based on revenue of the organization, but class of business and amount of data kept both play a significant factor in the pricing of coverage. While the coverage is relatively new, there is claims data available for several types of cyber-related losses, including data breaches. In addition to the potential individual risk, insurance companies should also be aware of exposures and potential claims that may arise in a catastrophic scenario, natural or man-made.

All perils insurance coverages, in property, casualty, and specialty lines, may cover cyber exposures not currently contemplated. Furthermore, both commercial and personal policies may be susceptible to catastrophic cyber scenarios. The aforementioned Lloyd's report explores the possibility of a nearly $1 trillion economic loss to the US economy, with up to a nearly $71.1B in insured loss coming from a cyber-attack on the Northeastern United States power grid. Like other "black swans" that have come before it, a new catastrophic scenario may arise from something not currently contemplated, but as the chart on the previous page illustrates, the effects can be disastrous. Insurance companies should be aware of the growing exposure cyber has on their current portfolios, and future potential exposures that could be into the future. The aforementioned AGCS report notes that most of the cyber policies written today are focused on data breach and response, but firms should be actively focusing on business interruption and supply chain implications of a cyber-attack.

Should reinsurance respond?

From a reinsurance perspective, language has yet to be tested in the event of a catastrophic cyber event. Nonetheless, buyers concerned about potential catastrophic exposures in their books should focus on ensuring that active exclusions of such cyber or IT hazards are evaluated and appropriately worded. Taken a step further, language can be appropriately crafted to proactively include these types of losses. In the current marketplace, opportunities exist for ceding companies to address these types of coverage issues. To do so, companies will need to demonstrate a firm grasp on where their exposures lie, have mitigation efforts in place, and underwriting guidelines / management initiatives that identify cyber exposures.

Holborn, as a matter of practice, regularly reviews wordings and continues to monitor the latest developments in this burgeoning sector. Holborn also maintains close relationships with several partners eager to take on cyber exposures in partnership with carriers. If you would like to discuss cyber, please do not hesitate to reach out to your Holborn broker.