PUBLISHED FEBRUARY 2022

Cyber Risk Resource Guide
CYBER RISK TOOLKIT

American Academy of Actuaries
Committee on Cyber Risk, Casualty Practice Council

American Academy of Actuaries
ACTUARY.ORG

The American Academy of Actuaries' Cyber Risk Toolkit, developed by the Academy's Committee on Cyber Risk, is a series of papers addressing issues pertinent to cyber risk insurance and cyber exposure. This toolkit is intended to be a resource for interested readers of the general public, public policymakers, the actuarial profession, the insurance sector, and other stakeholders.

While the paper that follows stands alone, the complete toolkit offers a cohesive overview of the challenges posed in the cyber insurance market. The toolkit will be updated periodically to reflect new and emerging work from the committee.

American Academy of Actuaries

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

Cyber Risk Resource Guide

Published February 2022

According to the 2021 *Allianz Risk Barometer* report, cyber risk is in the top three concerns for risk managers in the United States. It is a risk that impacts for both companies and individuals alike —from individuals to small businesses to large Fortune 100 corporations. As the world continues to become more digital, working from home becomes more prevalent, 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 at 27 billion devices in 2019—is projected to grow rapidly to over 75 billion by 2025, increasing the attack surface and providing attackers with additional opportunity to carry out large-scale attacks. Businesses, shifting some operations to remote work due to the COVID-19 pandemic, became even more reliant on technology, sparking concerns about business interruption due to cyber incidents. 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 expected to have exceeded $6 trillion in 2021.[1]

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,[2] will provide companies with additional incentives 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 can affect broader trends in the risk landscape. In examining companies' protocols for manufacturing and safety standards, and even the way properties are built, there is evidence of the impacts of insurance on risk engineering.

1 "Cybercrime To Cost The World $10.5 Trillion Annually By 2025"; *Cybercrime Magazine*; Nov. 13, 2020.
2 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)

The nuts and bolts of this function simply involve 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 risk engineering is operating effectively, it should provide insights on how to improve cybersecurity and manage its financial implications.

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 fundamental level, cyber can be approached the same way as with other risks. Because the capabilities do not exist to eliminate the risk, cyber risk needs to be understood and its financial implications managed.

This resource guide was developed to provide 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. A deeper understanding of cyber risk could 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. Information-sharing, which can take many forms, could be key to alleviating some of the significant challenges that plague the cyber insurance market. Operating in silos could 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, these hurdles 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 and any feedback on resources not listed is strongly encouraged.

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
- Market Size and Performance
- Cyber Incidents and Costs
- Cyber Accumulation Analysis
- Silent Cyber
- Cyber War & Terrorism
- Public Policy Resources

Cyber Risk and Insurance Background

Organization 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: https://www.oecd.org/daf/fin/insurance/Enhancing-the-Role-of-Insurance-in-Cyber-Risk-Management.pdf

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

OECD, Encouraging Clarity in Cyber Insurance Coverage (2020)

Executive summary:

This paper focuses narrowly on one reason that the stand-alone cyber market remains small: Policyholders often do not understand the coverage available or think that their current insurance policies will cover cyber events. In particular, this paper addresses

- Potential cyber coverage in property, liability, crime, and kidnap & ransom coverages
- Common exclusions due to politically motivated cyber attacks
- Government roles in providing policy clarity
- Types of losses covered by cyber insurance
- Treatment of ransom payments by insurers and governments

LINK: https://www.oecd.org/finance/insurance/Encouraging-Clarity-in-Cyber-Insurance-Coverage.pdf

OECD, Enhancing the Availability of Data for Cyber Insurance Underwriting (2020)

Executive summary:

This paper examines the general lack of data for cyber insurance underwriting as well as how public policy and regulation can play a role in data aggregation. Topics discussed include:

- Antitrust considerations
- Privacy/confidentiality requirements
- Current governmental and private efforts to compile cyber data
- Considerations for insurance regulators

LINK: http://www.oecd.org/pensions/insurance/Enhancing-the-Availability-of-Data-for-Cyber-Insurance-Underwriting.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://media-publications.bcg.com/pdf/cyber_insurance_as_a_risk_mitigation_strategy.pdf

Hiscox Cyber Readiness Report 2021

Executive summary:

This annual report is compiled from a survey of more than 5,500 executives, departmental heads, information technology (IT) managers, and other key professionals in the U.K., U.S., Spain, The Netherlands, Germany, France, Belgium, and Ireland, 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 practices in the fight to counter an ever-evolving threat. Especially informative statistics include:

- Frequency of cyber-attacks by country
- Median cost of cyber-attacks by country as well as cost of the largest incident or breach reported
- Distribution of companies based on "cyber readiness" according to three categories: novice, intermediate, and expert
- IT and cybersecurity budgets by country and level of expertise, as well as planned spending
- Cyber insurance take-up rates

