UPDATED JUNE 2022

CYBER RISK TOOLKIT

American Academy of Actuaries
Cyber Risk Task Force, Casualty Practice Council

American Academy of Actuaries
ACTUARY.ORG

The American Academy of Actuaries' Cyber Risk Toolkit, developed by the Academy's Cyber Risk Task Force, is comprised of 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. Cyber risk issues have been in the news regularly recently, and those using the toolkit can benefit from the perspectives offered in the papers. While each is a stand-alone paper, in total they offer a cohesive overview of the challenges posed in the cyber insurance market.

Since the initial publication of the Cyber Risk Toolkit, this document has been updated to include the "War, Cyberterrorism, and Cyber Insurance," "Cyber Risk Resource Guide," and "Autonomous Vehicles and Cyber Risk" sections. The toolkit will continue to be updated periodically to reflect new and emerging work from the task force.

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 policy makers 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.

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

Cyber Risk Toolkit

CONTENTS

An Introduction to Cyber

Published August 2021

This introductory paper addresses some of the key aspects of cyber risk and insurance such as general product market, and insurance coverages and features. It also discusses some of the more well-known cyberattacks. Other upcoming Task Force papers will explore more specific areas of interest related to cyber risk and insurance in more detail.

Cyber Insurance as a Risk Management Strategy

Cyberattacks are a real threat in today's ever-evolving cyber risk landscape. Furthermore, the COVID-19 pandemic has forced almost all organizations to speed up their digital transformation priorities. It changed the way organizations learn from and deal with cyber risks. During the pandemic e-commerce is booming, brick-and-mortar retailers shifted to digital platforms, while schools and offices adopted and embraced online classes and remote working. For organizations this meant re-thinking digitalization strategies and investing in information technology (IT), cloud capacity, and network infrastructure, to remain competitive and ensure business continuity. This rapid transformation, much of which will have a lasting effect, will inevitably increase systemic vulnerabilities to cyberattacks, meaning that the next decade will be the most important period of growth for the cyber insurance market thus far. Insurance coverage for cyber risk provides a means for businesses and individuals to transfer a portion of their financial exposure to insurance markets, reducing the costs associated with a cyber breach.

Cyber insurance coverage can be provided as a stand-alone cyber insurance policy, or as an endorsement (or rider) to an existing insurance policy. The stand-alone cyber insurance market has generally developed in response to the introduction of exclusions[1] of cyber-related losses from policies covering property, crime, kidnap and ransom, liability and other traditional insurance coverages. Types of exclusions include: (i) general exclusions of all losses resulting from a cyberattack or incident; (ii) an exclusion applied in general liability policies to exclude liability related to data breaches; and (iii) exclusion of losses related to data restoration. Most stand-alone cyber insurance policies have been developed to close the gaps from these exclusions and to cover some of the losses that result from privacy breaches and, to a lesser extent, denial-of-service attacks, cyber extortion, and cyber fraud. In fact, some cyber-related losses may alternatively be covered by traditional property, liability, crime/fidelity, and kidnap and ransom policies. This coverage may be included through the inclusion of an endorsement providing such coverage.

1 *Supporting an Effective Cyber Insurance Market*; OECD; 2017.

As the cyber market is still relatively new and maturing, some of the policy coverages, exclusions, conditions, and terminology are not as uniform as they are for other mature and developed lines of business and products in the market, and may develop further. Additionally, parts of the coverage may have lower sub-limits than the aggregate policy limit, and waiting periods (often acting like deductibles) may vary for various coverages.

This paper discusses the current coverages and approaches from some of the current market participants. As a developing product, some aspects of coverage and conditions are not uniform across the market. Additionally, market developments and product maturity may also take different directions and forms.

Current Landscape of the Cybersecurity Insurance Market

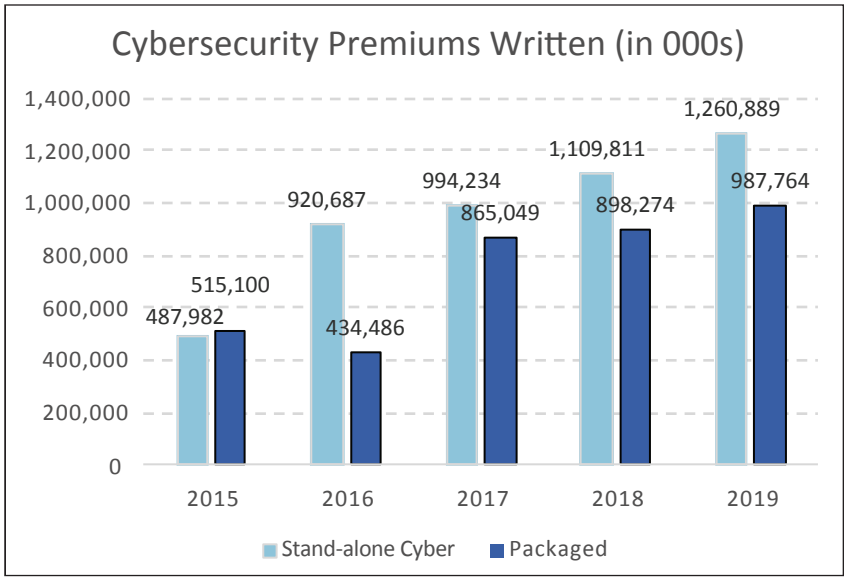
The National Association of Insurance Commissioners (NAIC) Cybersecurity Insurance and Identity Theft Coverage Supplement has been used to gather information about cybersecurity and identity theft insurance since 2015. Our paper focuses on statistics from cybersecurity coverage and not identity theft coverage which is a personal lines product. The cybersecurity data reported to the NAIC pertains to both single policies ("stand-alone") and endorsements added to an insurance policy ("packaged") associated with exposures arising out of network intrusions and improper handling of electronic data, including data such as personally identifiable information ("PII") and other sensitive information.

According to the NAIC[2], the risks covered may include (1) identity theft; (2) business interruption; (3) damage to reputation; (4) data repair costs; (5) theft of customer lists or trade secrets; (6) hardware and software repair costs; (7) credit monitoring services for impacted consumers; and (8) litigation costs.

Data reported to the NAIC and compiled by S&P Global Market Intelligence provides an illustration of the growth in the cybersecurity insurance market. Excluding surplus lines cybersecurity policies, both the stand-alone and packaged policies combined to a $2.2 billion U.S. market in 2019 and have more than doubled since 2015. This comprised of approximately 0.3% of the total direct premiums written in the U.S. property & casualty P/C) market. On average, 56% of cybersecurity coverage premiums written consist of the stand-alone product. However, a larger proportion (75% in 2019) of carriers are writing cybersecurity policies on a packaged basis.

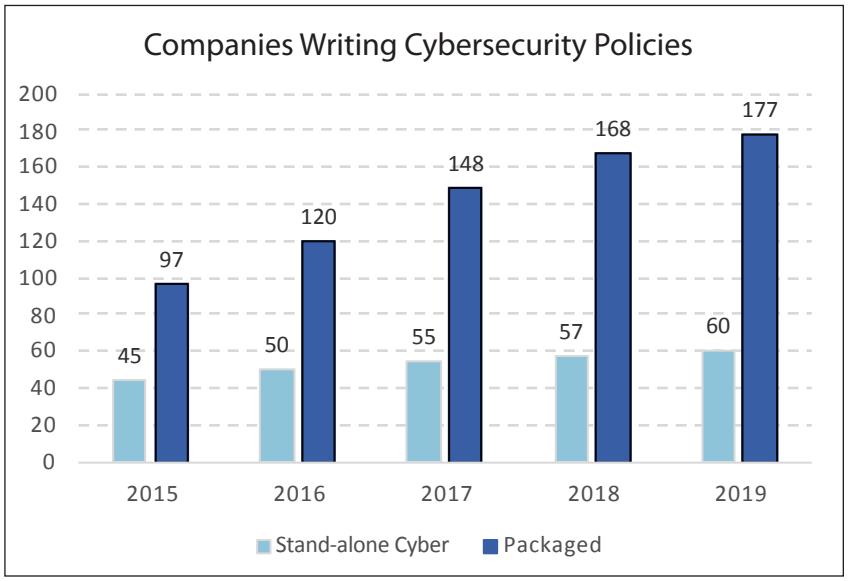
2 "Cybersecurity," National Association of Insurance Commissioners (NAIC); May 27, 2021.

Figure 1



*The figures shown in the graphs are limited to information reported to NAIC by insurance carriers.

Figure 2

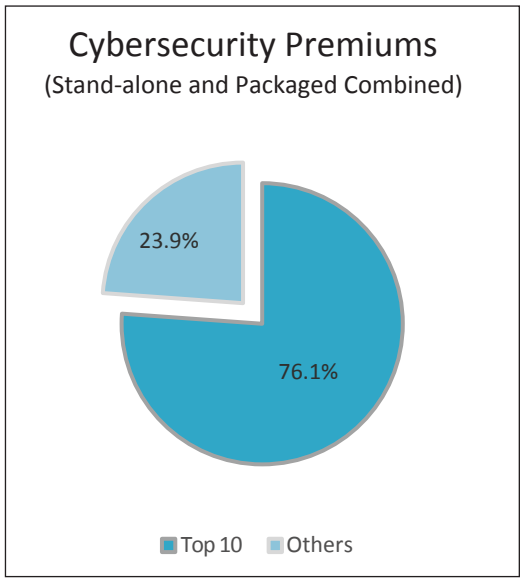


*The figures shown in the graphs are limited to information reported to NAIC by insurance carriers.

As more insurance carriers enter the market due to the increasing demand for cyber insurance and its growth potential, of note is the fact that the top 10 carriers hold a strong presence in the cybersecurity market. Their average market share from 2015 through 2019 was more than 75%.

According to recent cyber insurance surveys and studies published by Aon[3], Verisk[4] and a collaboration between Advisen and PartnerRe[5], the majority of cyber insurance buyers were from the healthcare industry and are increasingly purchasing coverage to protect the sensitive patient information they hold. Manufacturing and professional/financial services industry came in as the next largest purchasers of cyber insurance. Additionally, Advisen's and PartnerRe's survey pointed out that in recent years, the majority of the cyber insurance buyers consist of small and medium enterprises (SMEs), which is an indication that these smaller businesses are beginning to realize the need for coverage.

Figure 3



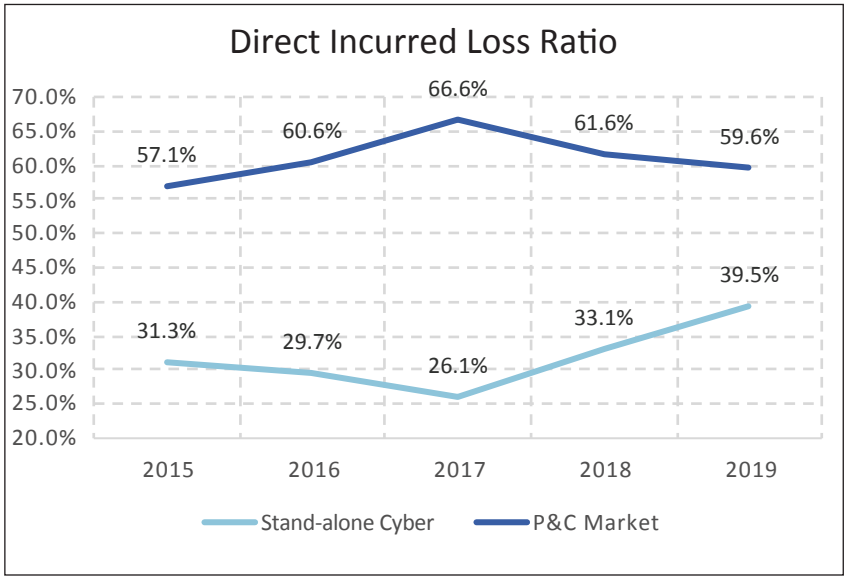
*The figures shown in the graphs are limited to information reported to NAIC by insurance carriers.

The cybersecurity insurance market has observed relatively lower loss ratios compared to the performance of the overall P&C market. Since 2015, the calendar year loss ratio for stand-alone policies has hovered between 26% to 40%. Packaged policy loss ratios have been excluded in figure 4 below given that NAIC required carriers to report only paid loss data for these policies. The entry of more companies into the cyber insurance market, the exponential growth in the Internet of Things (IoT), the increasing number and sophistication of cyberattacks, and the expansion of virtual work/educational environments

3 *Global Cyber Market Overview*; Aon Inpoint; June 2017.
4 *Sizing the Standalone Commercial Cyber Insurance Market*; Verisk; 2018.
5 *2018 Survey of Cyber Insurance Market Trends*; PartnerRe and Advisen; October 2018.

are some of the changes that may put pressure on the loss ratios. Additionally, cyberattackers are also increasing their sophistication. They look to the most financially viable companies. And, once in a company's network, some are not as focused on the immediate ransom. They may linger within the network as a "trusted" user, searching for the biggest opportunities. While an attacker may have already hacked into a system, a claim may not emerge for many years down the road.

Figure 4



*The figures shown in the graphs are limited to information reported to NAIC by insurance carriers.

Despite the favorable loss ratio performance, the cyber insurance market is still relatively young, and its true claim cost is still uncertain since we have yet to observe a global market-wide catastrophic insurance loss. The NotPetya and WannaCry cyberattack events, which are discussed in detail later in the paper, were considered catastrophic since they caused approximately 200,000 infections across 150 countries, but only a small portion of ultimate losses were insured losses. Multinational corporations lost billions of dollars as a result; however, insurance losses were relatively light due to the low penetration levels, retentions and coverage limitations and exclusions. The recent substantial increase in cyberattacks and ransomware has increased the market wide loss ratios.

The penetration levels or take-up rates of a mature market for commercial insurance can be as high as 100% across the different sectors. However, for cyber insurance, it is estimated that only 20% to 35%[6] of all U.S. companies purchased coverage, either stand-alone or packaged policies.

Additionally, cyber insurance policies are mainly written on a claims-made basis, which limits the insurers' exposures in the tail as compared to an occurrence policy, by requiring that the covered cyber event be reported during the coverage period. According to the NAIC 2018 Cybersecurity report,[7] the vast majority of third-party coverage for standalone cybersecurity policies continue to be written on a claims-made basis.

Silent Cyber[8]

The stand-alone and packaged policies described above are also known in the marketplace as affirmative coverage for cyber perils. On the contrary, non-affirmative, more commonly known as "silent cyber," coverage is triggered when cyber perils are not explicitly included or excluded in the policy wording. Failure of carriers to consider and quantify these ambiguous exposures in their insurance premiums can lead to significant accumulation of losses from a single cyber peril triggering multiple insurance policies in various lines of business. The conversation around "silent cyber" picked up only in recent years mainly due to the large losses insurers have faced from cyberattacks for policies that were not intended to provide such coverage. An indelible case—the NotPetya cyberattack, which occurred in June 2017, focused mostly on victims in Ukraine. However, several global corporations were also infected, including shipping giant Maersk and FedEx among others. Many of these corporations suffered cyber losses on non-cyber lines of businesses such as general liability and other liability, in which their insurance was not initially designed to cover cyber losses. On a positive note, carriers are increasingly taking proactive measures to address the issues for silent cyber by recognizing explicitly cyber exposures. They either explicitly include coverage for some aspects of cyber-related losses or clearly exclude any such losses.

6 *Supporting an Effective Cyber Insurance Market*, op. cit.
7 "Report on the Cybersecurity Insurance and Identity Theft Coverage Supplement"; NAIC and the Center for Insurance Policy and Research; Sept. 12, 2019.
8 Details on this topic are further described in a separate 2021 paper from the Academy on silent cyber.

