MAY 2019

CYBER RISK INSURANCE
A Resource Guide for Actuaries

Prepared by the Cyber Risk Insurance Task Force of the
American Academy of Actuaries Casualty Practice Council

American Academy of Actuaries
Objective. Independent. Effective.™

ACTUARY.ORG

Cyber Risk Insurance

A Resource Guide for Actuaries

Prepared by the Cyber Risk Insurance Task Force
of the Casualty Practice Council, American Academy of Actuaries

Edmund Douglas, MAAA, FCAS, *Chairperson*
Eduard Alpin, MAAA, FCAS, *Vice Chairperson*
Terry Alfuth, MAAA, FCAS, FCA
Anna Antonova, MAAA, FCAS
Wanchin Chou, MAAA, FCAS
Wei Chuang, MAAA, FCAS
Taylor Krebsbach, MAAA, FCAS, CERA
Mou Jian Teo, MAAA, ACAS
Janet Wesner, MAAA, FCAS, CERA
Navid Zarinejad, MAAA, FCAS
Zachery Ziegler, MAAA, FCAS

American Academy of Actuaries
Objective. Independent. Effective.

AMERICAN ACADEMY OF ACTUARIES
1850 M STREET NW, SUITE 300, WASHINGTON, D.C. 20036
202-223-8196 | WWW.ACTUARY.ORG

According to the 2018 *Allianz Risk Barometer* report, cyber risk is the No. 1 concern for risk managers in the United States. It is a risk that impacts everyone—from individuals to small businesses to large Fortune 100 corporations. As the world continues to become more digital, and more people, organizations, and the devices that they own become connected, the risk of cybercrime will continue to rise. The number of "internet of things" (IoT) devices—estimated to number roughly 20 billion in 2018—is projected to grow rapidly to over 70 billion by 2025, increasing the attack surface and providing attackers with additional opportunity to carry out large-scale attacks. As a result of the global digitization and the increasing capabilities of malicious cyber actors, the costs of cybercrime have continued to rise, and are estimated to have topped $600 billion in 2017.

With this tremendous global threat growing in scope, insurers have a unique opportunity to provide businesses and individuals with protection in the form of financial security, as well as promoting strong cybersecurity posture. Offering lower pricing and more favorable coverage to businesses with stronger cybersecurity controls, and requiring basic cybersecurity hygiene,[1] will provide companies with additional incentive to enforce appropriate controls and protect their data and systems. The actuarial function is an important component of the analytical mindset and strategic decision-making that is crucial for insurers' success.

Actuaries serve a key role in facilitating the risk transfer and risk engineering functions that insurance provides. The risk transfer function is one that more frequently comes to mind when considering the value that comes from insurance. However, just as important is the risk engineering function, because through it the insurance market has the ability to affect broader trends in the risk landscape. In looking at things like manufacturing and safety standards, and even the way properties are built, there is evidence of the risk engineering function that insurance has provided over the years.

The nuts and bolts of this function simply involves gathering relevant information and analyzing that information with the intent of determining effective risk management practices. Through this process, insurers can gain useful insights about a risk. They can learn more about what factors increase or decrease the likelihood of undesirable events occurring. And in the case of cyber risk, when the risk engineering function is effective it should be giving insights on how to improve cybersecurity and manage its financial implications.

1 Cyber hygiene refers to practices that users of computers and other devices take to maintain the health of their systems and to improve their online security. These practices are often part of a routine to ensure the safety of identity and other details that could be stolen or corrupted. Much like physical hygiene, cyber hygiene is regularly conducted to ward off natural deterioration and common threats. (DigitalGuardian.com)

However, cyber risk is unique. At the root of this peril are persistent adversaries who are constantly looking for new ways to carry out attacks and maximize their profit. This means that the risk is dynamic and evolving, which has implications for insurance coverages as well as analytical models. A lack of available relevant data adds to the challenge of quantifying and managing this risk. Nevertheless, at a very fundamental level cyber can be approached the same way as with any other risk. Because the capabilities do not exist to eliminate the risk, cyber risk needs to be understood and its financial implications managed.

The Casualty Practice Council's Cyber Risk Task Force of the American Academy of Actuaries[2] has produced this issue brief with the goal of providing a set of resources, selected from those with an actuarial perspective, that can move the user one step closer to understanding the risks and issues around cyber. Because the public domain is filled with various publications and literature on the topic, this resource guide is intended to make it less daunting to identify the most effective resources to educate oneself on the relevant issues.