LINK: https://www.hiscox.co.uk/sites/default/files/documents/2021-04/21486-Hiscox-Cyber-Readiness-Report-2021-UK.pdf

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

Aon, U.S. Cyber Market Update (July 2021)

Executive summary:

This report summarizes the profits and performance of the U.S. cyber insurance market through 2020 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. Key takeaways include:

- 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.aon.com/Documents/20210609-2021-cyber-market-update.pdf

Advisen & PartnerRe, Cyber Insurance—The Market's View (2020)

Executive summary:

This report is an annual collaboration between PartnerRe and Advisen, commenting on the evolution of the cyber insurance market. The 2020 survey was based on input from 260 brokers and 190 underwriters. The findings address shifts in sales, coverage, claims handling, risk aggregation management, and other insights on market demand, including thoughts on the potential impact of the COVID-19 pandemic.

LINK: https://www.advisenltd.com/cyber-insurance-the-markets-view

NAIC & Center for Insurance Policy and Research, Report on the Cybersecurity Insurance and Identity Theft Coverage Supplement (December 2020)

Executive summary:

This report provides an understanding of the U.S. cybersecurity insurance market. Each year, the NAIC collects data about cybersecurity insurance, with over 500 insurers submitting data for calendar year 2019. The data indicates a less than 1% decrease in direct written premiums. The report then goes on to describe the data across various dimensions to help facilitate a better understanding of the cybersecurity insurance market.

LINK: https://content.naic.org/sites/default/files/inline-files/Cyber_Supplement_2019_Report_Final_1.pdf

Cyber Incidents and Costs

Verizon DBIR 2021

Executive summary:

The Verizon DBIR provides a comprehensive summary of analysis of cyber incidents and data breaches. This report 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 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 2020

Executive summary:

Aggregates insurance claims information and provides information on number of records exposed, cost of data breaches, and cost per record across the years 2015–2019. The study provides a summary of 3,547 claims across 100 categories using 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/2021/03/NetD_2020_Claims_Study_1.2.pdf

Ponemon, Cost of Data Breach Study (July 2020)

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 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 25 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 identify and contain breaches, and the average cost

LINK: https://www.ibm.com/downloads/cas/RZAX14GX

Chubb Cyber Index 2020

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 segmented 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: http://www.chubbcyberindex.com/

Cyber Accumulation Analysis

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

Executive summary:

This report analyzes 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://assets.lloyds.com/assets/pdf-emerging-risk-report-2017-counting-the-cost/1/pdf-emerging-risk-report-2017-counting-the-cost.pdf

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 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://assets.lloyds.com/assets/pdf-air-cyber-lloyds-public-2018-final/1/pdf-air-cyber-lloyds-public-2018-final.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://assets.lloyds.com/assets/pdf-bashe-attack-cyrimbasheattack-finalbashe-attack/1/pdf-bashe-attack-CyRiMBasheAttack_FINALbashe-attack.pdf

Guy Carpenter/CyberCube/Lloyds, The Emerging Cyber Threat to Industrial Control Systems 2021

Executive summary:

This report assesses three scenarios detailing the most plausible routes by which a cyber-attack against industrial control systems (ICS) could generate major insured losses. This report is centered around four major industries depending on industrial control systems (manufacturing, shipping, energy, and transportation), analyzes historical precedents, and estimates potential impacts of each event. The report concludes with several recommendations and suggests potential areas of focus for insurers.

LINK: https://assets.lloyds.com/media/542bea95-0d28-4ce1-a603-63db54aa24f9/The%20Emerging%20Cyber%20Threat%20to%20Industrial%20Control%20Systems_Final%2016.02.2021.pdf

RMS, Managing Cyber Insurance Accumulation Risk 2020

Executive summary:

This report provides insurers with a starting point for a framework for assessing and managing cyber accumulation risk. The report begins with the data requirements that a company needs to track and monitor its potential accumulations from cyber insurance. Then it identifies key legislative and litigation trends that change the cost of cyber claims. Five key cyber loss processes are identified with potential to cause widespread and correlated losses. Frequency and severity distributions and modelling frameworks are then provided for each of the five cyber loss processes. An approach is then provided for managing and assessing cyber accumulation risk to determine risk appetite and loss potential.

LINK: https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-rms-managing-cyber-insurance-accumulation-risk.pdf

Michael Bean, Exposure Measures for Pricing and Analyzing the Risks in Cyber Insurance, (April 2020)

Executive summary:

This report uses a conceptual rather than empirical approach to identify and evaluate potential exposure measures for pricing and to analyze the risks in cyber insurance. The report analyzes historical experience in cyber as well as provides an overview of cyber insurance coverages currently available. The report also describes the criteria used to evaluate potential measures before identifying potential candidates for measurements. It concludes with recommendations for exposure measures that should be used for each type of cyber insurance coverage.