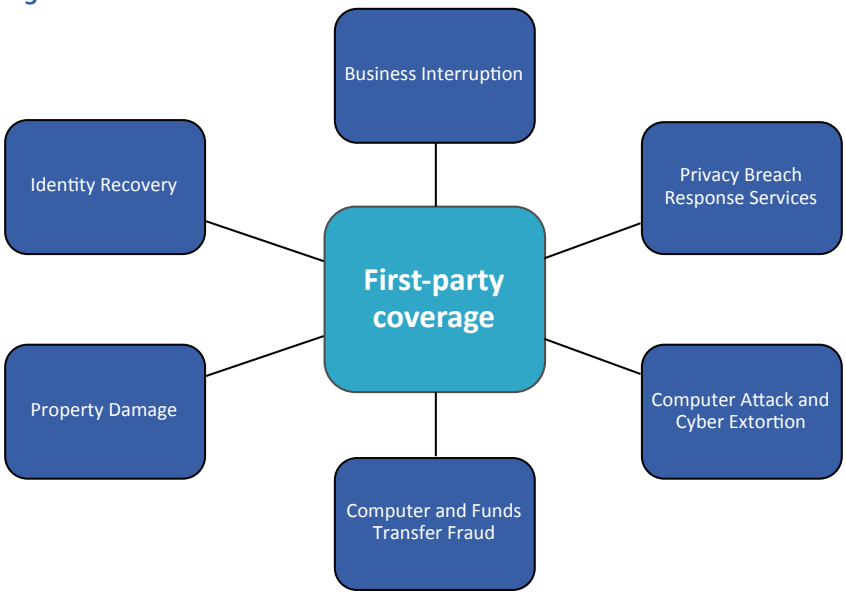
Policy Coverage Definitions/Services

This analysis relies upon publicly available rate and rule filings submitted to state Departments of Insurance. The information from these filings was gathered and compiled, in order to compare the cyber policies being offered and the coverage definitions.

Affirmative cyber coverage—either through stand-alone or packaged policies—typically offers first- and third-party coverage. Historically, insurance coverage was focused mostly on third-party liability coverage, but as businesses have become more digitalized and as this data plays a key role in the day-to-day operations, corporations are increasingly interested in protecting their digital assets and also protecting against consequences of interruption to operations through insurance.

First-Party Coverages

Figure 5



Business Interruption

Business interruption, also referred to as network interruption coverage, generally indemnifies the insured for business interruption loss, in excess of the retention, incurred by the insured during a period of restoration or extended interruption. To qualify the interruption should be a direct result of the actual and necessary interruption or suspension of computer systems that first takes place during the policy period and is directly caused by a failure of computer security to prevent a security breach. The security breach typically must first take place on or after the retroactive date and before the end of the policy period.

Business interruption loss often includes:

1. Income loss
    a. Net profit (loss) before income taxes.
    b. Fixed operating expenses including payroll incurred by the insured if:
        - Expenses must necessarily continue during the period of restoration; and
        - Expenses would have been incurred by the insured had such interruption or suspension not occurred.
2. Extra expense
    a. Reasonable and necessary expenses incurred by the insured during the period of restoration to minimize, reduce or avoid income loss.
    b. Forensic expense—Reasonable and necessary expenses incurred by the insured to investigate the source or cause of the failure of computer security to prevent a security breach.

In addition to security breach as a cause of loss, some carriers also cover business interruption loss as a direct result of system failure. System failure can be defined as an unintentional and unplanned interruption of computer systems and often does not include any interruption of computer systems resulting from a security breach, or the interruption of any third-party computer system. Another common cause of loss for this coverage can be from a computer attack or cyber extortion. Some carriers define the cause of loss more broadly: 1) unintentional programming or administrative error, and 2) unintended or unplanned outage.

With business interruption coverage, carriers typically include a time retention element per one insured event, which is often between 4 and 24 hours. Actual coverage will trigger after the designated period has elapsed.

Carriers sometimes offer dependent business interruption coverage, which provides the same coverage as Business Interruption, but for a dependent business. A dependent business is defined as an entity that is not part of the insured organization, but which provides necessary products or services to the insured organization. Such an endorsement may be for general third parties or require specific named third parties and would provide coverage for its inability to provide products or services due to a cyberattack.

Property Damage

Property damage coverage typically pays for direct physical loss of or damage to digital assets, covered property, and computer systems and media, if such loss or damage is caused by a cyber-event. This coverage may also include the expenses to replace digital asset losses sustained during the period of interruption caused by a cyber event resulting in the corruption or destruction of the insured's digital assets.

Within property damage coverage, some carriers may broaden coverage to provide:

1. Protection and preservation of digital assets:
    a. The reasonable and necessary cost incurred for actions taken by the insured to temporarily protect or preserve digital assets from further damage, during or after a cyber event, provided that such costs are over and above the insured's normal operating expenses.
2. Off-premises service interruption:
    a. The insurer will typically pay for the loss of or damage to the insured's covered property at an insured location sustained by the insured during the period of interruption, directly resulting from the necessary suspension of the insured's business activities at an insured location, resulting from a cyber event at a service provider company directly or indirectly supplying voice, data, video, or cloud services.

Similar to the business interruption coverage, carriers may incorporate the time retention element with property damage coverage. To trigger the time element component, the loss must result from the necessary suspension of the insured's business activities at the insured's location. The suspension must be due to a cyber event resulting in corruption, destruction, or loss of access to the insured's digital assets while within the policy territory. Coverage will only apply when the period of interruption exceeds the time defined as the qualifying period. The qualifying period for property damage coverage can be selected by the insured from a range of periods offered by the carrier.

Privacy Breach Response Services

Privacy breach response or data compromise response services commonly offer the insured services such as:

1. Computer expert services.
2. Professional information technologies review to determine the nature and extent of the breach, and the number and identities of the affected individuals.
3. Legal services:
    a. Professional legal counsel review of the breach, and the best response. If there is a reasonable cause to suspect that a covered event may have occurred, the costs will be covered.
4. Public relations and crisis management expenses:
    a. Professional public relations firm review of the potential impact of the breach on the insured's business relationships and the response.
5. Notification services:
    a. Notifying the individuals as required by the applicable breach notice law.
6. Call center services:
    a. Information to support customers;
    b. Helpline;
    c. Credit report and monitoring; and
    d. Identity restoration case management.
7. Regulatory fines and penalties.
8. Payment Card Industry (PCI) fines and penalties.
9. Breach resolution and mitigation services.

Privacy breach response services can also include assistance from the breach response services team and access to education and loss control information at no charge. Services do not include any internal salary or overhead expenses of the insured.

Some carriers offer similar type services as an optional coverage with the ability for insureds to decrease the limit. The resulting cost may vary quite significantly from industry to industry. For instance, given the nature of personal information and records, legal and regulatory notification and recovery costs may be high for the healthcare industry.

Computer Attack and Cyber Extortion

The computer attack and cyber extortion component typically provides coverage for loss directly arising from a computer attack or cyber extortion. A computer attack is commonly defined as one of the following involving the computer system:

1. An unauthorized access incident.
2. A malware attack.
3. A denial-of-service attack against a computer system.

The following coverage is generally provided in a computer attack and cyber extortion coverage:

1. Data restoration costs.
2. Data re-creation costs.
3. System restoration costs.
4. Public relations or crisis management—The insurer will pay for the services of a professional public relations firm to assist in communicating the insured's response concerning the computer attack to the media, the public, the customers, the clients, or members.

Extortion and extortion threats may have varying language in policies from different companies. One definition is a threat to breach "computer security" in order to:

1. Alter, destroy, damage, delete or corrupt any "data asset";
2. Prevent access to "computer systems" or a "data asset", including a "denial of service attack" or encrypting "data asset" and withholding the decryption key for such "data asset";
3. Perpetrate a theft or misuse of a "data asset" on "computer systems" through external access;
4. Introduce "malicious code" into "computer systems" or to third party computers and systems from "computer systems"; or
5. Interrupt or suspend "computer systems" unless an "extortion payment" is received from or on behalf of the "insured."

Different industries have different levels of appeal for cybercrime. For instance, companies with large amounts of consumer credit card information or medical data may be considered more lucrative targets. Insureds' general preparation, detection, recovery, and restoration plans, and the frequency of review of the plans and practice runs can lower the probability and extent of large losses.

Computer and Funds Transfer Fraud

This coverage will generally pay the insured for computer fraud or a fund transfer fraud incurred by the insured.

Computer fraud is typically defined as an intentional, unauthorized, and fraudulent entry of data or computer instructions directly into, or change of data or computer instructions within, a computer system. It does not include employees, independent contractors or any individual under the direct supervision of the insured. To be qualified for coverage it typically must cause:

1. Money, securities, or other property to be transferred, paid, or delivered.
2. An account of the insured or its customer, to be added, deleted, debited, or credited.
3. An unauthorized or fictitious account to be debited or credited.

Funds transfer fraud is commonly defined as an intentional, unauthorized and fraudulent instruction transmitted by electronic means to a financial institution. Coverage often provides for fraud if it results in a direct financial loss to the insured. This coverage typically does not include:

1. Threat or coercion of the insured to send money or divert a payment.
2. Dispute or a disagreement over the completeness, authenticity or value of a product, a service, or a financial instrument.

One way to assess the probability of such incidents is by reviewing an insured's employee training and protocols.

Identity Recovery

Identity recovery coverage is similar to identity case restoration management under privacy breach response services and is commonly grouped together with those services. If provided separately, this coverage may cover:

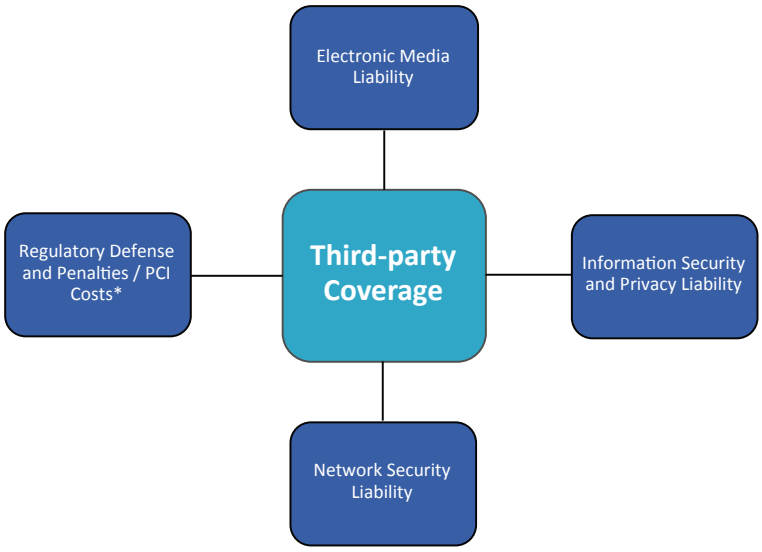
1. Case management services; and/or
2. Expense reimbursement.

Coverage generally applies if the following conditions are met:

1. There has been an identity theft involving the personal identity of an identity recovery insured.
2. Such identity theft took place in the coverage territory.
3. Such identity theft is first discovered by the identity recovery insured during the coverage term.
4. Such identity theft is reported to the insurer within a designated time period.

Third-Party Coverages

Figure 6



*Some carriers may include this coverage under the first-party privacy breach response services.

Electronic Media Liability

Electronic media liability coverage pays damages and claims expenses that the insured is legally obligated to pay due to any claim first made against an insured during the policy period for electronic media liability.

Electronic media liability is often defined as an allegation that the display of information in electronic form by the insured on a website resulted in:

1. Infringement of another's copyright, title, slogan, trademark, trade name, trade dress, service mark, or service name.
2. Defamation against a person or organization that is unintended.
3. A violation of a person's right to privacy, including false light and public disclosure of private facts.
4. Interference with a person's right of publicity.

This coverage may also be known as website media content liability. Other common causes of loss in addition to the four mentioned above include:

1. Misappropriation of ideas under an implied contract.
2. Plagiarism or unauthorized use of a literary or artistic format, character, or performance, in the insured's covered material.
3. Libel, slander, trade libel, or other tort related to disparagement or harm to the reputation or character of any person or organization in the insured's covered material.
4. Improper deep linking or framing within electronic content.

Information Security and Privacy Liability

Information security and privacy liability coverage pays on behalf of the insured for damages and claims expenses that the insured is legally obligated to pay as result of any claim, including a claim for violation of privacy laws:

1. Theft, loss, or unauthorized disclosure of personally identifiable information or third-party information.
2. One or more of the following acts or incidents that directly result from a failure of computer security to prevent a security breach:
3. The alteration, corruption, destruction, deletion, or damage to data stored on computer systems.
4. The failure to prevent transmission of malicious code from computer systems to computer or network systems that are not owned, operated, or controlled by an insured.
5. The participation by the insured's computer system in a denial-of-service attack directed against computer or network systems that are not owned, operated, or controlled by an insured.

Network Security Liability

Coverage of network security liability generally pays for damages and claim expenses, which the insured is legally obligated to pay because of any claim first made against the insured for:

1. Data breach
2. Security breach
3. Insured's failure to timely disclose a data breach or security breach
4. Failure by the insured to comply with the part of a privacy policy that specifically:
    a. Prohibits or restricts the insured's disclosure, sharing or selling of PII;
    b. Requires the insured to provide individuals access to their PII and to correct incomplete or inaccurate PII after a request is made; or
    c. Mandates procedures and requirements to prevent the loss of PII.

The cause of loss is commonly due to a network security incident, which can be defined as a negligent security failure or weakness with respect to a computer system that allowed one or more of the following to happen unintentionally:

1. Propagation or forwarding of malware, including viruses, worms, Trojans, spyware and keyloggers. Malware does not include shortcomings or mistakes in legitimate electronic code.
2. Abetting of a denial-of-service attack against one or more other systems.
3. Loss, release or disclosure of third-party corporate data.
4. Inability of an authorized third-party user to access a computer system due to a malware attack.

Regulatory Defense and Penalties / PCI Costs

Although some carriers provide regulatory defense and penalties coverage under privacy breach response services as a first-party coverage, others classify this as a separate third-party liability coverage. This covers claims expenses and penalties due to a regulatory proceeding caused by a cyber incident.

Similar to regulatory defense and penalties, PCI costs coverage can be commonly provided under privacy breach response services. PCI costs coverage is typically defined as the monetary amount owed by the insured under the terms of a merchant services agreement ("MSA") as a direct result of a suspected data breach. The MSA is an agreement between an insured and a financial institution, credit/debit card company, credit/debit card processor, or independent service operator enabling an insured to accept credit card, debit card, prepaid card, or other payment cards for payments or donations.

Common Policy Language Definitions

Cloud Services

A contracted service in the business of storing, processing, and managing the insured's digital assets and providing access and use of programs/software or a network of servers hosted away from the insured's location to store, process, and manage the digital assets.

Data

A representation of information, knowledge, facts, concepts, or instructions, which are being processed, or have been processed in a computer and may be in any form, including magnetic storage media, punched cards, or stored internally in the memory of such computer.

Distributed Denial-of-Service ("DDOS") attack

A malicious attack by an authorized or unauthorized party designed to slow or completely interrupt an authorized party from gaining access to the insured's computer systems or website.

Digital Assets

Electronic data, programs/software, audio, and image files. To the extent they exist as electronic data and only in that form, digital assets include the following: accounts, bills, evidence of debts, valuable papers, records, abstracts, deeds, manuscripts, or other documents.

Malicious code

Defined as any virus, Trojan horse, worm, or any other similar software program, code or script intentionally designed to insert itself into computer memory or onto a computer disk and spread itself from one computer to another.

Computer Systems

Computer hardware, devices, and electronic equipment used for the purpose of creating, accessing, processing, protecting, monitoring, storing, retrieving, displaying, or transmitting digital assets, including but not limited to, associated input and output devices, laptop computers, desktop computers, data storage devices of all kinds, external drives, magnetic tapes, discs, networking equipment, components, file servers, data processing equipment, computer memory, microchip, microprocessors, computer chips, integrated circuits, systems controlling or associated with the operation or monitoring of equipment or machinery, or similar device or equipment, but not including the digital assets contained therein.

Some carriers have also expanded their definition of computer systems to include any associated devices or equipment including mobile devices and drones.

Computer Virus

Any hostile or intrusive program/software, instructions, code or data which infiltrates and disrupts computer operations, gathers sensitive information, gains access to computer systems or digital assets without consent, or any other data or instructions introduced into any electronic system that affects the operation or functionality of computer systems or digital assets, including but not limited to any destructive program, computer code, worm, logic bomb, Smurf attack, vandalism, malware, Trojan horse, spyware, rootkits, ransomware, adware, keyloggers, rogue security software, or malicious browsers.

Cyber Event

Authorized access, unauthorized access, authorized use, unauthorized use, disappearance of code, malicious act, distortion, malfunction, deficiency, deletion, fault, computer virus, denial–of-service attack, or corruption perpetuated through the insured's computer network, an internet-enabled device or computer systems that occurs during the policy period.

Electronic Data

Facts or information converted to a form usable in computer systems and which is stored on electronic data processing media for use by computer programs.

Malware Attack

An attack that damages a computer system or data contained therein arising from malicious code, including viruses, worms, Trojans, spyware, and keyloggers.

