Issue Review
November 24, 2015

A.M. Best's View on Cyber-Security Issues and Insurance Companies

Rapidly changing threat landscape and potentially catastrophic impacts must be managed holistically, not isolated to IT Department.

INTRODUCTION

Prompted by several years of drastic increases in both the frequency and severity of cyber-attacks against public and private companies, A.M. Best has been heightening its focus on the many aspects of cyber-security risk, as well as the appropriate mitigation strategies and preparedness organizations need to manage this risk. From A.M. Best's vantage point, while all financial and non-financial organizations are susceptible to cyber-attacks, insurance companies are particularly exposed, given the nature of their business.

Insurance companies are important to mitigate all types of risk by providing wide-reaching solutions to both the commercial markets and consumers. Insurance is a business requiring broad adoption to function properly, which inevitably aggregates valuable data, dependence, and risk. Recent breaches at large managed health care organizations have highlighted the fact that an insurance company's breach can have wide-reaching effects impacting staggering numbers of individuals and organizations. A recent study by Gemalto/SafeNet found that in 2014, more than 1,540 breach incidents occurred and exposed more than 1 billion records; translating this into time frames: data records were lost or stolen at rates of 2.8 million per day, 117 thousand per hour, 1,950 per minute, and 32 every second[1], affecting 81% of large businesses and 60% of small businesses[2].

It is necessary to raise both the awareness and preparedness around cyber-security risk to confront the challenges faced by companies and their insurers. Effective risk management will require a holistic approach where a company's technology, people, and processes diligently work in concert to minimize cyber-security risk. Just as an earthquake presents risk that can be managed, but not eliminated, cyber-security risk must be managed for both its existence and aggregate impacts. However, the world of cyber-security risk has connections and interdependencies unlike those seen in the physical world, making locale almost irrelevant when measuring and managing the aggregation of risk within cyber insurance portfolios.

A.M. Best still considers natural catastrophe losses to be the primary threat to the financial strength and credit quality of property and casualty insurers due to the significant, rapid, and unexpected impact that can occur. However, the increasing frequency and severity of cyber-attacks and difficulty in measuring the risk pose a potentially substantial threat to the insurance industry.

A.M. Best is analyzing cyber-security exposure in an effort to increase awareness of this threat and assess the impact on an organization's financial strength. A.M. Best is utilizing a holistic framework that accounts for the many opposing forces, which contribute to overall cyber-security risk. Assessments have historically been limited to the technology-based controls an organization has in place, but technology alone is not an adequate predictor of overall cyber-security posture or risk. One must assess the susceptibility of a company's cyber-security posture from the perspective of technology, people, processes, and preparedness. Susceptibility provides a comprehensive measure of a company's ability to fend off simple

Analytical Contact
Fred Eslami, Oldwick
+1 (908) 439-2200 Ext. 5406
Fred.Eslami@ambest.com
SR-2015-734

[1]2014 Year of Mega Breaches & Identity Theft, http://breachlevelindex.com/pdf/Breach-Level-Index-Annual-Report-2014.pdf.
[2]UK Cyber Security: The Role of Insurance In Managing and Mitigating The Risk, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/415354/UK_Cyber_Security_Report_Final.pdf.

attacks and minimize larger ones. The next step in understanding a company's overall cyber-security risk is an evaluation of the motivation of threat actors like criminal hackers, state-sponsored groups, and rogue employees to direct their efforts at a particular company. It is A.M. Best's opinion that an evaluation of the offensive and defensive forces apparent in the susceptibility and motivation of an organization is essential to understanding and managing an entity's overall cyber-security risk.

While the industry is still in need of more advanced modeling capabilities, A.M. Best expects organizations to have the ability to provide credible assessments regarding their cyber risk exposure. A.M. Best views an organization's ability to generate detailed and credible assessments of its potential cyber risk as a valuable tool in its overall risk management approach. As it has been A.M. Best's view for many years, "modeling" in general should not be the sole mechanism of managing risk, and over-reliance on models could in fact be problematic as such a practice cannot be expected to provide an exact solution.

This report will also summarize the results obtained from various surveys and questionnaires A.M. Best has conducted over the years.