The resources listed in this guide provide a good starting point for a better understanding of cyber risk. The hope is that a deeper understanding will ignite more engagement—especially for actuaries, who are on the front lines developing solutions to address the various challenges that make cyber risk unique.

This publication aims to encourage the idea of information-sharing. Most would agree that information-sharing, which can take many forms, is key to alleviating some of the significant challenges that plague the cyber insurance market. Operating in silos will undoubtedly result in greater struggles to keep pace with the quickly evolving risk of cyber. Indeed there are various hurdles in developing an ideal platform for information-sharing; however, this should not discourage from sharing insights at a more basic level. Any momentum gained on information-sharing has the potential to snowball into something of greater value. This resource guide intends to set the tone—feedback on any resources not listed is encouraged.

2 The American Academy of Actuaries is a 19,500-member professional association whose mission is to serve the public and the U.S. actuarial profession. For more than 50 years, the Academy has assisted public policymakers on all levels by providing leadership, objective expertise, and actuarial advice on risk and financial security issues. The Academy also sets qualification, practice, and professionalism standards for actuaries in the United States.

This annotated reading list is offered as a first step in helping to understand the unique challenges of cyber risk. The task force makes no endorsement nor statement of support or concern of any of the industry practices or policy recommendations at the links in this list. To provide easier access, the materials are divided into the following subject areas:

Cyber Risk and Insurance Background

Organisation for Economic Co-operation and Development (OECD), Enhancing the Role of Insurance in Cyber Risk Management (December 2017)

Executive summary:

This comprehensive report lays out various policy recommendations aimed at enhancing the contribution of the cyber insurance market to manage the risk posed by digitalization. It includes:

- An overview of the different types of cyber incidents, as well as the types of losses that may result
- A crash course on the cyber insurance market, including the types of losses that commonly are covered by stand-alone cyber insurance policies and traditional policies, as well as the losses that are more difficult to cover
- Information on how insurers underwrite cyber insurance coverage and the additional risk mitigation and crisis response services frequently offered with policies
- An overview of the main challenges that constrain the capacity of the cyber insurance market from both the supply and demand perspective
- An examination of the initiatives being explored and ideas that have been proposed to address ongoing challenges

LINK: http://www.oecd.org/publications/enhancing-the-role-of-insurance-in-cyber-risk-management-9789264282148-en.htm

OECD, Supporting an Effective Cyber Insurance Market (May 2017)

Executive summary:

This 20-page report concisely summarizes the comprehensive OECD report "Enhancing the Role of Insurance in Cyber Risk Management." It is a great source of information for someone looking to gain a high-level understanding of the cyber insurance space, without having to dive deep into the subject. The content offers high-level information on the following topics:

- Common cyber incidents
- Potential coverage for cyber risk in traditional policies
- Market maturity and take-up rates
- Cyber insurance market challenges

LINK: https://www.oecd.org/daf/fin/insurance/Supporting-an-effective-cyber-insurance-market.pdf

The Geneva Association, Cyber Insurance as a Risk Mitigation Strategy (April 2018)

Executive summary:

This paper "analyzes the state of the cyber market and the role insurers play in advancing cyber resiliency. Moreover, it reviews the transformation along the value chain as insurers are moving from providing risk transfer products only to offering prevention, mitigation, and resolution services." The benefits of providing cybersecurity services, which go beyond an additional revenue stream, are discussed. Some of the services falling into the pre-breach category including "consulting services to train and assist organizations in best practices for reacting to and limiting the damage from a cyberattack or incident." Post breach services discussed include: "evaluate the impact of an attack, help implement response and recovery plans, provide public relations and communications support, and identify appropriate mitigating actions." Key challenges discussed in the research are accumulation risk, the human element in cyberattacks, and limited data availability. Future research topics such as understanding the political impacts of cyber risk on insurance are proposed.

LINK: https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/cyber_insurance_as_a_risk_mitigation_strategy.pdf

Hiscox Cyber Readiness Report 2018

Executive summary:

This report is compiled from a survey of more than 4,100 executives, departmental heads, information technology (IT) managers and other key professionals in the UK, US, Germany, Spain and The Netherlands, from organizations both large and small, in both public and private sectors. The report not only provides an up-to-the-minute picture of the cyber readiness of organizations large and small, it also offers a blueprint for best practice in the fight to counter an ever-evolving threat. Especially informative statistics include:

- Frequency of cyber attacks by country and size of organization
- Cost of cyber attacks by country and size of organization, including averages and min to max ranges
- Distribution of companies based on "cyber readiness" according to three categories: novice, intermediate and expert
- IT and cyber security budgets by country and level of expertise, as well as planned spending
- Cyber insurance take up rates

LINK: https://www.hiscox.co.uk/cyberreadiness

Carnegie, Addressing the Private Sector Cybersecurity Predicament (November 2018)

Executive summary:

This report discusses a range of barriers that impede a more effectively "functioning cyber insurance market—including practical, technical, operational, and strategic challenges, within and outside the insurance industry—and explores a series of individual and complementary efforts by the insurance industry, governments, vendors of information and communications technologies (ICTs), and other key stakeholders in the private sector toward realizing the full potential of insurance to reshape the risk environment."