Media

Punch cards, paper tapes, floppy disks, CD-ROM, hard drives, magnetic tapes, magnetic discs, or any other tangible personal property on which digital assets are recorded or transmitted, but not the digital assets themselves.

Network

Any and all services provided by or through the facilities of any electronic or computer communication system, including Fedwire, Clearing House Interbank Payment System ("CHIPS"), Society for Worldwide Interbank Financial Telecommunication ("SWIFT"), and similar automated interbank communication systems, automated teller machines, point of sale terminals, and other similar operating systems and includes any shared networks, internet access facilities, or other similar facilities for such systems, in which the insured participates, allowing the input, output, examination, or transfer of data or programs from one computer to the computer system.

Personally Identifiable Information ("PII")

Information, including health information that could be used to commit fraud or other illegal activity involving credit, access to health care, or identity of an affected individual. This includes, but is not limited to, Social Security numbers or account numbers. It does not mean or include information that is otherwise available to the public, such as names, and addresses.

Personal Sensitive Information

Private information specific to an individual the release of which requires notification of affected individuals under applicable law. It does not mean or include PII.

Privacy Breach

Typically defined as:

1. Theft or improper disclosure of or unauthorized access to any private information in any form while in the care, custody, or control of the insured, third party, or outsourced vendor under written contract including the unauthorized disclosure of such private information or the disclosure of such private information to the wrong party; or the improper or unauthorized disclosure of private information while in transit or at an offsite storage facility.
2. An actual or alleged violation by the insured, or an actual or alleged failure to comply with of any federal, state, local, or foreign law, rule, or regulation (including but not limited to those brought by a data protection authority), relating to the use, collection, storage, disclosure, protection, minimization, destruction, dissemination, retention, other processing of or protection of private information, or failure to comply with notification requirements.

3. The physical loss of any of the insured's laptop computers, computer disks, other portable electronic devices, or any other part of a computer system. Private information means any non-public personal, confidential or proprietary information in any form relating to or owned by any person or entity; including but not limited to metadata, other tags, usage or consumption data, or confidential personal healthcare or financial information of a customer or an employee, including but not limited to account numbers, passwords, biometric data, and personal identification numbers (PINs)

Security Breach

Is typically defined as:

1. The unauthorized access to or unauthorized use of the computer system.
2. The transmission of malicious code, software program or script from the computer system.
3. The theft or unauthorized copying or use of data on the computer system.
4. The infection or implantation of malicious code, software program or script on the computer system.
5. An attack or series of attacks intended by the perpetrator to interrupt, impede or prevent authorized access to such computer system.
6. The physical loss of any of the insureds' laptop computers, computer disks or other computer system.
7. The alteration, corruption, destruction, deletion or damage to electronic data on the computer system.
8. Denial of service attack.

Trade Secret

Information that is stored in an electronic format that has intrinsic value to the organization such that it garners increased protection and is accounted for in the insured's financial statements.

Services

Along with first-party privacy breach response services coverage, carriers are providing additional pre-breach services to aid insureds to identify, mitigate and reduce cyber losses.

Some of the common services include:[9, 10, 11, 12, 13]

1. Active risk management—Work with insureds to find and control computer and network vulnerabilities. For instance, carriers can assist insureds with generating stronger passwords throughout their system. Insurers are also finding ways to partner with leading experts from other industries to bring more comprehensive loss mitigation and prevention services. One industry partnership between a carrier, broker, and two commercial software and hardware companies introduced an all-in-one solution by integrating technology, services, and enhanced cyber insurance coverage.
2. Cybersecurity education and coach helpline.
3. Response readiness assessment.
4. Cyberattack simulation and vulnerability scans.
5. Cybersecurity benchmarking—May monitor and measure the insured's cybersecurity scores from an outside-in approach.
6. Additional services and coverage enhancements—In addition to the traditional first and third-party cyber coverage, some more recent market entrants offer additional coverage enhancements and services. For instance, they may offer a bring-your-own-device ("BYOD") coverage which covers an employee's personal device that is used for business purposes for a cyber loss. Also, cybersecurity mobile applications ("apps") these companies offer may provide threat intelligence, expert guidance and ongoing monitoring as additional services.

9 "Loss Mitigation for Cyber Policyholders"; Chubb.
10 "Protect Your Business before a Cyber Threat"; Travelers; 2021.
11 "Confidence to Thrive in the Digital World"; At-Bay; 2021.
12 "Coverages"; Coalition; 2021.
13 "A comprehensive cyber risk solution"; Cisco.

General Policy Characteristics and Rating Plan

In general, cyber insurance premiums are typically rated based on traditional actuarial ratemaking using schedule rating modifications. A simplified example of a rating plan includes:

Premiums = Base Rate x Increased Limits Factors ("ILF") x Deductible Factor x Cyber-specific Rating Factors x Schedule Modifications

This section provides an overview of some of common policy characteristics such as, limits, attachment points, rating variables, etc. For each cyber insurance policy, there is generally a maximum policy aggregate that caps all insurance loss payouts, in addition to each coverage's limits. For instance, an insured with a $1.5 million policy aggregate limit, and a $1 million limit for each information security and privacy liability coverage and network security liability coverage, will be covered only up to a maximum of $1.5 million even if both coverages are triggered to its maximum limits of $1 million each. However, maximum policy aggregate limits may not apply to certain coverages or sub-coverages such as legal services, public relations, and regulatory fines and penalties. They may have their own specific (often lower) limits. The most common exposure base for cyber insurance policies is revenue. For a global company, the base rate may vary by country or region, or an overall geographic adjustment factor may be calculated.

The base rates for cyber coverages vary, and insureds can opt to select various limits for each coverage, commonly ranging between $50,000 to millions of dollars, and self-insured retentions (attachment points) ranging between $2,500 to $1 million. Common deductibles offered by carriers range from $2,500 to $1 million. Instead of varying base rates for each coverage, some rating plans use one common base rate and determine each coverage premium by multiplying a coverage-specific factor.

For a coverage with a time element component such as business interruption coverage, a waiting period (commonly in hours) factor would be applied to determine the coverage premiums. For example, coverage will only be effective after a 48-hour waiting period from the suspension of the insured's business activity due to a cyber event. The waiting period serves as another layer of insured's retention, in addition to the loss amount retentions. In addition to a waiting period, some carriers also include a protection period factor, particularly for the property damage—protection and preservation of digital assets coverage.

Since the majority of cyber policies are written on a claims-made basis, carriers offer an optional extended reporting period, typically as a factor of the annual premium. This option extends the insurance coverage to a fixed number of years past the original policy period.

Other variables also commonly used to determine premiums are revenue and hazard groups. Insurers use hazard groups to differentiate the riskiness of industries. Businesses that store and utilize numerous PII or sensitive information such as the healthcare and professional services industry will be classified as higher risk hazard groups over others. Insured's revenue is also widely used among carriers as an exposure base for rating. However, there are ongoing debates on whether revenue is an acceptable proxy to indicate the risk level of cyber exposures. Variables such as number of connected devices, number of records, IT spend, or number of employees are also widely discussed and can also be considered as an exposure basis. Some carriers have instead accounted for these factors through schedule rating. For instance, a 25% debit or credit can be applied in rating for the volume of sensitive information stored and managed.

Some of the other characteristics commonly used in schedule rating are:

1. Loss history
2. Type and nature of sensitive information
3. Dependency on network
4. Data encryption and security patch processes
5. Privacy and security control procedures, including awareness training
6. Business continuity and disaster recovery plan
7. Use of third-party vendor management
8. Merger-acquisition activity
9. Age of company
10. Financial condition

Policy Exclusions

Some of the more common cyber-specific policy exclusions are:

1. War, invasion, acts of foreign enemies, hostilities (whether war is declared or not), civil war, rebellion, revolution, insurrection, military or usurped power or confiscation or nationalization or requisition or destruction of or damage to property by or under the order of any government or public or local authority. The exclusion is typically not applied to acts of cyberterrorism.
2. Infrastructure outage, arising out of or attributable to any electrical or mechanical failure or interruption, electrical disturbance, surge, spike, brownout, blackout, or outages to electricity, gas, water, internet access service provided by an internet service provider that hosts an insured's website, telecommunications, or other infrastructure. This exclusion does not apply to failures, interruptions, disturbances, or outages of telephone, cable or telecommunications systems, networks, or infrastructure that are:
    a. under an insured's operational control which are a result of a failure in network security; or
    b. a result of a cyber incident.
3. Nuclear, arising out of or attributable to the planning, construction, maintenance operation, or use of any nuclear reactor, nuclear waste, storage or disposal site, or any other nuclear facility, the transportation of nuclear material, or any nuclear reaction or radiation, or radioactive contamination, regardless of its cause.
4. For property damage replacement of digital assets coverage, the coverage-specific exclusions may include:
    a. Errors or omissions in programming, processing or copying; and
    b. Correcting for any deficiencies or problems including remediation of digital asset errors or vulnerabilities that existed prior to the cyber incident and the insured failed to correct.

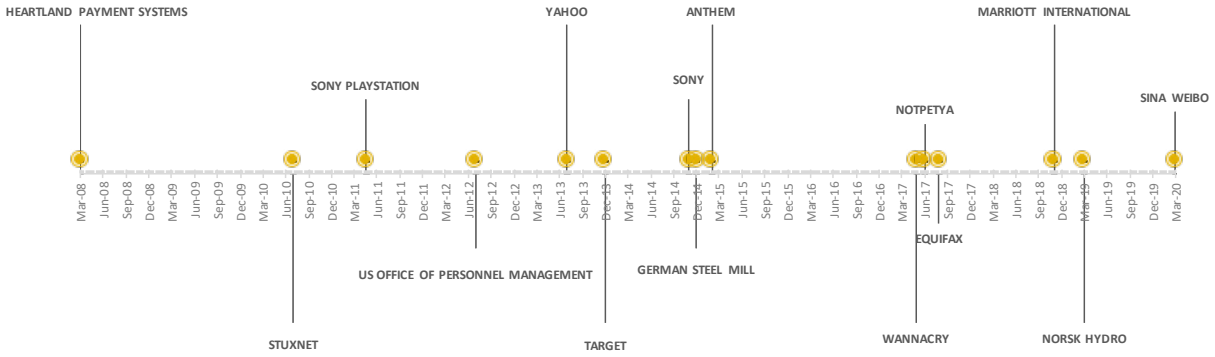
Mondelez v. Zurich

On June 27, 2017, one of the major global cyberattacks, NotPetya, commenced and Ukrainian companies were among the first victims. The NotPetya malware resembled the original Petya virus but spread easily and quickly infected internet networks and disabled computers. Despite a demand for a ransom to unlock these computers, the attack is believed to have been designed to cause massive destruction rather than extortion. Cybersecurity experts believe the attacks were designed to spread as quickly as possible. Shortly after, companies in several other countries including major corporations such as Mondelez International, FedEx, and Maersk among many others were infected. Under a cyber insurance policy, the NotPetya attack would likely trigger a property damage and/or computer attack and cyber extortion coverage from a first party's perspective. This would potentially cover physical loss or damage to electronic data, programs, or software. However, some insurers have defined this cyberattack as an "act of war," an insurance coverage specifically excluded in the policy definition.

Zurich Insurance has denied Mondelez's claim for losses suffered in the 2017 NotPetya attack due to Zurich's "hostile or warlike action" clause and at time of publication this is under litigation in Illinois state court. The policy was a property policy.

Discussion on Case Studies

Figure 7



The timeline shows several large cyberattacks; NotPetya is discussed previously, and others are discussed below.

Norsk Hydro

In March of 2019, the Norwegian-based aluminum maker, Norsk Hydro was attacked by a virus known as LockerGoga, a ransomware that encrypts computer files and demands payment in exchange to unlock them. Norsk Hydro did not pay for the ransom and instead was forced to repair its data from backup systems. As a result, many production-related operations from smelting plants to extrusion plants were halted. By isolating all affected plants and switching to manual operations to prevent the spread of the LockerGoga infection, Norsk Hydro estimated that it was operating at only 50% percent of its original capacity[14] a week following the cyberattack. The company's executives have been reported as positive that this event will be covered by its cyber insurance policy under its business interruption coverage, unlike NotPetya's case where the event can be defined vaguely under certain policy exclusions. In Norsk Hyrdo's 2019 third quarter report it estimated costs of $60 million to $70 million with insurance compensation of $3.6 million.[15]

Sony Cyberattack

The November 2014 cyberattack on Sony Pictures Entertainment was a notable incident in the history of cyber insurance because it was one of the initial attacks which had a motive and was initiated by a nation-state. The hacker group identified themselves as "Guardians of Peace," demanded Sony and its affiliated theatres withdraw the upcoming release of a film, "The Interview" which was supposed to be a comedy involving the North Korean leader, Kim Jong Un. Although the actual hacker identity remains unknown, cybersecurity experts[16] have determined the attack was caused by the North Korean government. During the hack, Sony's computers were disabled, and it lost substantial data stored on its network such as emails, contacts, budgets, etc. The company at the time of the breach had about $60 million[17] in insurance coverage via multiple insurers. This incident is an example of insurance coverage being present when a cyberattack is purportedly perpetrated by a nation-state. A nation-state attack can be broadly defined[18] as an act of war since it is the intent of a nation's government. However, in 2014, some cyber insurance policies may or may not have had a specific nation-state or act of war exclusion, which presents coverage inconsistencies across the insurance industry. More of an issue is that some insurers may not even have contemplated this exclusion when offering coverage, putting them at great risk of a catastrophic loss.

14 "Norsk Hydro Unit Begins Operating at 50% of Capacity After Cyber Attack"; *Insurance Journal*; March 21, 2019.
15 "Insurance Pays Out a Sliver of Norsk Hydro's Cyberattack Damages"; *Threat Post*; Oct. 30, 2019.
16 "The Sony Pictures Hack, Explained"; *The Washington Post*; Dec. 18, 2014,
17 "Your cyber insurance isn't protecting you from elite hackers"; Cyberscoop; Nov. 3, 2016.
18 "Cyber Attack, or Act of (Cyber) War?"; *Insurance Journal*; Feb. 2019.

German Steel Mill[19]

In December 2014, phishing emails that contained malicious code once opened, were sent to target on-site industrial operators of a German steel mill (undisclosed). The emails allowed the attackers to gain access to credentials of any unsecured systems and connections, including the steel mill plant's network, which ultimately caused failures to multiple components of the Industrial Control Systems ("ICS"). This incident is designated by the National Institute of Standards and Technology as an Advanced Persistent Threat attack which is classified as highly targeted attacks on organizations that often have full-time staffing and monetary support to pursue operations usually for the purposes of espionage. No definitive evidence has been concluded to date on the motive of this attack, however, the 2014 annual report by Germany's Federal Office for Information Security, suggests that the attack was intentional since the perpetrators had advanced knowledge on ICS. This pivotal incident in the history of cyberattacks is known to have caused massive physical and material damage. Aside from another Stuxnet[20] cyberattack in 2010, to date, it is unknown whether the losses on this steel mill was covered by insurance. Cyber insurance coverage at the time of the attack typically excluded physical loss, but property and general liability policies would likely have covered property damage unless a cyber event was specifically excluded. Alternatively, crime and fidelity policies would also provide coverage if the attack was determined to be from an employee of the company. If coverage were indeed provided through these non-cyber policies, this is likely another case of "silent cyber."

19 "A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever"; *Wired*; Jan. 8, 2015.
20 A sophisticated digital weapon the U.S. and Israel launched against control systems in Iran in late 2007 or early 2008 to sabotage centrifuges at a uranium enrichment plant. That attack was discovered in 2010.

Cyber Threat Landscape

Published August 2021

The cyber threat landscape is continually changing and evolving as attackers develop new tools and discover new attack vectors and defenders find new techniques to counter these attacks. Machine learning and artificial intelligence are being increasingly used by both attackers and defenders, and the importance of these tools is likely to increase in the future.[21] Modern computer networks are complex systems, and a weakness in any component of the system could render the entire system vulnerable.