Finally, A.M. Best is cognizant of the fact that the industry may be contemplating new formations of companies exclusively writing cyber-security insurance. As cyber-security risk is better understood, underwriting and risk management (e.g., pricing and reserving methods) are enhanced, and specific consequence-oriented data and actuarial studies become available, A.M. Best will continue to incorporate its findings into the rating process.

BACKGROUND

The literature concerning research (i.e., scholarly, technical, surveys, and those with a focus on specific industries and sectors) on the current state of cyber-security risk is becoming quite extensive. Given the widespread attention and publicity to this topic in the general media, recent research has shown that most organizations in various industries place cyber-security among their top five high-priority risks both in terms of likelihood and severity of impact.

The core issue is cyber-security risk is an intractable problem that cannot be eliminated from the modern, technologically driven world. The rapidly changing threat landscape and potentially catastrophic impacts must be managed holistically throughout an organization like any other business risk, not isolated to the IT Department. Appropriate technology is requisite in maintaining a resilient cyber-security posture, but it must be complemented by a skilled staff to manage that infrastructure and appropriate processes within all operational units to minimize risk. Although no organization can completely eliminate its cyber-security risk, those with a stronger risk management framework should fare better at mitigating the impact of attacks on computer networks, which can cause disruption and harm to operations and assets.

New technologies are continually being developed and upgraded for an eager market of both commercial and consumer users who are ready to rapidly adopt them. As each new technology product is released, hackers (both white hat and black hat) discover exploitable features and vulnerabilities within software and hardware that can be misused by unscrupulous actors. White hat or ethical hackers are computer security experts who work tirelessly to identify the flaws in technology products and services in an effort to alert users so they can protect themselves from criminal (black hat) hackers looking to take advantage of these vulnerabilities and cause harm to users. Criminal hackers rush to develop sophisticated software and tactics to exploit these vulnerabilities before researchers and manufacturers develop and distribute patches. Criminal hackers will hold on to these zero-day vulnerabilities as their weapons to stay one step ahead of their targets.

Today's environment is one where all organizations from local businesses to global financial organizations have an apparent and increasing dependence on information technology, network infrastructure, and big data. As a result, these organizations tend to hold tremendous amounts of their customers' proprietary business information, financial information, and sensitive personal information. In some cases, these organizations even share varying levels of access to company systems. This aggregation of customer data and interconnectedness among organizations has certainly served its intended purpose of providing an ease of service and communication; however, it also presents scenarios where single events can impact many individuals and organizations simultaneously, which can have potentially catastrophic consequences affecting the financial system and real economy. These events could cause tremendous and possibly uninsurable losses for the affected institutions.

Insufficient or lack of any proven governance, regulation, and control of cyber-security has and could further permeate throughout national borders and globally. As a result, cyber-attacks have become not only real and present dangers but also, given the different motivations behind such attacks by various dangerous, malicious, and criminal inter-state or intra-state actors, they continue to threaten a broad and expansive range of targets.

This dynamic interaction between evolving threats and tactics of a motivated adversary creates a landscape where companies continue to fall victim to increasing numbers of cyber-attacks and data breaches year after year. Furthermore, the increasing usage of shared infrastructure, service providers, cloud-based software, and storage of massive amounts of customer data presents increased potential for catastrophic loss events.

A.M. Best's Approach to Evaluating Cyber-Security

Cyber-security exposure is relevant to A.M. Best's rated entities on at least two major fronts: First, how is the company protecting itself against cyber threats, both internal and external? And second, if the company underwrites cyber-security insurance, how does it aggregate such exposure, e.g., arrive at potential loss estimates?

How Do Companies Protect Themselves Against Cyber Threats?