LINK: https://www.soa.org/globalassets/assets/files/resources/research-report/2020/exposure-measures-cyber-insurance.pdf

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.

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, experts inside and outside of the insurance community have debated *Erebos*. Nonetheless, its thorough depiction of the potentially extreme impacts of cyber risk on the global economy and the insurance industry merits consideration.

LINK TO PAPER: https://assets.lloyds.com/assets/pdf-business-blackout-business-blackout20150708/1/pdf-business-blackout-business-blackout20150708.pdf

LINK TO CALCULATION WORKSHEET: https://assets.lloyds.com/assets/pdf-business-blackout-appendix-1/1/pdf-business-blackout-appendix-1.pdf

Willis Towers Watson, The Problem of Silent Cyber Risk Accumulation (2020)

Executive summary:

This article examines the impacts of recent cyber-attacks on the insurance industry, including a summary of what changes various major insurers, such as AIG or Lloyds of London, have taken to address the silent cyber issue.

LINK TO PAPER: https://www.willistowerswatson.com/en-US/Insights/2020/02/the-problem-of-silent-cyber-risk-accumulation

Cyber War & Terrorism

Geneva Association, "Cyber War and Terrorism: Towards a common language to promote insurability" (July 2020)

Executive summary:

This article introduces the term "hostile cyber activity" (HCA) as a potential tool for the insurance industry to mitigate the terminological ambiguity surrounding cyber policy wording, especially in the context of war and terrorism. HCA is the intent to cause serious damage in or to another state regardless of publicity or the causing of terror. According to the Geneva Association, HCAs are distinctly different from cyber terrorism, and cannot currently be classified as an act of war. This report seeks to distinguish between what is clearly insurable and what is not, with the aim of reducing uncertainty.

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

Public Policy Resources

United States Government Accountability Office, "Cyber Insurance—Insurers and Policyholders Face Challenges in an Evolving Market" (May 2021)

Executive summary:

This report prepared by the Government Accountability Office is a report to congressional committees. It highlights key trends in the cyber insurance market as well as key challenges faced by the insurance industry and options to address those challenges.

LINK: https://www.gao.gov/assets/gao-21-477.pdf

United States Department of Justice, "U.S. Government Launches First One-Stop Ransomware Resource at StopRansomware.gov" (July 2021)

Executive summary:

This article highlights the commitment of the U.S. Department of Justice (DOJ) and U.S. Department of Homeland Security (DHS) to combat ransomware. It also announces the launch of StopRansomware.gov, a website that provides broad resources to use to be used in the fight against ransomware.

LINK: https://www.justice.gov/opa/pr/us-government-launches-first-one-stop-ransomware-resource-stopransomwaregov

New York Department of Financial Services, Cyber Security Resource Center (2021)

Executive summary:

This site provides various resources from New York's Department of Financial Services (DFS) on the topic of cyber security.

LINK: https://www.dfs.ny.gov/industry_guidance/cybersecurity

New York Department of Financial Services, "Cyber Insurance Risk Framework—Insurance Circular Letter No. 2 (2021)" (February 2021)

Executive summary:

This Insurance Circular Letter outlines a cyber risk framework and DFS overall concerns regarding insurers' readiness to measure their true cyber risk exposure. It provides a seven-point cyber risk framework of "best practices" for insurers to use. The discussion includes reference to the DFS position on ransomware and the payment of ransoms, silent cyber, evaluation of systemic risk, and measuring and monitoring aggregate insured risk.

LINK: https://www.dfs.ny.gov/industry_guidance/circular_letters/cl2021_02

U.S. Securities and Exchange Commission, "SEC Announces Three Actions Charging Deficient Cybersecurity Procedures" (August 2021)

Executive summary:

This press release notes the SEC sanctioning several firms for cybersecurity deficiencies. In particular, these companies had policies requiring advanced cybersecurity procedures, but these procedures were not being implemented.

LINK: https://www.sec.gov/news/press-release/2021-169

National Association of Insurance Commissioners (NAIC), "Cybersecurity" (May 2021)

Executive summary:

This site highlights actions taken by the NAIC regarding cybersecurity. These actions include:

- Adopting principles for insurance regulatory guidance related to cybersecurity
- Revising cybersecurity protocols for company financial examinations
- Adopting a Cybersecurity Insurance and Identity Theft Coverage Supplement for the property/casualty annual financial statement

LINK: https://content.naic.org/cipr_topics/topic_cybersecurity.htm

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