Most businesses today rely heavily on computer systems, and when these systems do not function as expected or when private data is stolen or lost, the impact to the business can be significant. When critical network infrastructure is compromised (either made unavailable or accessed by unauthorized individuals), the business can be impacted in a number of ways, including:

- Business interruption—Data loss (whether accidental or due to hostile action) could hamper a company's ability to conduct business. For example, if a company's inventory control database goes down, the company may be left unable to handle outgoing orders, leading to significant financial harm. Likewise, if a company's online store website stops working, revenue may plummet.
- Competitive risk—A company may store proprietary business information such as product designs, business strategies, and pricing/cost information on computer systems. If these systems are compromised and the information falls into the hands of a competitor, the company may be placed at a competitive disadvantage.
- Liability risk—Many companies store user and/or employee data. If this information is not handled securely, a company may be held legally liable for any harm caused.
- Direct costs—Victims of cyberattacks may incur significant costs related to the incident. This could include costs for investigation and defense of regulatory actions associated with the incident, payment of ransoms, fines or penalties, costs to restore or replace digital assets, and costs for legal assistance and credit monitoring for victims of the breach.

21 "The Real Challenges of Artificial Intelligence: Automating Cyber Attacks"; Wilson Center blog post; Nov. 28, 2018.

Who conducts cyberattacks, and why?

Attackers use knowledge of computer hardware and software to identify and exploit vulnerabilities in computer systems and networks. These attacks may be conducted by individuals or groups, and the attackers' motives and skill levels vary widely. Some attacks are sophisticated, using previously unknown techniques and vulnerabilities to gain access to the target system. Such attacks typically require advanced knowledge of software design and network services. Other attacks are launched using publicly available hacking software. These attacks do not require any specialized knowledge and can be launched by anyone who can find the software online.[22] While cyberattacks often come from outside an organization, there is also a significant risk of insider attacks from employees who misuse their access to company data and computer resources. A 2018 survey of cybersecurity professionals found that over half had dealt with insider attacks within the previous 12 months.[23]

Cybercrime can be remarkably lucrative. An estimated 76% of 2018 cyber breaches were conducted due to the attacker's financial motivation.[24] A 2018 study found that low-earning cyber-criminals can bring in $3,500+ per month, middle-earners can make $75,000+, and high-earners can make over $166,000 per month.[25] Some make money by holding data "hostage." These attackers gain access to a user's system and install software (ransomware) that encrypts data on the user's system using an encryption key known only to the attacker. To regain access to the data, the user is required to make a payment to the attacker, who then provides the key to unencrypt the data. Paying the ransom does not guarantee that data access will be regained. A 2019 report found that 38.8% of organizations that paid the ransom as directed still lost their data despite paying the ransom.[26] Cybersecurity experts generally recommend against paying such ransoms.[27]

Other attackers attempt to gain access to companies' systems in order to steal the data stored there. Common targets for theft are personally identifiable information (PII), such as names, birthdates, addresses, phone numbers, and Social Security numbers; personal financial information (PFI), such as bank account and credit card numbers; and protected health information (PHI), such as medical history and diagnoses. This information can be used directly for identity theft, sold on the black market, or used as the basis for other types of fraud.[28] Attackers may also target data regarding a company's intellectual property (IP), which can be sold to competitors or on the black market.

22 "Script Kiddie: Unskilled Amateur or Dangerous Hackers?"; *United States Cybersecurity Magazine*.
23 *Insider Threat—2018 Report*; Cybersecurity Insiders and Crowd Research Partners; 2017.
24 *2018 Data Breach Investigations Report*—Executive Summary; Verizon; 2018.
25 *Into the Web of Profit*; Bromium; April 2018.
26 *2019 Cyberthreat Defense Report*; Cyber-Edge; 2019.
27 "Why You Should Never Pay A Ransomware Ransom"; *Forbes*; March 9, 2018.
28 "Hacked Health Records Prized for their Black Market Value"; Fox Rothschild blog post; March 16, 2015.

While most cybercrime is driven by financial motives, some cyber criminals are motivated by other goals such as making a political statement, trying to cause disruption to a specific organization, or simply trying to disrupt society at large. For example, the Anonymous "hacktivist" group made headlines for its attacks on PayPal and Mastercard (2010), Sony (2011), and various U.S. government websites (2012).[29] The group was named one of Time magazine's "World's 100 Most Influential People: 2012".[30] The motivation for these attacks was apparently political, not financial,[31] though the financial impact on the affected organizations was significant. For example, the losses to PayPal were estimated at almost $5 million.[32]

Other cyberattacks occur on behalf of nation-states. Such attacks may intentionally target private companies for strategic reasons.[33] For example, in 2014, attackers broke into the computer networks of Sony Pictures Entertainment, stole a large amount of data, and then erased many of the company's servers,[34] costing the company an estimated $35 million in repair and recovery costs.[35] In 2018 the U.S. Department of Justice officially charged a North Korean programmer (believed to have been operating at the direction of the North Korean government) for his participation in this and several other cyberattacks. The motivation for the Sony attack is believed to have been Sony Pictures' planned release of a comedy film depicting the assassination of the North Korean leader.[36] Private firms may also be unintended targets of government-sponsored attacks. The NotPetya attack, described below, is believed to be an example of one such scenario.

Threat vectors

The complexity of the software and hardware underlying modern computer networks affords attackers a multitude of points upon which to focus their efforts. In practice, external attackers usually rely on legitimate users of the system to gain initial access to a company's network, and then use other techniques to continue the attack. A company targeted in a cyberattack may also be attacked through a third-party vendor or contractor who has access to its systems. In order to properly assess its cyber risk profile, a company may also need to evaluate the systems and protocols of other entities and contractors with whom it has a business relationship.

29 "The Return of Anonymous"; *The Atlantic*; Aug. 11, 2020.
30 "Anonymous"; Time 100: The List; April 18, 2012.
31 "Hacker group Anonymous is a nuisance, not a threat"; *CNN Money*; Jan. 20, 2012.
32 "Anonymous cyberattacks cost PayPal £3.5m, court told"; *The Guardian*; Nov. 22, 2012.
33 "Today's enterprises face increasing risk of state-sponsored cyberattacks"; *Thomson Reuters*; Jan. 14, 2019.
34 "The Sony Hackers Were Causing Mayhem Years Before They Hit the Company"; *Wired*; Feb. 24, 2016.
35 "Hack to cost Sony $35 million in IT repairs"; *Network World*; Feb. 4, 2015.
36 "North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions"; U.S. Department of Justice; Sept. 6, 2018.

In the most common form of external attack, known as "phishing," an attacker sends an email message to recipients within the company. The message appears to be legitimate but may contain an infected attachment which, if opened, will grant the attacker access to the recipient's computer. The email may also contain a link to a fake login page, where the attacker can collect the user's login credentials. A 2017 report concluded that 90% to 95% of successful cyberattacks were launched via phishing attacks.[37] If a computer's software is misconfigured or outdated, merely visiting an infected website or opening an infected email could be enough to give an attacker access to the machine.

Attackers may also use software vulnerabilities to gain access to a target system. A software vulnerability may be the result of a misconfiguration (for example, the system administrator may forget to change a default password) or may be due to a problem with the design or coding of the software itself (these are commonly referred to as "bugs"). Many software producers periodically release updates, or "patches," to their software to fix recently discovered bugs. Attackers may use known vulnerabilities to attack unpatched, out-of-date systems, or may use publicly unknown "zero-day" vulnerabilities to attack fully up-to-date software. Additionally, some network-connected devices may not receive security updates from the device manufacturer, or the manufacturer may stop providing patches after some period of time. Companies may also delay applying security patches to production-critical systems, as carrying out the update may require a temporary production slowdown or shutdown. These vulnerable, unpatched devices and systems can become entry points, allowing attackers to gain access to other parts of a company's network.

The majority of cyberattacks are carried out by external attackers, but an estimated 28% of attacks in 2018 involved some level of participation by a company employee.[38] Given that employees typically have a legitimate need to access company systems and data, insider attacks can be especially difficult to defend against.

The use of simple/weak passwords, or the re-use of login credentials across multiple websites, can also contribute to the vulnerability of a company's system. Simple passwords are vulnerable to dictionary-based attacks, where attackers use "dictionaries" of common words/passwords to attempt to gain access to password-protected systems. Even complex passwords, if not of sufficient length, are vulnerable to "brute force" attacks wherein the attacker tries every possible password combination. Many organizations have implemented password complexity and length requirements in order to mitigate against such attacks.

37 "Phishing Remains Top Cyberattack Vector in 2017"; *Infosecurity Magazine*; Sept. 27, 2017.
38 *2018 Data Breach Investigations Report—Executive Summary*; Verizon; 2018.

Once attackers have obtained a legitimate user's login credentials (username and password), they may attempt to use the stolen credentials to access other systems in a process known as "credential stuffing." In a 2018 study, 52% of users were found to reuse identical or slightly modified passwords across multiple online services.[39] In a corporate environment, the practice of password re-use can allow an attacker who has gained initial entry to company systems to easily move into other parts of the network. An attacker who gains access to company systems may also wait for weeks or months before actually launching the attack at a time that will maximize its impact.[40]

Examples of incidents

Recent history offers numerous examples of the impact a cyberattack can have on a company. The following incidents illustrate the variety of forms that such attacks can take and the variety of motivations that may lie behind these attacks.

Target data breach

During a two-week period in late 2013, attackers stole approximately 40 million credit and debit card numbers and 70 million customer records from the Minnesota based retailer Target Corporation. While some recent data breaches have been much larger in terms of the number of records exposed, the incident had a high profile at the time and helped to accelerate movement toward greater security within the payment card industry.[41] The breach is also notable for the relatively complex approach the attackers used to access Target's systems. The attackers used a phishing email to gain access to the network of a refrigeration contractor that provided services to Target. The attackers were then able to collect the credentials used by the contractor to access Target's vendor systems. The attackers were able to use their access to Target's vendor portal to gain access to other portions of the company's systems. Eventually, the attackers reached their goal: Target's in-store point-of-sale terminals that process credit and debit card transactions. The attackers installed software on the terminals that would capture credit and debit card information and periodically send it to a compromised server within Target's network. The attackers could access this server and retrieve the stolen information as needed.[42] As of 2016, Target had incurred a reported $291 million of costs related to the breach, of which roughly $90 million was expected to be covered by the company's cyber insurance policies.[43]

39 "The Next Domino to Fall: Empirical Analysis of User Passwords across Online Services"; Chun Wang et al., 2018.
40 "The Covid-19 Pandemic Reveals Ransomware's Long Game"; *Wired*; April 28, 2020.
41 "Target targeted: Five years on from a breach that shook the cybersecurity industry"; We Live Security; Dec. 18, 2018.
42 "Anatomy of the Target data breach: Missed opportunities and lessons learned"; *ZD Net*; Feb. 2, 2015.
43 "Target's Cyber Insurance: A $100 Million Policy vs. $300 Million (So Far) In Costs"; Patterson Belknap blog post; April 7, 2016.

Dyn distributed denial-of-service (DDoS) attack

The 2016 Dyn attack was short-lived but is an example of a DDoS attack and a possible catastrophic loss scenario for cyber insurers. This attack was directed at a Domain Name Service (DNS) provider, Dyn, which served several prominent websites. The services provided by Dyn translate easily remembered domain names to the more cryptic numeric internet protocol (IP) addresses used to route traffic on the internet. The Dyn attack took place in three waves on October 21, 2016, and caused several well-known websites to become temporarily unavailable including Amazon, the BBC, CNN, GitHub, Netflix, PayPal, Sony PlayStation Network, Squarespace, Twitter, and Visa.[44,45,46] The attacker(s) flooded the Dyn DNS servers with so many fake requests for DNS information that the company's systems were temporarily overloaded and unable to respond to genuine DNS requests. During this period, many users were unable to visit the impacted websites because their web browsers were not able to retrieve website IP addresses from the Dyn servers. The attack was conducted, at least in part, using a "botnet" consisting of tens of thousands of internet-connected devices such as digital video recorders and web cameras. Due to poor security on these devices, attackers were able to cause them to direct a huge amount of bogus traffic toward the Dyn servers.[47] As of this writing, the attacker(s) behind the Dyn attack have not been publicly identified.[48] There was no obvious financial motive for this attack, and some have suggested that a disgruntled gamer launched the attack in an effort to take Sony's PlayStation Network offline.[49] This incident is an example of a catastrophic risk for cyber insurers. In this case, many companies relied on a single entity (Dyn) to provide critical DNS services, and when Dyn was attacked, the effects were widespread. Because the impacted websites were restored quickly, the financial impact of this attack was relatively small. One estimate pegged the total costs of the attack at $110 million, most of which would fall within the insureds' cyber insurance policy deductibles.[50]

NotPetya attack

As of 2020, the costliest cyberattack has been the 2017 NotPetya attack, with total costs estimated as high as $10 billion. The attack began in Ukraine but quickly spread to countries around the world. At its outset, the incident appeared to be a typical ransomware attack. Once the malware gained access to a company's computer systems it would spread

44 "Friday's third cyberattack on Dyn 'has been resolved,' company says"; *CNBC*; Oct. 21, 2016.
45 "Here are the sites you can't access because someone took the internet down"; *Splinter*; Oct. 21, 2016.
46 "U.S. internet disrupted as firm hit by cyberattacks"; *CBS News*; Oct. 21, 2016.
47 "The DDoS Attack Against Dyn One Year Later"; *Forbes*; Oct. 23, 2017.
48 "FBI: How we stopped the Mirai botnet attacks"; TechTarget; March 7, 2019.
49 "Angry Gamer Blamed For Most Devastating DDoS Of 2016"; *Forbes*; Nov. 17, 2016.
50 "Types of cyber incidents and losses"; Enhancing the Role of Insurance in Cyber Risk Management; *OECD Publishing*; Dec. 8, 2017.

automatically from computer to computer, causing the victim's computers to spontaneously shut down. When restarted, the screen would display a message giving the user instructions for paying a ransom and obtaining a key to decrypt their data. Some victims attempted to pay the ransom following the instructions shown on the screens of their locked computers but discovered that the payment did not cause their data to be unlocked.[51] Researchers soon discovered that the data had been encrypted with a random key, so there was no way for the attackers to unlock the data, even if they wanted to do so.[52]

Later investigation revealed that the attack had begun with the servers of a Ukrainian software company that produced a piece of accounting software used widely within that country. Attackers took control of the company's update servers and used them to send the NotPetya malware, disguised as a software update, to computers running the accounting software. The malware took advantage of two vulnerabilities in the Windows operating system to spread automatically within the networks of infected companies. First, the NotPetya worm used a known vulnerability to gain access to unpatched systems. Then a second vulnerability allowed the malware to use the compromised system to find usernames and passwords, which gave it access to other computers with fully up-to-date software. After taking over a target machine, the malware would alter the information stored on the computer's hard drives, effectively destroying any software and data located there. The worm spread with incredible speed, taking down the networks of several large Ukrainian companies in less than 60 seconds from the time the first computers in those networks were infected.[53] The worm quickly spread beyond Ukraine, impacting companies in a wide range of locations and industries. Two of the most heavily impacted companies were the Danish shipping company Maersk and the U.S.-based delivery company FedEx, each of which lost approximately $300 million due to the attack.[54] At the time of the attack, neither company appeared to have had a cyber insurance policy in place to cover such an attack.[55,56] Food and beverage company Mondelez carried a property insurance policy that supposedly provided coverage for "physical loss or damage to electronic data, programs, or software including physical loss or damage caused by the malicious introduction of a machine code or instruction".[57] The company filed a $100 million claim to cover the damages incurred as a result of the attack.[58]

51 "The Untold Story of NotPetya, the Most Devastating Cyberattack in History"; *Wired*; Aug. 22, 2018.
52 "ExPetr/Petya/NotPetya is a Wiper, Not Ransomware"; SecureList; June 28, 2017.
53 "The Untold Story of NotPetya, the Most Devastating Cyberattack in History"; *Wired*; Aug. 22, 2018.
54 "Is the world ready for the next big ransomware attack?"; CSO Online; March 4, 2019.
55 "Risk management"; Maersk; 2017.
56 "Cyber attack, hurricane weigh on FedEx quarterly profit"; *Reuters*; Sept. 19, 2017.
57 "Cyber Warfare and the Act of War Exclusion"; International Comparative Legal Guides; 2020.
58 "Cyber Insurance Not Valid in Case of Cyber War, Says Major Insurance Company"; *CPO* magazine; Jan. 17, 2019.