Insurers know they are not immune from being attacked by hackers due to internal weaknesses in dealing with network or system vulnerabilities. As part of A.M. Best's interactive rating process, and in order to enhance awareness and augment preparedness against cyber-attacks, a questionnaire containing the following simple questions is sent to companies rated by A.M. Best:

- Has the company been a target of a data breach/cyber-attack?
- If yes, how many times and how quickly were they identified?
- What remedial measures were taken?
- Where does the responsibility to manage cyber-security reside?
- What controls (internal and external) are in place to manage a data breach/cyber-attack (policies and procedures)?
- How often does the company conduct penetration testing?
- During the past five years, what systems investments have been made to improve resilience against cyber-attacks?
- How much of such investments were specifically dedicated to preventive measures on cyber-attacks and data breaches?
- How much is the company planning to invest during the next two years?
- If the company uses TPAs, cloud, shared devices (storage or otherwise), how are these risks being managed?
- What is the company doing to ensure implementation of up-to-date best practices and latest preventive methods?

- Does the company buy cyber-security insurance for additional protection?
- If yes, what are the policy limits and what is covered and excluded under such policy?

The responses are then reviewed and analyzed by a group of analysts who are focused on cyber-security risks. A "No" response to the first question, for example, is always concerning as it is commonly believed that most companies are exposed to an attempted attack of some sort. Thus, if warranted, further inquiries are made during rating discussions. This dialogue could potentially alleviate concerns that A.M. Best may have relevant to the issue of cyber-security. Besides augmenting the rating analysis, it may also ingrain a higher level of awareness of potential cyber risks that may enhance a company's understanding and preparedness to cope with cyber-security risk.

Most, if not all, companies recognize cyber-security threats are an existential risk of doing business. As such, two main trends have become evident in the A.M. Best surveys: First, most companies tend to be inclined to invest large sums of money to improve security on their IT systems and infrastructure. And second, larger companies tend to buy cyber insurance policies to further manage the risk associated with a cyber–attack, protecting themselves and ultimately their policyholders. A.M. Best is utilizing an analytical cyber risk assessment procedure, whereby a company's technology, people, and processes are examined along with the motivation of threat actors to conduct an attack.

There are several areas where companies can improve their risk profiles with respect to cyber-security insurance, both from the perspective of being the insurer or insured. A.M. Best intends to identify industry best practices in future reports, but the following three areas are worth mentioning as these may enhance a company's risk management and mitigation initiatives while lowering expenses related to disputes arising from unnecessary litigation.

First, data breaches covering physical damage and advertising injuries are currently covered under traditional insurance products such as Commercial General Liability Policies (CGLP), Business Interruption (BI), or Directors & Officers (D&O), which were developed decades ago and at a time when cyber liability claims were not contemplated. Policyholders may expect coverage under CGLP/BI/D&O for cyber-attacks or data breaches; while some court rulings have sided with policyholders, given the general language in such policies, long and expensive litigation has made insurance companies realize they can better serve policyholders and themselves by designing, developing, and selling specifically targeted types of specialty coverage forms addressing cyber liability risks separate from CGLP/BI/D&O.

Second, given the interconnectedness of cyber risk, the development of single-risk limits would be a conservative approach. As the regulatory environment expands and becomes enhanced, this may be unavoidable. However, in the meantime, devising single-risk limits with regard to policyholders' shared service providers, common vectors of attack, and other correlational factors, could prevent massive losses that may occur as a result of a single event, simultaneously causing losses at many organizations.

Finally, relevant to the above and given the lack of consequence-oriented data and actuarial information, the establishment of contingency reserves for cyber losses would demonstrate prudent risk management, as well as a conservative approach relative to this emerging risk, and this would be a positive factor in terms of the rating analysis. This practice is normal for certain mono-line insurers (i.e., financial and mortgage guaranty companies); given the lack of solid actuarial analysis and regulatory requirements, this may be a prudent practice for the time being for insurers to protect themselves and their policyholders.

How Should Cyber Exposure Be Aggregated for Companies Issuing Cyber-Security Insurance?

A.M. Best expects insurers to provide detailed information on their specific cyber-security insurance policies and, through the utilization of various techniques, be able to aggregate such exposures and arrive at a potential loss estimate in the foreseeable future. A quantification of the aggregation paths among policyholders across the cloud-based continuum of services ranging from shared infrastructure to software as a service, other types of service providers, and common exploitable vectors of attack will be crucial to an insurer's ability to understand and manage the aggregation of risk within its portfolio.