LINK: https://carnegieendowment.org/2018/11/07/addressing-private-sector-cybersecurity-predicament-indispensable-role-of-insurance-pub-77622

Market Size and Performance

ISO Marketstance, Sizing the Standalone Commercial Cyber Insurance Market (March 2018)

Executive summary:

This report discusses the size of the cyber market today as well as projected into the future. Written premiums are broken out by:

- Standalone vs. Package Policies
- Industry sectors
- Size of companies including small, middle market, and national accounts
- Additional commentary on historical loss distribution by industry

LINK: https://www.verisk.com/insurance/campaigns/iso-marketstance-commercial-insight-market-sizing-white-paper/

Aon, Cyber Insurance Profits and Performance (June 2017)

Executive summary:

This report summarizes the profits and performance of the U.S. cyber insurance market based on data from the National Association of Insurance Commissioners (NAIC) cyber statutory filings. The findings give some perspective on industry experience and might serve as a performance benchmark for insurers interested in offering cyber insurance. Particularly interesting information includes:

- Number of carriers writing cyber insurance, including year-over-year changes
- Total amount of premiums written, split out by standalone and package policies
- Industrywide cyber loss ratio and combined ratio, split out by standalone and package policies
- A distribution of company counts by written premiums

LINK: http://thoughtleadership.aonbenfield.com/sitepages/display.aspx?tl=659

Advisen & PartnerRe, 2018 Survey of Cyber Insurance Market Trends (2018)

Executive summary:

This report is an annual collaboration between PartnerRe and Advisen, commenting on the evolution of the cyber insurance market. The 2018 survey was based on input from 270 brokers and 70 underwriters. 79% of respondents were from North America, but there was also a representative international presence. The findings address shifts in sales, coverage, claims handling, risk aggregation management and other insights on market demand.

LINK: https://www.advisenltd.com/2018-survey-of-cyber-insurance-market-trends/

Cyber Incidents and Costs

Verizon DBIR 2018

Executive summary:

The Verizon DBIR provides a comprehensive summary of analysis of cyber incidents and data breaches. This report is particularly useful because of the way it is summarizes a large amount of data about cyber incidents, both recent and old, in an easily digestible and intuitive way, combining charts and graphs, bullet point highlights, deep dives, and stories. Some of the valuable insights include:

- Actors behind the breaches, including a breakdown by internal, external, criminal groups, nation states
- Tactics used such as hacking, malware, social attacks
- Assets that were compromised such as databases, web apps, and laptops
- High level statistics by industry sectors as well as deep dive analysis into specific industries
- Deep dive into Distributed Denial of Service DDoS attacks including length and severity
- A discussion of the cyber risks targeting mobile phones

LINK: https://www.verizonenterprise.com/verizon-insights-lab/dbir/#report

Net Diligence, Cyber Claims Study 2017

Executive summary:

aggregates insurance claims information and provides information on number of records exposed, cost of data breaches, and cost per record. The study provides a summary of the following statistics:

- Overall breach costs, number of records exposed and cost per record by year, business sector and company size
- causes of loss such as hacking, virus, or system glitch and the impact of each
- Deep dive into several attack types including ransomware, W-2 fraud, and business email compromise
- breakdown on type of cost related to the loss (crisis management, regulatory, legal), etc.

LINK: https://netdiligence.com/wp-content/uploads/2017/10/2017-NetDiligence-Claims-Study_Public-Edition.pdf

Ponemon, Cost of Data Breach Study (July 2018)

Executive summary:

Ponemon in partnership with IBM Security performs a study of the cost of data breaches for a sample of companies around the world. Some of the main takeaways from the report include:

- Average cost of data breaches by country, industry and size of company
- Year over year trends in cost of data breaches
- Data breach costs by root causes such as malicious, system glitch and human error
- Impact of top 22 factors on cost of data breaches; factors include incident response team, use of encryption and employee training.
- Likelihood of data breaches by number of records exposed
- Analysis of mean time to contain breaches and the average cost

LINK: Document1https://www.ibm.com/downloads/cas/861MNWN2

Chubb Cyber Index 2019

Executive summary:

The Chubb Cyber Index is a website containing summarized statistics of Chubb's cyber claims history over the past 20 years. The graph views can be sliced by industry, company size and date range. The information contained includes: total claims volume by year, types of threats and actors, and impacted digital assets. Additionally, educational information is provided for various subjects including: ransomware, IoT and DDoS.