Shortly after the attack, Ukrainian officials placed blame on Russia, with which Ukraine was embroiled in an undeclared war.[59] In 2018, the U.S., U.K., and Australian governments officially attributed the attack to the Russian military,[60] though no proof of this allegation has been made public. Government officials believe that the Russian goal was to disrupt Ukrainian energy production and financial and government operations,[61] and that damage to other companies was unintentional. Following this official attribution, Mondelez's insurer denied the company's claim, citing the policy's "act of war" exclusion.[62] This claim denial is reportedly the subject of ongoing litigation between Mondelez and the insurer. [63]

59 "Cyberattack Hits Ukraine Then Spreads Internationally"; *The New York Times*; June 27, 2017.
60 "US, UK, Australia Warn Russia of 'International Consequences'—NotPetya Outbreak Attributed to the Kremlin"; *WCCF Tech*; Feb. 16, 2018.
61 "Russia Accused of Massive $1.2 Billion NotPetya Cyberattack"; *Newsweek*; Feb. 15, 2018.
62 "Cyber Insurance Not Valid in Case of Cyber War, Says Major Insurance Company"; *CPO* magazine; Jan. 17, 2019.
63 "Mondelez's action against Zurich signals potential gap in cyber policies"; *Insurance Business America*; April 4, 2019.

Silent Cyber

Published August 2021

As cyber risks continue to emerge, insurers are facing losses from unintended coverages, despite explicit coverage of cyber perils in their underlying written policies. With each day, the world faces emerging cyber threats, including infrastructure attacks, identity theft, data breaches, hackers, and malware. This unintentional, non-affirmative coverage—or "silent cyber" risk—can be devastating to insurance and reinsurance companies.

While silent cyber is not a new issue in the property and casualty industry, it has become much more pronounced as businesses continue to be more connected than ever and the frequency of high-profile cyberattacks has increased. For instance, the NotPetya global cyber catastrophe in 2017 resulted in billions of dollars in losses to affected businesses.

Due to the potentially devastating financial impact on the insurance market, global rating agencies and regulators are increasingly scrutinous with regard to the risk of silent cyber and the debilitating effects it could have on an insurer. For example, the insurance credit rating agency AM Best announced it "expects companies to be proactive and forthcoming with their own evaluation and measurement of the exposure and accumulation of their cyber liability exposure."[64] More clarity on coverages (or lack of) would be beneficial for all stakeholders.

A greater concern for insurers is not the affirmative coverage of cyber perils, but the potential silent cyber risk underlying traditional insurance policies. In other words, insurers are concerned about the risk that a cyber event could trigger unexpected payouts under existing policies where the cyber risk was not considered and/or priced.

Wording of policy terms has not evolved at the rapid pace that technology has. This has led to ambiguity as cyber coverage may be available under policies that were not originally designed for this exposure. Businesses have increased their dependency on technology and have welcomed the use of online networks. Although technology increases the efficiency of business operations, there is a trade-off because of the increased exposure to technology misuse, ultimately harming the business and its customers. Many evolving cyberattacks were not even anticipated when the insurance policy forms were written in the pre-digital era.

64 "What is Silent Cyber Risk"; *Insurance Business;* Nov. 26, 2018.

If a policy does not have named perils coverage, there is a potential for coverage for anything not explicitly excluded. Typically, ambiguity in an insurance policy is viewed in favor of the insured, as the carrier is the author of the insurance contract wording and therefore responsible for clarity of coverage. Even policies written to provide affirmative coverage of cyber perils face silent cyber risks. As cybercrimes continue to emerge, the covered perils must keep up.

The systemic nature of cyber risk means silent cyber is becoming prevalent in virtually every type of insurance policy and line of business. Further, cyber attacks do not rely on geographical boundaries, and therefore could be one of the largest sources of accumulation risk in the insurance industry.

Insurers in the global insurance market have made initiatives to begin the "affirmation" process of cyber risk. Affirmative cyber coverage is expanding as the demand for cyber insurance products increase and exposures continue to grow, providing ample opportunities for the market. Further, offering affirmative cyber coverage can incentivize insureds to improve their cyber "hygiene," ultimately reducing losses.

Managing Silent Cyber Exposure

It is difficult for insurers to assess their silent cyber exposures due to the complications surrounding cyber risk. Determining exposure is complicated by ambiguous policy wording, disparate data systems and sources, and the ever-evolving nature of cyber risk. Therefore, the insurers may not have charged adequate premiums to address the extent of their exposure and cover this aspect of the risk. Additionally, given the developing nature of cyber risk and also the development of relatively new insurance products, assessing silent cyber risk requires new skill sets and knowledge for companies and their underwriters.

There are two major aspects of silent cyber risk: unintentional coverage and unpriced coverage.

Unintentional coverage occurs when insurance policy language does not explicitly address the potential for loss caused by a cyber incident or a cyberattack. For example, consider a hypothetical cyberattack that hacked the industrial control system of a dam. Such an attack could result in millions of dollars of property and flood damage covered by the policy language where flood is the covered cause of loss. In this example, many lines of business covering the dam and its operator could have potential exposure to silent cyber losses due to unintentional coverage. In today's connected world, even many cars and homes have significant cyber exposure.

Coverage that is extended without having been initially incorporated into its pricing occurs when there is no adjustment made to the policy pricing to account for the potential unintentional cyber risks or cyber risks that were assumed to be very insignificant. In the dam flooding example, there would be unpriced coverage if the pricing did not consider the potential rise of frequency and severity of floods due to third-party liability resulting from cyberattacks. Over time, pricing would respond to cyber claim emergence regardless of the original recognition of the coverage. That is, the cyber claims will drive up the price of the policies.

To manage risks, insurers typically review their policy forms continuously and carefully for all lines of business. It is also an important consideration of how policies written coordinate with the reinsurance coverage purchased by the insurer for these potential cyber losses. For example, do the insurer's reinsurance policies exclude losses caused by a cyberattack? If so, the insurer could face a catastrophic loss due to lack of protection. The previous example of the flood damage caused by the cyber attack on the dam raises the question of whether the policy should explicitly list or exclude cyber as a named peril.

One aspect of silent cyber risk is an expectation gap between an insurer and the insured on coverage written in the traditional lines that do not explicitly include or exclude cyber risk. Due to this misperception of coverage, there may be increased friction and legal action against the (re)insurers. Further, when ambiguous policy wording exists, some court rulings have favored the insured, and therefore the potential legal judgments could add to the costs of silent cyber risk.

After their first unintended cyber claim payment, some insurers might either exclude or sub-limit cyber risk from new standard policies and renewals. Granting affirmative full cyber limit coverage for an additional premium in such legacy policies has not been common and has developed slowly. By observation of some large insurance companies, the 2017 total amount of cyber-related business interruption claim payments were greater under property insurance policies than under stand-alone cyber policies or an endorsement.[65] To limit silent cyber exposure, companies can either explicitly exclude it from policies, or offer a cyber standalone policy (or an endorsement). These actions may take several years as companies adjust underwriting and policy forms but is an essential element for creating clarity, ending the ambiguity around the coverage, and helping insurers best manage their exposure.

In a competitive insurance market environment, it can be difficult for insurers to address silent cyber, as they have concerns over losing business to their competitors. Despite this fact, several participants in the marketplace have taken strides to address their silent cyber exposures. In July 2019, Lloyd's of London unveiled a plan ordering its syndicates to explicitly affirm or exclude cyber coverage to avoid any silent cyber complications. The Lloyd's mandate was phased and aimed to address all policy types by July 2021.[66]

In January 2018, Insurance Services Offices (ISO) of Verisk Analytics introduced standardized cyber insurance forms.[67] Further, major market participants have moved to address silent cyber. In 2019, AIG stated that it will begin to account for silent cyber by affirmatively covering or excluding cyber risk in virtually all of its commercial property or casualty policies by 2020.[68] These changes require great effort, and it may take time for other carriers to follow suit.

Challenges to Quantifying Silent Cyber

There are challenges in changing policy language and coverage issues to address pricing silent cyber risk. Because cyber risks are expanding and evolving at a rapid pace, it is difficult to expect or predict what future types of losses and claims may look like. Anyone with a computer, time, and creativity could cause trouble. There are many cyberattack software tools available for sale on the "dark web." Every individual and entity that engages the internet must be careful about their online security and behavior. A simple lapse in judgment or protocol in place for company employees could cause a major data breach,

65 "Future of Insurance to Address Cyber Perils"; *Insurance Thought Leadership*; Oct. 31, 2018.
66 *Recent Clarifications in Traditional Insurance Lines*; Marsh JLT Specialty; June 2020.
67 "ISO's New Cyber Insurance Program Implemented in 42 States and U.S. Territories"; Verisk; March 19, 2018.
68 "AIG to affirm or exclude cyber cover in P&C policies from January 2020"; *Commercial Risk*; Sept. 6, 2019.

releasing personal consumer information or critical internal company information and create consequential catastrophic business interruption and losses. Further, a loss could occur if the protocols were in place, as cybercrimes are becoming more and more sophisticated and far-reaching. Continuous surveillance of potential targets and vulnerabilities, rigorous security measures and protocols, monitoring, and a reactive plan and practice can all help lower the risk and reduce possible consequences.

Cyber risk assessment requires data that is not typically collected in traditional property and casualty insurance exposure datasets. For example, underwriting for medium and small policies typically follow a very streamlined process. To address the complexity of the issues and to attempt to quantify the silent cyber risk, collective expertise from various perspectives such as underwriting, actuarial, claims, risk engineering, and information technology (IT) experts is needed. During the insurance underwriting process, it would be optimal to collect information regarding an insured's website and any supply chain dependencies they have. When underwriting a risk, an insurer would typically learn more about the insured's cybersecurity strength and effectively communicate this to the pricing actuaries. If an insurer were to specifically exclude cyber perils from their policies, an insured might need to request an endorsement for cyber coverage. This method would trigger a more thorough underwriting process because the underwriters will need to explore the insured's cyber exposure.

Insurers typically do not have sufficient historical data to accurately forecast their future silent cyber risk exposures and price appropriately. To date, there have been a handful of catastrophic cyber events, each impacting millions of individuals or hundreds of businesses simultaneously. To review silent cyber exposure, insurance companies can start by compiling their exposure data from various policy forms and systems supporting all their lines of business. This can be a daunting task, as many questions need to be answered during this process, such as determining whether all policy limits are exposed and how policies with exclusions and sub-limits are treated.

With some basic information, insurance companies can set a tolerance level for silent cyber risk based on the line of business' earnings and surplus. To quantify the silent cyber exposure, insurers can determine the range of potential exposures that could result from a cyber event and then overlay those exposures with their existing insurance portfolio. A number of vendors have also developed software for assessment of some cyber risks, which may add additional insight.

A major struggle is the lack of statistically significant actuarial data to model risk. Many property and casualty coverages have experienced vulnerabilities. For example, if a business is located in the U.S. Gulf Coast, there is significant and measurable hurricane risk. Cyber perils, however, do not have physical constraints, and businesses can be impacted on a global basis overnight. The lack of boundaries on a cyber peril loss can ultimately lead to large accumulation risk across all policy types.

Normally, data modelers and carriers rely on historical data; however, quantifying cyber exposure is a *forward*-looking exercise. Many losses that may have been cyber-related may not have been previously identified as such or coded as a cyber peril in the data. Therefore, there is a compounding effect of both the lack of data and the historical data not being indicative of the future silent cyber risks as technology is rapidly evolving. The immaturity of silent cyber risk makes it even more difficult for insurers to quantify their risks.

It is also difficult for insurers to compare the reasonability of modeled results for silent cyber against actual claims experience because this is not generally recorded. In the absence of data, determining the potential scale of cyber losses requires a large element of judgment. Another implication affecting consideration of silent cyber is legal judgments. It can be difficult to assess how decisions might determine the extent of coverage under non-affirmative policy wordings. Lastly, keeping models up to date in such a rapidly evolving claims environment represents a major challenge. For some carriers, a handful of legal claims could drive the loss ratio. This has a potential to create a lack of credibility for analyzing the experience.

Conclusion

Ultimately, the way to address silent cyber risk is to examine the ambiguities and provide affirmative and specifically priced cyber coverage. In some lines of insurance business, at least initially, there may be explicit exclusions. Many cyber experts view future cyber catastrophes that have a much larger and more significant ramifications than what has been experienced so far as not "if" but "when." As cybercrimes continue to escalate, the availability of more claims data will allow the production of more sophisticated models to help insurers and reinsurers better understand the possibilities presented by cyber as an insurance product and the risks posed by cyber as a peril. In most developed global markets, cyber insurance will become one of the key growth areas for insurers over the next decade.

Cyber Data

Published August 2021

Unlike most other property/casualty insurance lines of business where insurers typically have relied on vast amounts of premium, exposure, and claims data collected over many years to develop tools based on statistically significant results, cyber insurers have historically had a lack of in-house data for evaluating cyber risk. While the amount of data available to cyber insurers is growing, standard actuarial pricing models used for other property/casualty lines of business do not work as well with cyber because insurers have either just entered the market and therefore have limited data, or they have been writing cyber for years but the exposure continues to evolve. This same limitation applies to reserving for cyber as well.

Through the lens of cyber, incident data may be viewed as referring to events whether insured or uninsured, cyber insurance applications, threat intelligence,[69] outside-in vendor scoring,[70] an organization's internal risk assessment, and security vendor research papers, among others. The term "data" in the context of cyber can be difficult to define as each individual or organization may have a different perspective of what to include when it comes to cyber data. For the purpose of this general overview, details will be primarily discussed that are directly related to cyber data as collected via the cyber insurance placement process and claims activity received from insureds that have purchased cyber insurance. For future overviews and actuarial research, there are other areas of cyber data to explore such as security industry publications, threat intelligence feeds,[71] vulnerability scans, and professional services publications from law firms and forensics providers.

Availability

Historically and even today, there is limited data on the linkage between an entity's propensity to experience a cyber incident and its security risk and vulnerabilities. In addition to the continuously developing and changing cyber landscape, the high level of complexity of these risks and breaches can lead to a misattribution of signal versus noise when it comes to the leading indicators of a future cyber incident. However, the availability of cyber data from both a security and incident perspective are growing with the digitization of society and business. The digitization of organizations changes the cyber risk landscape but also allows for valuable information to be extracted and organized by technology in a way that helps inform cyber insurance decision making.

69 Cyber threat intelligence: information about threats and threat actors which helps mitigate harmful events. Example of sources: social media, intelligence from the dark web.
70 Risk/threat measures by scanning a company's network perimeter to identify security risks and weaknesses.
71 Real-time data providing information on potential cyber threats and risks.

Actuaries often look at historical events as being indicative of future risk. In the cyber risk environment, a continually improving internal security environment within organizations and continually evolving adversaries create additional complications that are not as pervasive with other insurance lines of business. Just because a certain vulnerability is patched within an organization does not mean that a threat actor will not pivot to a different vulnerability or access point to achieve their objectives and cause a loss to the organization. Additionally, reliance upon common software suites or technology vendors creates a systemic aggregation issue that is not as common with other types of risks.

In addition to the evolving changes, new laws surrounding cybersecurity and data privacy are being put in place around the globe. These new laws provide additional potential liability risks associated with noncompliance or a lack of appropriate internal controls. Understanding the potential liabilities associated with these laws is important, as a historical event may have a significantly higher cost to an organization had the incident occurred after the law went into effect. Where certain liability lines of business deal with social inflation and nuclear verdicts,[72] cyber events have a similar concern over inflation due to changing laws and class action settlement trends.

Challenges

Within any new insurance market, insurers are hesitant to underwrite risk they do not fully understand. To prevent unexpected losses, insurers have historically employed a conservative strategy by structuring coverage under narrow terms and conditions (e.g., low limits, high retentions, etc.). As a new line of business matures and more experience emerges, these initial restrictions might be loosened. A similar evolution has been observed in the cyber insurance marketplace in which sub-limits that were once common have now been removed, waiting or qualifying periods have decreased, and the amount of capital to support most limits requested by insureds has increased. However, the broadened coverage terms always have the potential to revert back toward more restrictive terms if significant losses materialize.

72 Awards that are considered to be out of proportion with the damages suffered.

Despite the maturation of cyber insurance, there is still a concern around how well organizations understand what cyber insurance will or will not cover. Due to restrictions in terms and conditions or a lack of understanding of the product, insurance buyers may feel the product does not adequately meet their needs. For example, an organization may choose *not* to purchase cyber business interruption coverage within its cyber insurance policy. If that organization has a cyber business interruption event, the insurer will appropriately deny covering the claim because business interruption coverage was not purchased. The organization may still sue for coverage either because they did not understand that they did not have coverage or they are hoping there is enough ambiguity in the insurance policy that coverage may still be provided. This conundrum over the lack of understanding of terms and conditions within cyber insurance policies could lead to a lower amount of cyber insurance purchased, which can in turn reduce the amount of data insurers can collect.