A.M. Best captures information and data regarding cyber-security insurance policies a company may issue through two primary ways: first, data submitted via the annual Supplemental Rating Questionnaire (SRQ), and second, ongoing discussions with each company's management as part of the analytical process. Given the importance of cyber-security exposure, A.M. Best expects to include more specific questions in the SRQ going forward. As far as the aforementioned second factor is concerned, the following questions are examples of those provided to a company prior to each annual meeting as part of the interactive rating process:

- Is the company's cyber-security insurance a separate policy or bundled in with
  - CGGL
  - D&O
  - Property & BI
- What are the numbers of policies sold?
- What are the limits?
- What are the top five industries the company provides cyber-security insurance?
- How are non-obvious paths of aggregation, such as common service providers and vectors of attack, being evaluated?
- If the company provides reinsurance, what is the reinsurance tower?
- What are premium expectations for 2015-2017?
- What are the loss expectations for 2015-2017?
- What is the average claim size?
- What is the average cost of crisis services (e.g., forensics, notification, and legal guidance)?
- What is the average legal defense cost?
- What is the average cost for legal settlements?
- Briefly describe the following items:
  - The underwriting process.
  - How are premiums and reserves determined?
  - What is covered under the policies?
  - What is excluded?

As explained above, A.M. Best expects companies to provide an overview of their assessment of cyber-security coverages. At the present time, determining whether the information gathered via the SRQ and the pre-meeting questionnaire would impact a company's ratings depends on the materiality of the types of coverage and limits provided, relative to the capital position of the company. A.M. Best views an organization's ability to generate detailed and credible assessments of its potential cyber risk as a valuable tool in its overall risk management approach. As such, methodologies that examine aggregate exposures and potential disaster scenarios involving correlated cyber risk will be crucial to insurance companies with portfolios of cyber insurance policies. The interconnectedness of cyber risk among companies is not necessarily correlated to attributes like physical location and class of business, so carriers must act accordingly and take a deeper look at the business written when examining potential aggregated loss scenarios affecting their portfolio. These insurance companies should have

an understanding of their portfolio's exposure to major service providers and other common vectors of attack and adequately analyze the potential catastrophe scenarios on their book to arrive at reliable measures of potential losses.

Insurance carriers will need an understanding of both the idiosyncratic risk of the companies within their portfolio as well as the aggregate risk of those companies and policies to arrive at reliable loss estimates. An assessment of the correlation of risk based upon service providers and other common vectors of attack, such as common vulnerabilities and systems, should be the basis of catastrophe scenario testing of a carrier's portfolio. These catastrophe scenarios can be modeled via Monte Carlo methods to generate many different states of the world based upon the individual risks and the interaction of those risks to examine what the potential financial impacts on the cyber insurance portfolio could amount to and with what likelihood over the course of a year. These general methods have been utilized in the examination of property and casualty risks for decades; it is now time they be appropriately modified and applied to analyze cyber insurance portfolios. Measuring the annual loss estimate of cyber insurance portfolios will promote appropriate discussions with regard to pricing adequacy and ensure that carriers are requiring appropriate compensation for the risks underwritten.

Additionally, A.M. Best recognizes that cyber-security insurance policies offered in the market are limited in terms of exposure and cover certain measurable losses and claims, and it takes into consideration management's overall approach to risk management and mitigation. Of particular importance is whether the company is proactive or passive in assessing the current and prospective views of risk, as well as the planned actions to mitigate exposure.

A.M. Best views a company's data quality as an extremely important component of its risk management capabilities. The process of data collection and aggregation relating to cyber risk is in its infancy, so the information provided via the SRQ and the pre-meeting questionnaire will be relied upon during the rating process.

It is A.M. Best's opinion that all insurers should be concerned about risk aggregation, given the possibility of single attacks leading to losses across a large number of insureds. Such risks are present dangers, and while they have not materialized, it does not mean that they could be avoided. Recent research[3] warns that a total realistic probable maximum loss for cyber-security risk globally is currently around GBP 20 billion (USD 31 billion). While that amount is within the reinsurance capacity for single-event risk of GBP 65 billion (USD 100.8 billion), it is well above that of GBP 3 billion (USD 4.6 billion) for a nuclear loss.