LINK: https://www.chubbcyberindex.com

Cyber Accumulation Analysis

Cyence/Lloyds, Counting the Cost: Cyber Exposure Decoded (June 2017)

Executive summary:

This report analyses the cyber exposure of two potential aggregation scenarios: a cloud service provider outage, and a mass vulnerability causing widespread data breaches. The report gives related historical examples for each scenario, and walks through a detailed consideration of the technology exposures that could cause each scenario to happen. This cybersecurity perspective is complemented by an analysis of return period losses along with confidence intervals. The report is a good resource to understand two of the most common aggregation risks seen by cyber re/insurers today.

LINK: https://www.lloyds.com/news-and-risk-insight/risk-reports/library/technology/countingthecost

AIR/Lloyds, Cloud Down Report 2018

Executive summary:

This study analyzes the potential financial impact on the U.S. economy stemming from a major disruption to top cloud service providers. Estimates for total economic losses from such an event range from several billion dollars to over $20 billion, the majority of which is uninsured. One of the main accomplishments of this study is the use of a detailed accumulation approach for modeling (as opposed to market share) which identifies the insureds that would be impacted by a scenario and omitting those that would not. Key findings of the study include:

- A discussion of the difference between ground up losses and insurable losses from a potential aggregation event
- Modeled business interruption losses associated with the disruption of a cloud provider varying by industry and time offline
- A breakdown of expected losses by company size
- A comparison of expected losses using two different methodologies: market share and detailed accumulation approaches

LINK: https://www.lloyds.com/~/media/files/news-and-insight/risk-insight/2018/cloud-down/aircyberlloydspublic2018final.pdf

CyRiM/Lloyds, Bashe Attack Report 2019

Executive summary:

This report assesses the impacts of a global ransomware attack, where companies' devices are infected with malware that threatens to destroy or block access to files unless a ransom is paid. The report estimates a cyber-attack on this scale could cost $193 billion and affect more than 600,000 businesses worldwide. Despite the high costs to business, the report shows that the global economy is underprepared for such an attack with 86% of the total economic losses are uninsured, leaving an insurance gap of $166 billion.

LINK: https://www.lloyds.com/news-and-risk-insight/risk-reports/library/technology/bashe-attack

Silent Cyber

Jon Laux, "Silent cyber risks prompt insurers to update policies, gather exposure data, plan security" (December 2018)

Executive summary:

Originally published in *Business Insurance*, this article provides an overview on the topic of silent cyber risk. Attention is given to the technical and organizational challenges that insurers face in managing silent cyber risk, and potential approaches are discussed. The article also discusses the role that actuaries can play to improve the situation.

LINK: https://www.linkedin.com/pulse/silent-cyber-risks-prompt-insurers-update-policies-gather-jon-laux/

Lloyds/University of Cambridge, Business Blackout 2015

Executive summary:

This paper is a common starting point for many insurers' analysis of "silent" or non-affirmative cyber risk in traditional P&C policies. *Business Blackout* presents a detailed analysis of a hypothetical cyberattack ("*Erebos*") on the Northeastern U.S. power grid, including three variants of the attack scenario at increasing levels of severity. The paper is accompanied by a calculation worksheet whereby re/insurers can estimate their losses across many lines of business. Since its publication in 2015, the *Erebos* scenario has been debated by experts inside and outside the insurance community. Nonetheless, it should be considered for its thorough depiction of the potentially extreme impacts of cyber risk on the global economy and the insurance industry.

LINK TO PAPER: https://www.lloyds.com/~/media/files/news-and-insight/risk-insight/2015/business-blackout/business-blackout20150708.pdf

LINK TO CALCULATION WORKSHEET: https://www.lloyds.com/~/media/files/news-and-insight/risk-insight/2015/business-blackout/business-blackout-appendix-1.pdf

AMERICAN ACADEMY OF ACTUARIES
1850 M STREET NW, SUITE 300, WASHINGTON, D.C. 20036
202-223-8196 | **ACTUARY.ORG**