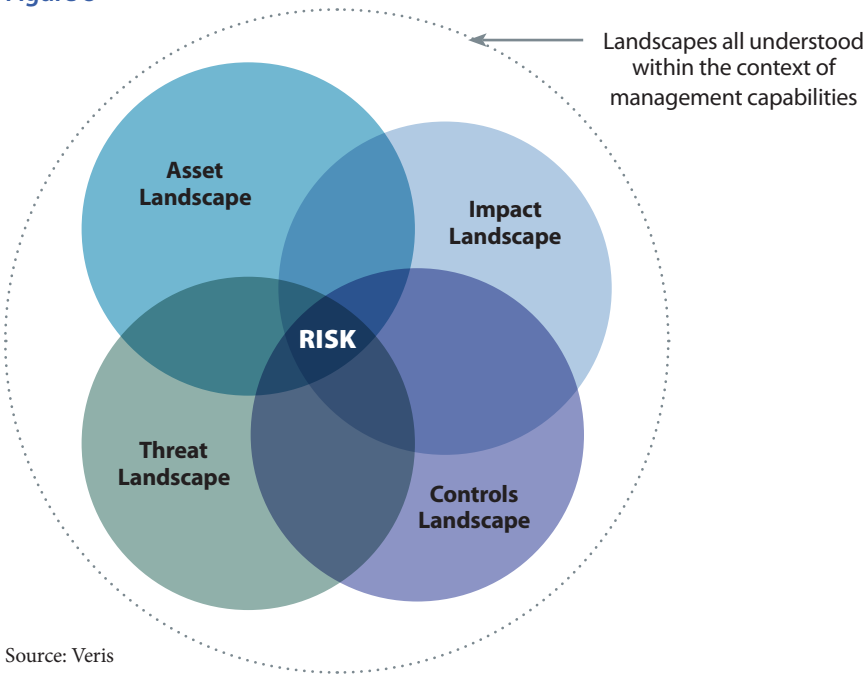
Regardless of the social environment and understanding of cyber insurance, cyber insurers may look to supplement the information obtained via the underwriting process and claims activity with third-party data. Armed with this additional data, insurers may simplify the process of providing cyber insurance, increase their confidence in selling adequate cover, and expand to segments of the market where they previously were unwilling or uncapable to enter using data of their own. Third-party data may include cyber catastrophe models, licensed incident data from risk aggregators, outside-in security scoring vendors, common technology vendor/software aggregation, and threat intelligence data, among others. The pivotal step to making this third-party data useful is gathering and reviewing all available information in a way that makes it easy for insurers to access and cross-reference with their internal data. The essential component is the matching algorithm work done to map the insurer's data to the various third-party data elements.

Insurers may face challenges in collecting data on their own as they are bound by policy and claim systems that may need significant amendments in order to respond to the evolving nature of cyber policies. These policies often require new policy and claims fields to be coded, such as new coverages, attack vectors, assets impacted, etc. Making these IT changes is difficult for companies due to legacy systems and associated high costs and therefore companies may not capture all of the important information that may be valuable for analysis and ratemaking.

Enhanced Data Collection

As insurers in the cyber insurance market look to evolve their understanding and use of data when evaluating cyber risks, third-party vendors and data providers have been working to bridge this gap. There are many vendors available with different products and capabilities. Each insurer can assess its needs, data availability, and the capabilities it requires in reviewing vendors. The following provides an illustration of the work being undertaken in the broader cyber security and cyber insurance industries.

Figure 8



Source: Veris

Which Data Elements Should Be Collected and Why

The management and analysis of cyber data collected is not consistent across the cyber insurance industry. This inconsistency can create issues while evaluating risk since there is no commonly adopted data classification and security rate scoring map. Additional time and energy must be spent standardizing the cyber data collected to analyze trends overtime. Not only are insurers capturing different data, the data they do collect may not be continuous and contextualized. It is crucial to have continuity of assessment of cyber risks.

Data limitations and availability results in significant challenges for cyber insurance underwriters. Examples of ways cyber insurers can overcome some of these challenges include:

- Expand sources and collection of data—ask companies about their endpoints, servers and encryptions; include questions about known previous security threats and breaches, which should be validated by a third party; listing of all the domains of the company as well as their subdomains, certificates, port scanning and all hostnames pointing to IP blocks the company owns. All these are of critical importance to getting a picture of the company's infrastructure. Finally, collecting the publicly available information about the company is important as that is the information that attackers are most likely to exploit first.
- Receive input from a variety of subject matter experts—it is important to engage the corporate information security officer (CISO), IT department, chief financial officer, risk managers, legal department, claims department, and the marketing team.
- Obtain an understanding of the industry and its exposure to cyber—work with companies closely related to the industry you are most familiar with so you can most accurately assess what kind of coverage is necessary.
- Leverage information from third-party cyber information providers—leverage companies providing cyber threat intelligence and aggregation risk data to help create a better-informed cyber risk profile.

Information to inform cyber underwriting and cyber risk is not as scarce as some believe. Technology firms are providing a diverse range of data, including:

- Firmographics—organizational characteristics, such as industry, revenue, and employee count, are extracted from public and private data sources.
- Outside-in scans—sensors on the public space of the internet scan a company's network perimeter to identify their virtual supply chains and monitor security outcomes.
- Inside-out scans—sensors installed in a company's network scan its internal architecture to identify assets, device configuration, access points, and other security aspects.
- Threat monitoring—machines read streams of data from the surface, deep, and dark webs to uncover intelligence on compromised organizations and new vulnerabilities.
- Process and policy—data exchanges, used by organizations to assess compliance with security process and controls, are mined for cyber information.
- Incident data—scraping algorithms compile cyber incident and loss data from governments and other public sources.
- Incident tracking—incident ID, source ID, incident confirmation, incident summary, related incidents, confidence rating, and incident notes.
- Victim demographics—victim ID, primary industry, country of operation, state, number of employees, annual revenue, locations affected, notes, and additional guidance.
- Incident description—actors (external, internal, and partner), actions (malware, hacking, social, misuse, physical, error, and environment), assets (variety, ownership, management, hosting, accessibility, cloud, and notes), and attributes (confidentiality/possession, integrity/authenticity, and availability/utility).
- Discovery & response (incident timeline, discovery method, root causes, corrective actions, targeted vs. opportunistic, and additional guidance).
- Impact assessment (loss categorization, loss estimation, estimation currency, impact rating, and notes).

Sample Cyber Data Websites

The list below includes sample websites that may be accessed to understand cyber incident data and trends in the cyber landscape.[73]:

https://breachlevelindex.com/

https://www.advisenltd.com/data/cyber-loss-data/

http://veriscommunity.net/vcdb.html

https://www.privacyrights.org/data-breaches

https://www.hackmageddon.com/

https://cyber.fsi.stanford.edu/

https://businesslawtoday.org/2018/03/whats-lurking-back-there-cybersecurity-risks-in-legacy-systems/

https://www.sitelock.com/blog/black-box-vs-white-box-part1-dast/

https://www.sitelock.com/blog/tag/white-box-testing/

https://securitytrails.com/blog/improve-cyber-insurance-underwriting

https://www.cyberriskanalytics.com/#features

73 These links are being provided as a convenience and for informational purposes only; they do not constitute an endorsement or an approval by the American Academy of Actuaries of any of the products, services, or opinions of the corporation or organization or individual. The Academy bears no responsibility for the accuracy, legality, or content of the external site or for that of subsequent links. Contact the external site for answers to questions regarding its content.

Cyber Risk Accumulation

Published August 2021

Accumulation risk in insurance, also known as aggregation risk, refers to the likelihood of a greater-than-anticipated accumulation of claim costs due to multiple exposures being tied to the same event or a related event. Our growing digital connectivity and interdependence mean that a single cyber event has the potential to simultaneously impact a significantly large number of businesses around the world.

For example, a rapidly increasing number of companies entrust their data and business operations to cloud services providers. The risk of disruption was realized in November 2020 when Amazon Web Services suffered an outage of undisclosed origin that took down a number of websites and online services.[74] Consequently, a successful cyberattack against a web service provider could translate into widespread business interruptions, or even the permanent loss of valuable data, depending on the severity of the attack. An insurance company or reinsurer exposed to such a cyber event—and an accumulation of claim liabilities—runs the risk of incurring extremely high aggregate portfolio losses.

Modeling accumulation risk is difficult because it can be challenging to identify the full set of dependencies among risks in a portfolio. Furthermore, traditional frequency/severity approaches are considered to be inadequate, or even unreliable, due to the lack of sufficient statistical data for new and emerging insurance lines. This is even more so for cyber insurance as the cyber breach targets and attack methods continuously evolve, and the bad actors continue to adapt and multiply.

Assessing accumulation risks requires transparency about digital supply chains and how commonly used software and systems can create systemic risk potential. Insurance consumers may not always understand their own cyber risk exposure sufficiently well to assemble and disclose the relevant data. And in a highly competitive insurance market, underwriters are often unable to obtain all of the key data points needed for the effective pricing of cyber risks. Fortunately, data such as company usage of information technology (IT) system components and malware propagation rates for devices, servers, and applications have become more available in recent years. While statistical data can be derived from past cyber incidents, historic events may be of limited use because of the rapid development of new threat vectors.[75] A recent example is the significant increase in working from home during the pandemic, which has made protection against cyber breaches more difficult and more complicated.

74 "Amazon Web Services outage causes issues for Roku, Adobe"; *CNBC*; Nov. 25, 2020.
75 Method or way a bad actor can breach or infiltrate an entire network/system. They enable hackers to exploit system vulnerabilities, including the human element.

Even with the availability of some data to model accumulation risk, cyber expertise is needed to piece together the useful data, apply judgment, and extrapolate what a tail event could look like. It is essential to evaluate the variety of commonalities among companies to identify non-obvious paths of aggregation. Cyber experts can help to understand the types of cyberattacks that are technically possible, the consequences of exploiting certain vulnerabilities, the motivations of different threat actor groups, the path a threat vector could take, and the plausibility that an adversary would attack a particular organization through a specific threat vector. Though reliance on cyber experts may be necessary when assessing accumulation risk, underwriters and actuaries would do well to remain abreast of cyber risk developments, including basic IT technology and terminology.

For decades, insurers have modeled accumulation risk from natural catastrophes, and some expect cyber accumulation modeling to mature in a similar manner. While both natural catastrophe and cyber accumulation modeling require blending data with expert opinion—and there can even be natural catastrophes, such as solar flares, that lead to insured cyber losses—cyber risk modeling presents many new challenges. Subject-matter experts strive to stay abreast of developments in the rapidly changing cyber landscape. Systemically important technology vendors can be the source of large-scale business interruption risk to global companies. Cyber damage is harder to quantify than property damage because the duration of a cyber event and reporting lag can vary significantly depending on the specific cyberattack. Sometimes a cyber breach, and the extent of the resulting damage, might not be known for months or more. Further, there is the possibility of underreporting of events as some organizations may be inhibited by the reputational damage from publicizing a significant breach or internal IT system/process failures.

Another distinguishing feature of cyber risks is that cyber catastrophes are typically man-made. An active adversary and motivational aspects of cyberattacks affect which entities are targeted. While people can be evacuated from the expected path of a hurricane to reduce the risk of harm, an active cyber adversary can adapt new tactics to cause damage that are not anticipated. Cyber catastrophic losses are also not isolated in confronting further risks. An earthquake in California may hardly influence expectations for the landfall of a hurricane in Florida, but a major cyberattack may expose new vulnerabilities, leading to further attacks.

To quantify cyber accumulation risk, a simple and conservative approach is to aggregate full insurance policy limits for the entire insurance portfolio. Beyond this, there are two main approaches to model accumulation: deterministic and probabilistic.

Deterministic accumulation modeling

A simple deterministic approach estimates potential losses using a third-party IT service provider's market share. For example, if a hypothetical Technology Provider A has a 20% market share, it can then be assumed that the firm has a roughly similar exposure to the universe of cyber threats. This means that 20% of the client companies in the insurer's well-diversified cyber portfolio would be at risk of experiencing a loss if Technology Provider A has a cyber event.

A more involved approach requires obtaining data on the technology providers (or at a minimum the primary ones) for each company in the insurer's cyber portfolio, taking care to identify those with higher limits. With specific data on which businesses are using which technology providers and other important information, exposures can be linked to aggregation points based on their particular technology providers. This approach can produce more accurate results because it relies on the detailed exposure data of entities in an insurer's portfolio instead of relying on broad industry statistics—but it requires significantly more effort and data to implement.

A possible basis on which to combine the two deterministic approaches would be to consider the mix of industries in one's portfolio and then make a separate assessment of the cyber threat level for each industry.

In both approaches, insurers will need to make deterministic assumptions for a cyber catastrophe scenario in order to assess its insured loss implications. For each cyber catastrophe scenario, estimates would be needed for the number of affected companies, the average costs per affected company, potential claim types triggered, and the available coverage per claim type. The total insured loss can then be calculated for each scenario.

Probabilistic accumulation modeling

In a probabilistic approach, losses are modeled using distributions instead of fixed averages to allow for variations in results. The market share approach can be expanded into a probabilistic model by assuming different technology provider market shares by industry and then creating a distribution of outcomes by repeatedly sampling across various segments of the insurer's portfolio. The process can be repeated for multiple technology providers. Correlation assumptions will be necessary to aggregate the potential losses.

The more complex form of probabilistic modeling is similar to some deterministic approaches, but the estimates made in each step need to be parameterized. The model begins with the creation of a catastrophic scenario narrative. The scenario needs to be realistic, relevant to the insurance market, and have some data available that can be used along with expert opinion to quantify its impacts. Examples of such scenarios include cloud provider outages, denial of service attacks, and mass data breaches. An annual probability of the catastrophic scenario occurring is estimated and assumed. Conditional on the scenario occurring, the next step is to estimate and assume the conditional probabilities of different severities. Finally, given both the annual probability and the severity probabilities, the last step is to determine the insurance cost of the cyber event. Probabilistic models like these have to be continually reviewed and revised based on changes in the cyber environment, including both the technological and legal aspects.

Emerging ideas

Much of the accumulation research to date has focused on an analysis of what potential attack scenarios might be encountered and assessing their likely impact. There are various models to help insurers manage affirmative cyber accumulation, but capabilities for non-affirmative (silent) cyber have been limited. Additionally, there is a gap in understanding the motivations of those behind these attacks. Technological vulnerability alone is not an adequate predictor of cyber risk, though the perennial risk of latent programming errors or compatibility issues cannot be ignored.

The manmade aspect of cyber risk is one of its fundamentally unique characteristics. Many businesses with state-of-the-art technology are breached while others with legacy technology have not been. Organizations with weaker security protocols and older IT operations are more likely to succumb to cyber events (e.g., spear-fishing and ransomware). Yet it is not clear whether they have been specifically targeted or whether they became one of many targets in an attack that was broadcasted widely. In this regard, cyber events could actually be much less random than they seem—in stark contrast to natural catastrophes. Studying the motivation of attackers could aid in looking at the problem.[76] Also, because cyber risks take place in a wide network of computers and systems, they could be modeled using interactive Markov chains or other network modeling techniques.[77]

76 "See No Evil, Hear No Evil? Dissecting the Impact of Online Hacker Forums"; *MIS Quarterly*; 2019.
77 "Pricing of Cyber Insurance Contracts in a Network Model"; *ASTIN Bulletin: The Journal of the IAA*; 2018.

Vendor models

Vendors providing cyber accumulation modeling services can be broadly grouped into two camps: traditional catastrophe insurance modelers expanding into cyber risks, and the typically newer cyber risk service providers moving into insurance. Generally speaking, the natural strengths and weaknesses of each type of vendor have become less pronounced as they are quickly learning from each other.

Many cyber accumulation model vendors were originally IT service providers, and they tend to have more in-house cyber expertise. Where data is sparse, expert judgment becomes increasingly important for assessing the next big emerging risk in the cyber domain, as well as staying on top of the dynamic landscape. Different models provide different degrees and types of flexibility in customizing parameters to reflect different views on cyber risk.

Due to data reporting requirements and data collection methods in the U.S., data may have a bias toward newsworthy, data breach events. Many cyber model vendors partner with others and incorporate multiple other data sources including outside-in scans (gathered from the public space), inside-out scans (gathered from an organization's internal network), threat monitoring (vulnerabilities on the surface, deep and dark webs), and firmographic data (company characteristics such as revenue and employee count).