A.M. Best will continue to follow the ever-changing cyber risk environment, and will provide reports and updates as warranted to inform the industry about the rating implications of cyber risk.

[3]UK Cyber Security: The Role of Insurance In Managing and Mitigating The Risk, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/415354/UK_Cyber_Security_Report_Final.pdf.

Published by A.M. Best Company

Special Report

A.M. BEST COMPANY
WORLD HEADQUARTERS
Ambest Road, Oldwick, NJ 08858
Phone: +1 (908) 439-2200

WASHINGTON OFFICE
830 National Press Building
529 14th Street N.W., Washington, DC 20045
Phone: +1 (202) 347-3090

A.M. BEST AMÉRICA LATINA, S.A. de C.V.
Paseo de la Reforma 412
Piso 23
Mexico City, Mexico
Phone: +52-55-5208-1264

A.M. BEST EUROPE RATING SERVICES LTD.
A.M. BEST EUROPE INFORMATION SERVICES LTD.
12 Arthur Street, 6th Floor, London, UK EC4R 9AB
Phone: +44 (0)20 7626-6264

A.M. BEST ASIA-PACIFIC LTD.
Unit 4004 Central Plaza, 18 Harbour Road, Wanchai, Hong Kong
Phone: +852 2827-3400

A.M. BEST ASIA-PACIFIC (SINGAPORE) PTE. LTD.
6 Battery Road, #40-02B, Singapore
Phone: +65 6589 8400

DUBAI OFFICE* (MENA, SOUTH & CENTRAL ASIA)
Office 102, Tower 2
Currency House, DIFC
PO Box 506617, Dubai, UAE
Phone: +971 43 752 780
*Regulated by the DFSA as a Representative Office

A Best's Financial Strength Rating (FSR) is an independent opinion of an insurer's financial strength and ability to meet its ongoing insurance policy and contract obligations. An FSR is not assigned to specific insurance policies or contracts.

A Best's Issuer Credit Rating (ICR) is an independent opinion of an entity's ability to meet its ongoing financial obligations and can be issued on either a long- or short-term basis.

A Best's Issue Rating (IR) is an independent opinion of credit quality assigned to issues that gauges the ability to meet the terms of the obligation and can be issued on a long- or short-term basis (obligations with original maturities generally less than one year).

Rating Disclosure: Use and Limitations
A Best's Credit Rating (BCR) is a forward-looking independent and objective opinion regarding an insurer's, issuer's or financial obligation's relative creditworthiness. The opinion represents a comprehensive analysis consisting of a quantitative and qualitative evaluation of balance sheet strength, operating performance and business profile or, where appropriate, the specific nature and details of a security. Because a BCR is a forward-looking opinion as of the date it is released, it cannot be considered as a fact or guarantee of future credit quality and therefore cannot be described as accurate or inaccurate. A BCR is a relative measure of risk that implies credit quality and is assigned using a scale with a defined population of categories and notches. Entities or obligations assigned the same BCR symbol developed using the same scale, should not be viewed as completely identical in terms of credit quality. Alternatively, they are alike in category (or notches within a category), but given there is a prescribed progression of categories (and notches) used in assigning the ratings of a much larger population of entities or obligations, the categories (notches) cannot mirror the precise subtleties of risk that are inherent within similarly rated entities or obligations. While a BCR reflects the opinion of A.M. Best Company Inc. (AMB) of relative creditworthiness, it is not an indicator or predictor of defined impairment or default probability with respect to any specific insurer, issuer or financial obligation. A BCR is not investment advice, nor should it be construed as a consulting or advisory service, as such; it is not intended to be utilized as a recommendation to purchase, hold or terminate any insurance policy, contract, security or any other financial obligation, nor does it address the suitability of any particular policy or contract for a specific purpose or purchaser. Users of a BCR should not rely on it in making any investment decision; however, if used, the BCR must be considered as only one factor. Users must make their own evaluation of each investment decision. A BCR opinion is provided on an "as is" basis without any expressed or implied warranty. In addition, a BCR may be changed, suspended or withdrawn at any time for any reason at the sole discretion of AMB.