Many vendors have built their databases though internal efforts and in partnership with others. Some vendors hire teams of "white hat" hackers to map out company networks and direct the types of data captured. Other creative methods include scraping online IT job ad requirements to make inferences about a particular organization's software and systems. The fact remains, however, that many small companies are still not included in these databases, and one may need to adopt a deterministic market share approach as a result. However, the small company databases are growing quickly as more vendors target small businesses in their initiatives.

At the March 2019 Cat Risk Management and Modelling conference held in London, the first public cyber model comparison exercise was completed.[78] Cyber model vendors were each provided with a common portfolio of 46 U.S. companies and a standard cyber insurance policy to model. The results of the models showed significant variation, indicating that the industry has not yet reached a consensus on accumulation modeling assumptions or its approach. As the industry matures, similar comparisons will likely continue to be performed for different cyber accumulation models. Additionally, given data challenges

78 "Cyber Risk Models: Time for a Bench Test"; RMS, April 4, 2019.

and the ongoing evolution of the nature of cyber risk, a vendor's model output may vary significantly from one version of its model to the next.

Accumulation modeling, and cyber risk modeling in general, are very active fields of endeavor and consequently subject to continual redevelopment and improvement. This means that the relative strengths and weaknesses of each vendor's products can be expected to shift and change over time. From an insurance writer's perspective, it may well be the case that no single vendor is able to completely capture cyber accumulation risk with a high degree of confidence. Inevitably, the cost to build and maintain models is a major factor to consider. Because of the difficulties that underlie accumulation risk modeling, managing the exposure may be as important as trying to accurately measure the risk.

Cyber Risk Reinsurance Issues

Published August 2021

Like the primary cyber insurance market, reinsurers are approaching cyber insurance with caution, and many are investing heavily in cyber underwriting capabilities. Nevertheless, confidence in understanding the risk has increased, which has led to an active appetite and expansion of reinsurance capacity in recent years.

For instance, the world's largest reinsurer, Munich Re, has seen growth in premium written for cyber policies from $100 million in 2013 to $400 million in 2018. The current supply of capacity has increased in response to demand for the product, with several reinsurance towers exceeding $500 million. It is estimated that 40% of the global cyber insurance premium written flows to reinsurers,79 compared to 10% to 15% for more mature lines such as property and liability. In addition, the offerings of reinsurers sometimes extend beyond reinsurance capacity into other areas, such as assisting insurers with product development, providing advice on policy wording, and managing accumulation risk.

Despite the progress reinsurers have made over the years, underwriting to a large enough scale remains a key challenge. Underscoring the classic chicken-and-egg problem, insurers find writing cyber insurance difficult without reinsurers, but reinsurers need significant scale before the pooling effects make such reinsurance possible. Many of the challenges impacting primary insurers become more acute for reinsurers, such as lack of data and risk aggregation. Risk quantification is especially challenging for reinsurers due to aggregation potential and silent cyber risk. Enabling the scale necessary for more efficient risk-sharing is a critical element to the development of the overall cyber (re)insurance market where the top 10 carriers of cyber coverage write about half the global premium. Government backstops such as Terrorism Risk Insurance Act of 2002 (TRIA) may provide an avenue to mitigate this scaling challenge for reinsurers (and insurers)—particularly for cyber events with the potential for significant accumulation of losses.

For the many backstop programs across the world, cyber-related losses are either excluded, receive limited coverage (e.g., physical damage only), or the cyber coverage is unclear. The U. S. Department of the Treasury issued a Notice of Guidance on Dec. 27, 2016, which clarified that stand-alone "Cyber Liability" insurance policies are included under TRIA, thus demonstrating the importance of maintaining the program in the face of evolving threats.

79 "Cyber reinsurance in the 'new normal'"; Swiss Re; Oct. 5, 2020.

While the U.S. insurance industry is being pushed to cover acts of cyber terrorism under cyber-specific insurance policies, the case law is still relatively new and has not been tested by a catastrophic cyber terrorism event. Property and general liability coverages would generally still exclude this event and there is not a uniform approach under cyber-specific policies. There also is some question about coverage for widespread secondary events such as business interruption resulting from a terrorist-caused cyberattack on public utilities or internet infrastructure. Further adding to the ambiguity is that such backstop programs are usually designed to respond to terrorism attacks, which may present a challenge for cyber as such attacks are rarely attributed to terrorist organizations openly. More clarity that explicitly addresses the handling of cyber-related losses would help reduce some of the caution in the appetite of reinsurers. TRIA was reauthorized in December 2019 for seven years (expiring December 2027); nevertheless, the insurance industry and Congress has been giving increasing attention to better understanding the concerns around the handling of cyber risk. In a letter to the U.S. Government Accountability Office, the Cyber Risk Task Force of the American Academy of Actuaries shared its views on how TRIA would apply in the case of large-scale cyberattack against U.S. businesses[80]. Whether it would be best to continue extending the program in its current form or create a new program specifically designed to address these questions around the treatment of cyber perils should be part of future discussions. In several other countries, these programs are also being examined to assess the coverage being provided for cyber-related losses. For example, reinsurance for terrorism incidents provided by Pool Re, Britain's leading terrorism reinsurer, has been expanded to cover physical damage from cyber-terrorism.

Alternative risk transfer provides another avenue for reinsurance capacity, namely through insurance linked securities (ILS). The underlying complexity of cyber risk and the lack of relevant experience compared to natural catastrophes could potentially be deterrents for alternative capital providers; however, significant natural catastrophe losses in recent years has put pressure on the ILS market to improve investor returns. As a result, the ILS market is expected to be more selective with the risks it takes on in the short term. Wildfire, flood, and terrorism risks have been transferred to the capital markets successfully and so more activity is expected around cyber risk. However, in addition to the usual challenges posed by cyber risk to the traditional markets, there is a high potential for a triggering event to have an impact on bond and equity markets and therefore reduce the diversification benefits that have attracted investors to ILS covering property risks. While models are improving, data challenges contribute to not very sophisticated cyber risk models, which is also a big hurdle in transferring cyber risk to the ILS market.

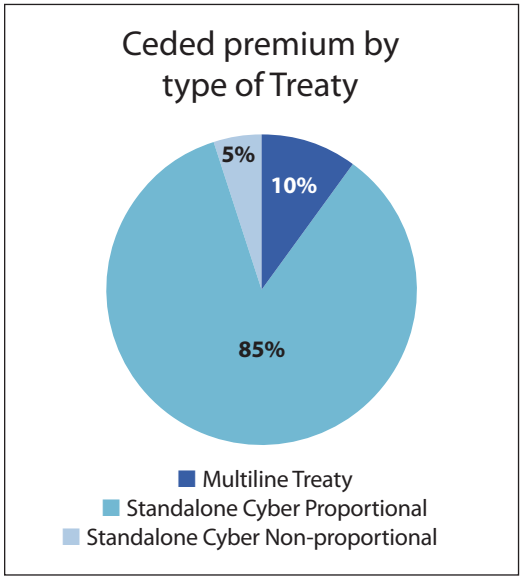
80 Academy Comments to GAO on Cyberattacks and TRIA.

A natural choice to structure a cyber risk in the ILS sector would be to follow the existing catastrophe-bond structure. One problem with this structure is that it requires upfront funding from investors, which may be a deterrent given the number of unknowns perceived to be associated with cyber risks. A potential solution to this problem could be the use of contingent capital. In this arrangement, investors would effectively promise to pay out the full amount when the structure is triggered. The drawback to this arrangement is the increased credit risk, underscoring the point that there are no easy solutions to the problem.

Availability of an industry-loss index could also be helpful in the effective retrocession of cyber risks to the ILS and reinsurance market. Such an index can be used to set up industry loss warranty arrangements (ILWs) for cyber risks. In such arrangements, loss trigger and payout after an event are typically based on the total industry losses, and in some cases the buyer's own losses too. PCS Global Cyber is one such index provided by Property Claim Services.[81] The ASTIN (Actuarial Studies In Non-life insurance) working party is also researching to provide a cyber risk index.[82]

Traditional risk transfer is currently provided primarily through standalone cyber treaties, with quota share treaties making up the vast majority.

Figure 9



Source: Swiss Re data

81 "Loss Aggregation for Cyber Events"; Verisk; 2021.
82 "ASTIN Working Party on Economic Cyber Loss Index for Parametric Covers—A Proof of Concept Study"; International Actuaries Association; May 2019.

Reinsurers have gravitated mostly to proportional (quota share) treaties due to their ability to alleviate capital requirements. In addition, proportional treaties help to fund the significant investment required to build a robust underwriting process for cyber insurance through commissions. Although proportional treaties are still the norm, non-proportional covers such as aggregate excess of loss treaties have seen increased demand due to their ability to provide balance sheet protection for insurers by ceding catastrophe risks. Aggregate excess of loss covers typically to attach at loss ratios between 90% to 200%.

Primary insurers and reinsurers have finite capital available for managing cyber risk. If reinsurers retrocede some of the cyber risk to the ILS market, additional capital could absorb a portion of the cyber risk. Further growth in the cyber market may require more innovation to attract market participants from the securities market. One such innovation could be to structure the program that allows lower barrier of entry for sponsors/cedants seeking protection from the capital market. This will enable more participants to enter the ILS market. Innovation could also be done by the modeling firms to enhance their cyber risk models. That will increase confidence of institutional investors, leading to further demand of cyber ILS instruments.

Ransomware

Published August 2021

Cybercrime is expected to keep growing as businesses increasingly rely on remote workers and the internet of things (IOT) continues to expand. One type of cybercrime that is rapidly increasing is ransomware attacks. According to insurance industry experts, ransomware has become the biggest cyber threat facing businesses over the past two years.[83]

Ransomware has many consequential effects from temporary or permanent loss of data and complete shutdown of operations, to making some hardware inoperable. The victim is then instructed to pay a ransom, generally in bitcoin, with a promise of reversing the malware damage (restoring access to systems or data, etc.).

The earliest example of ransomware is PC Cyborg, which was spread by infected floppy disks in 1991.[84] Now there are many ways ransomware might victimize potential targets—email, downloads, malicious online advertisements, cloud storage, and others.

Ransomware victims face choosing between paying the ransom or investing the cost and time in repairing the infected system. After a 2016 ransomware attack on San Francisco's Municipal Transportation Agency (SFMTA), the agency chose not to pay the ransom and relied on backup systems to restore affected computers. Ticket machines and faregates were turned off for three days in order not to inconvenience passengers.[85] The city of Atlanta during a ransomware attack in 2018 chose not to pay a ransom demand of $50,000 in bitcoin and spent more than $7 million on recovery costs as of June 2019.[86]

83 "Frequency of Cyber Events Targeting Businesses Increasing: Travelers"; MyNewMarkets powered by *Insurance Journal*; Dec. 11, 2020.
84 "Ransomware: Reinsurance Association of America"; 2021.
85 SFMTA Blog, Nov. 28, 2016.
86 "Don't Pay Cyber Ransoms, Officials Warn"; *WSJ Pro*; Feb. 12, 2020.

To pay or not to pay?

As shown in the table below, some ransomware victims ended up paying considerably more than the ransom demand to restore their systems.

Table 1

Entity	Ransomware-Demand	Ransomware-Paid (Y/N)	Cost to Repair If N
Atlanta, Georgia	$50,000	N	$7,000,000[4]
Baltimore, Maryland	80,000	N	18,000,000[87]
Newark, New Jersey	30,000[5]	Y	
U.S. County infected by Ryuk	132,000[6]	Y	
U.S. City infected by Robbinhood	76,000	N	9,000,000[6]
U.S. County infected by Ryuk	1,200,000	N	1,000,000[88]

There are several reasons advocated by the Federal Bureau of Investigation (FBI) not to pay the ransom demand:

- Emboldens adversaries to target additional organizations
- Encourages criminals to use ransomware to fund illicit activities
- Does not guarantee files will be recovered[89]

Does paying ransom increase risk of getting another attack?

One concern with paying a ransom is that the targeted organization/entity will be marked as a receptive target for future ransomware attacks. However, while larger organizations may receive targeted attacks (such as "big game ransomware"), smaller organizations are more likely to be caught in a mass scanning approach wherein hackers cast a wide net for victims by exploiting a specific weakness in cyber systems. Hence, an organization's size may be a consideration in whether or not to pay a ransom.

87 "What Cities Can Learn from Atlanta's Cyber Attack"; *Bloomberg*; Oct. 29, 2019.
88 "Ransomware, What It Is & What To Do About It"; National Cyber Investigative Joint Task Force.
89 Ibid.

Others disagree that the risk of getting attacked increases after paying ransom. According to international insurance brokerage and risk adviser company Marsh, victims are rarely "targeted"—instead, attackers select a specific vulnerability to exploit and use the vulnerability as a wide net to try and bring in as many victims as possible.[90] Similar comments were made during a webinar by Advisen.[91] On the other hand, the attack-and-penetration landscape changes continuously and in new directions and new ways.

Where is the ransom money going?

In late 2020, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) issued an advisory regarding the risk of sanctions associated with ransomware payments. If the victim chooses to pay the ransom and the ransomware payment goes to an individual or entity on OFAC's Specially Designated Nationals and Blocked Persons List, OFAC may impose civil penalties on the ransomware victim.[92] This is challenging as generally a criminal's identity and associations are not known.

Does paying the ransom work?

It is estimated that recovery keys are only effective 20% to 50% of the time and there still are rebuilding costs.[93] According to one ransomware specialty firm, ransom paid to delete stolen data is not always successful. Victims have been re-extorted weeks later, or data has been leaked after ransom was paid.[94]

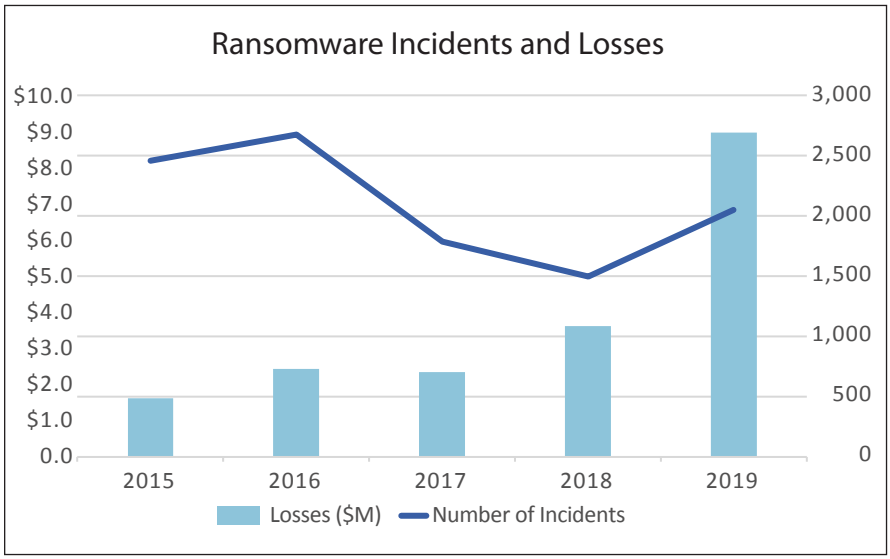
90 "Cyber Insurance is Supporting the Fight Against Ransomware"; Marsh JLT Specialty; October 2019.
91 "Advisen Quarterly Cyber Risk Trends: 2020 Wrap-Up Webinar"; Feb. 3, 2020.
92 Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments; U.S. Department of the Treasury; Oct. 1, 2020.
93 "Don't Pay Cyber Ransoms, Officials Warn"; op. cit.
94 "Ransomware Demands Continue to Rise"; CoveWare blog; Nov. 4, 2020.

Insurance industry outlook

Insurance companies must respond to the increasing frequency and severity of ransomware attacks. The FBI's Internet Crime Complaint Center (IC3) reported 1,493 victims with $3.6 million in loss for 2018 and 2,047 complaints with adjusted losses over $8.9 million for 2019.[95] Coalition reports there was a decrease in the frequency of ransomware from 2019 to the first half of 2020 but there has been a 47% increase in severity from first quarter 2020 to second quarter 2020.[96] Lloyds of London insurer Beazley PLC reported that the total costs of ransom payments doubled year on year through June 30, 2020.[97]

The following graph shows the number and cost of ransomware attacks reported to the IC3 in the years 2015 through 2019. While the number of ransomware incidents actually decreased from 2015 through 2018, the cost of such incidents has trended upward with a noticeable jump in 2019.[98] There are cyber industry reports that the average ransom increased 33% from the fourth quarter of 2019 to the first quarter in 2020 as large enterprises were targeted.[99]

Figure 10



95 FBI Internet Crime Reports for 2018 and 2019.
96 Cyber Insurance Claims Report H1 2020; Coalition Inc.; page 8.
97 "Ransomware attacks on the rise even as cyber insurers scale back"; *Reuters*; Dec. 16, 2020.
98 Graph values from FBI Internet Crime Reports for 2019 and prior years.
99 "Ransomware Payments Up 33% as Maze and Sodinokibi Proliferate in Q1 2020"; CoveWare blog; April 29, 2020.

As concerning as these trends are, costs may be underreported. The IC3 ransomware costs data do not include estimates of lost business, time, wages, files, equipment, or any third-party remediation services acquired by a victim and only includes what victims report to the FBI via the IC3.[100] Company culture can determine what cybercrimes are reported. A company may underreport, or not report at all given concerns with potential reputational risk. Current OFAC guidance may deter reporting if the company decides to pay a ransom due to potential civil penalties.

Moody's Investors Services Inc. reports that the surge in ransomware is increasing cyber insurance prices, reducing limits and raising attachment points.[101] Another industry report indicates that cyber insurance prices were expected to increase 20%-50% in 2021.[102] Insurance companies offering ransomware coverage may require that the insured make "every reasonable effort" not to reveal that they have this coverage.[103] Another way to limit costs is to require pre-approval before paying any ransom.[104] While insurance policies may not directly pay a ransom, some policies will reimburse insureds that choose to do so.

Conclusion

Ransomware is not going away anytime soon. Understanding the basics of ransomware is the first step in equipping companies and insurers to underwrite, price, and manage this cyber risk effectively. Insurers can consider providing guidance to their policyholders to help prevent attacks as well as how to respond after an attack.

100 *Internet Crime Report*; FBI; 2018 (page 20).
101 "Cyber insurance prices increase on ransomware claims: Moody's"; *Business Insurance*, Feb. 5, 2021.
102 "Cyber insurance rates to increase 20-50% this year: Aon"; *Business Insurance*, March 4, 2021.
103 Insurance company rate filing.
104 Insurance company rate filing.

War, Cyberterrorism, and Cyber Insurance

Published February 2022

As cyber insurance coverage continues to evolve and grow in application, an increasing concern among policyholders is whether policies will cover them when cyber incidents impacting them are tied to cyber and technology disruptions stemming from attacks that may be supported by nation-states. In particular, malicious actors might be tied to a given political or ideological affiliation and are sometimes—either directly or indirectly—associated with nation-states and state-backed military units. While cyber insurance has paid claims from attacks attributed to nation-states, policy clauses and endorsements (i.e., riders) within cyber insurance such as the War Exclusion and Cyberterrorism endorsements create uncertainty over whether the policy will respond to certain attacks in the future.

The purpose of this section is to provide a general overview of the War Exclusion and Cyberterrorism endorsements within cyber insurance policies along with the nuances associated with attributing attacks to nation-states and malicious actors.

What Is the War Exclusion Within Cyber Insurance?

Most, if not all, cyber insurance policies include an explicit exclusion to losses arising out of or attributable to war and military actions, which are also present in most other types of property and casualty insurance policies. Various cyber insurance policies were reviewed and analyzed for this issue brief. The examples shown below from American International Group, Inc. (AIG) and AXIS Insurance were selected as illustrative from the policies reviewed. The policy forms referenced herein were obtained via the National Association of Insurance Commissioners' (NAIC) System for Electronic Rates & Forms Filing (SERFF) Access. Please note that the American Academy of Actuaries does not endorse these two insurance companies over other insurance companies but is using them as a representation of the inherent language utilized within cyber insurance policies.

The following is an example War Exclusion from an AIG cyber insurance policy, specifically its Specialty Risk Protector® CyberEdge℠ Security Failure/Privacy Event Management Insurance policy 101018 (12/13). For simplicity, the focus here is on the agreements within this specific coverage section, but there are other coverage sections with regard to Network Interruption and Cyber Extortion among others. The general exclusions are similar across the different coverage sections. Please note that this is a specific form and different insurance company cyber insurance policy forms vary from one another.

3. *Exclusions*

   The insurer shall not be liable to make any payment for Loss:

   (e) arising out of, based upon or attributable to any war, invasion, military action (whether war is declared or not), civil war, mutiny, popular or military uprising, insurrection, rebellion, revolution, military or usurped power, or any action taken to hinder or defend against any of these events

As written, this War Exclusion is quite broad, and cyber-attacks stemming from military units within a nation-state have the potential to fall under this exclusion within the cyber insurance policy. In the following section, endorsements to the cyber policy that provide changes to the War Exclusion will be discussed as well as an introduction to additional terminology to better clarify the intent of the cyber policy. The policy endorsements provide some clarity, but ambiguity may still exist and may create uncertainty for policy issuers, policyholders, and regulators.

While the United States has been involved in recent military engagements and armed conflicts such as the "First Libyan Civil War,"[105] the Iraq War,[106] and the "War on Terror,"[107] it is important to note that there have only been five formally declared wars by Congress, the most recent being World War II.[108] Further, there has yet to be a certified act of terrorism for reimbursement under the Terrorism Risk Insurance Act (TRIA). The current TRIA law implements the Terrorism Risk Insurance Program, effective December 20, 2019, which reauthorized TRIA, originally passed in the aftermath of the terrorism attacks of Sept. 11, 2001.[109] While certain acts may be called "terrorism," only those that are deemed a "certified act of terrorism" by the secretary of the Treasury as defined by the law are eligible for coverage under TRIA.[110] Regarding war and TRIA, acts are not to be certified by the secretary if the acts are committed as part of the course of a war declared by the Congress.[111]

105 "Resolution 1973 (2011)"; UN Security Council; March 17, 2011.
106 "Authorization for Use of Military Force Against Iraq Resolution of 2002"; 107th Congress; Oct. 16, 2002.
107 "Authorization for Use of Military Force"; 107th Congress; Sept. 18, 2001.
108 "About Declarations of War by Congress"; U.S. Senate website.
109 "Terrorism Risk Insurance Program"; U.S. Department of the Treasury website.
110 "Certified Act of Terrorism"; IRMI Glossary; 2022.
111 *Title I of the Terrorism Risk Insurance Act of 2002—Terrorism Risk Insurance Program*; U.S. Department of the Treasury; 2005.

The Treasury Department provided guidance in 2016 that TRIA applies to stand-alone cyber insurance policies.[112] However, many organizations utilize their Technology Errors & Omissions and Professional Liability insurance policies to protect themselves from cyber incidents. That same guidance from the Treasury Department explicitly states that "Professional Errors and Omissions Liability Insurance" is excluded from the TRIA program. Hence, many organizations and their corresponding insurers are precluded from protection under the TRIA program to the extent that their insurance protection from cyber incidents is derived from a Professional Errors and Omissions Liability insurance policy. The American Academy of Actuaries Cyber Risk Task Force provided commentary to the U.S. Government Accountability Office[113] in June 2020 and the Department of the Treasury[114] in January 2021 in response to request for comments.

Endorsements to the War Exclusion and Defining Cyberterrorism

Given the War Exclusion above, how do policies respond to various cyber incidents when those incidents are tied to nation-states? The circumstances lie within an endorsement to the War Exclusion as well as an endorsement that introduces a new term—Cyberterrorism. In general, the War Exclusion and Cyberterrorism endorsement works as follows:

1. The definition of the War Exclusion is amended such that it does not apply to acts of Cyberterrorism.
2. The coverage sections are amended such that acts of Cyberterrorism are included within the coverage.
3. The term Cyberterrorism is defined accordingly.

Below are two examples regarding how policies are amended to provide coverage for Cyberterrorism.

Going back to the AIG cyber insurance illustration from its Specialty Risk Protector® CyberEdge℠ Security Failure/Privacy Event Management Insurance policy 132711 (05/19), two endorsements to the cyber policy are as follows:

112 "Guidance Concerning Stand-Alone Cyber Liability Insurance Policies Under the Terrorism Risk Insurance Program"; Federal Register; Dec. 27, 2016.
113 "Re: Cyberattack and the Terrorism Risk Insurance Program"; American Academy of Actuaries; June 1, 2020.
114 "Re: 2019 TRIA Reauthorization Proposed Rules Comments"; American Academy of Actuaries; Jan. 7, 2021.

AIG Endorsement Example #1

1. *The insurer shall not be liable to make any payment for Loss:*
   (2) war (whether war is declared or not), invasion, use of military force, civil war, popular or military uprising, rebellion, revolution, or any action taken to hinder or defend against any of these events

AIG Endorsement Example #2

2. *"Security Failure" also includes any failure or violation resulting from* ***Cyberterrorism****.*

AIG Endorsement #1 reads very similar to the original exclusion. While the War Exclusion remains, there is now have coverage from Cyberterrorism, but what does that term mean? A third endorsement to the cyber policy defines Cyberterrorism as follows:

AIG Endorsement Example #3

For the purposes of this endorsement, ***"Cyberterrorism"*** *means the premeditated use of disruptive activities against any computer system or network by an individual or group of individuals, or the explicit threat by an individual or group of individuals to use such activities, with the intention to cause harm, further social, ideological, religious, political or similar objectives, or to intimidate any person(s) in furtherance of such objectives. "****Cyberterrorism****" does not include any such activities which are part of or in support of any war or use of military force.*

In another example from AXIS, policy form AXIS PRO® TECHNET SOLUTIONS TM TECHNOLOGY PROFESSIONAL SERVICES LIABILITY AXIS 1010001 0117, the War Exclusion is stated as follows:

EXCLUSIONS

This policy does not provide coverage for ***Claims****, or coverage for any amounts:*

War

based upon or arising out of war, invasion, hostilities or warlike operations (whether war is declared or not), strike, lock-out, riot, civil war, rebellion, revolution, insurrection, civil commotion assuming the proportions of or amounting to an uprising, military or usurped power, or the confiscation, nationalization or destruction of, or damage to, property under the order of government or other public authority.

The following endorsements are then added to the AXIS policy via 1011688 0518 to provide coverage for acts of Cyber Terrorism as defined by AXIS.

AXIS Endorsement Example #1

Cyber Terrorism Coverage Endorsement Definition

It is agreed that:

1. The following new definition is added to the policy:
   Cyber Terrorism *means an act or series of acts of any person or group of persons, whether acting alone or on behalf of or in connection with any entity committed for political, religious or ideological purposes and directed towards the destruction, disruption or subversion of communication and information systems, infrastructure, computers, the internet, telecommunications or electronic networks or the contents thereof or sabotage or threat there from. This shall include, but is not limited to, the intention to influence any government and/or to put the public in fear for such purposes.*

Axis Endorsement Example #2

2. The War exclusion, if any, is amended to add the following at the end thereof:
   Notwithstanding the foregoing, this exclusion does not apply to acts of ***Cyber Terrorism****.*

In both of these examples, coverage under the policy is provided for acts associated with cyberterrorism. However, acts associated with war or military force are not covered under the policy. The confusion and significant gray area associated with these endorsements and carve-back provisions come into play when analyzing attribution along with the intent and individuals behind the attack.

The last sentence of the AIG definition of Cyberterrorism says that it does not include *any such activities which are part of or in support of any war or use of military force.* Questions arise as to how the coverage would respond if a foreign government's military force was directly tied to an attack. Would an insurance carrier deny the claim, stating that the attack fell outside the scope of the Cyberterrorism clause? In other lines of business, for example property insurance, War Exclusions have been invoked with denial of coverage related to cyber incidents as experienced with the *Mondelez International, Inc. v, Zurich American Insurance Company 2018 WL 4941760 (Ill.Cir.Ct.)*, No. 2018L011008, property insurance case related to the NotPetya cyberattack. In contrast, there has yet to be a publicly known denial of a cyber incident corresponding to the War Exclusion under a cyber insurance policy. This is an important distinction as it means that cyber insurance policies might be continuing to pay claims even as private organizations are targeted by nation-state actors.

Next, some key examples of known cyberattacks and issues underlying attribution to different parties will be addressed.

Nation-state Attacks, Criminal Groups, and Attribution

When analyzing the endorsements and clauses above, the attribution (who was behind the attack) and the reasoning for the cyber-attack comes into play because a War Exclusion would require the identification of the party(s) who caused the incident. Under the War Exclusion, war does not have to be declared, and the Cyberterrorism definitions do not explicitly incorporate military action. To the extent that an attack is related to a nation-state's military unit—such as has been charged against the Russian military in the NotPetya attack[115] or the Russian General Staff Main Intelligence Directorate's (GRU) Main Center for Special Technologies (GTsST, also known as Unit 74455 and Sandworm) with the cyber-attacks against the Republic of Georgia[116]—there may be reasoning for the cyber insurance policy to deny coverage due to lack of coverage under the definition of cyberterrorism or the War Exclusion.

Further, when analyzing the groups behind an attack, nations and private threat intelligence teams may not always delineate between hacking groups and specific nation-states. While it is generally believed that the DarkSide and REvil hacking groups operate out of Russia, there has been no specific or direct connection between these hacking groups and the Russian government.[117,118] To the extent that a nation-state provides directives to these hacking groups to carry out certain attacks, there is a further gray area over whether the attribution of the attack is tied to the nation-state or the specific hacking group that may be simply carrying out orders from government leaders. As such, attribution of attacks is very difficult to achieve and is often not completed in a timely manner because it may take months or years to fully understand the scope of the attack.

Underwriters and actuaries are carefully analyzing the risks and footprints associated with the organizations that are being underwritten. The NotPetya incident in June 2017 is a prime example as many of the Western country-based entities impacted by the NotPetya attack were indirect targets of the attack. As the Russian military attacked organizations based in Ukraine, many Western-based organizations such as Merck, FedEx, Maersk, and Mondelez among others were impacted by the attack due to their operations in Ukraine.[119] Given that companies may be collateral damage to conflicts between nations, insurers need to determine whether the intent of the cyber insurance policy is to cover cyber incidents related to these conflicts as well as adjust pricing on cyber premiums to account for an organization's global footprint.

115 "Statement from the Press Secretary"; WhiteHouse.gov; Feb. 15, 2018.
116 "United States Condemnation of Russian Cyber-Attack on Georgia"; U.S. Mission to the OSCE; Feb. 27, 2020.
117 "DarkSide Ransomware Gang: An Overview"; Palo Alto Networks; May 12, 2021.
118 "Press Briefing by Press Secretary Jen Psaki, July 6, 2021"; WhiteHouse.gov; July 6, 2021.
119 "One Year After NotPetya Cyberattack, Firms Wrestle With Recovery Costs"; Wall Street Journal; June 27, 2018.

Table 1 shows a sampling of notable cyber incidents in which there has been public attribution surrounding the attacks. For the purpose of this issue brief, most of the examples in the sampling are related to incidents attributable to nation-states and their corresponding military units.

Table 2: Sampling of Cyber Incidents With Public Attribution

Incident	Approximate Attack Date / Disclosure	Approximate Attribution Date	Alleged Attacker	Attributed By
Sands Casino[120, 121]	02/11/2014	09/10/2015	Iran	United States
Sony Pictures Entertainment[122]	11/24/2014	12/19/2014	North Korea	United States
Office of Personnel Management Breach[123, 124]	06/05/2015	09/21/2018	China	United States
Wannacry[125]	05/12/2017	12/19/2017	North Korea	United States, United Kingdom, Australia, Canada, New Zealand, and Japan
Equifax Breach[126]	05/13/2017	02/10/2020	Chinese PLA	United States
NotPetya[127,128]	06/27/2017	02/14/2018	Russian military	United States,
United Kingdom, etc.				
Russian Cyber-Attack on Georgia[129,130]	10/28/2019	02/27/2020	Russian GRU	United States,
United Kingdom, etc.				
Solar Winds' Orion[131,132]	12/14/2020	01/05/2021	Russia SVR	United States
Microsoft Exchange Server Attack[133,134]	03/02/2021	07/19/2021	Chinese MSS	United States, United Kingdom, EU, NATO
Colonial Pipeline Attack[135,136]	05/07/2021	05/10/2021	DarkSide	United States
JBS Attack[137,138]	05/31/2021	06/02/2021	REvil (aka Sodinokibi)	United States
Kaseya Attack[139]	07/02/2021	07/04/2021	REvil	Self-acknowledged by REvil

120 "Worldwide Cyber Threats"; House Permanent Select Committee on Intelligence—Statement for the Record; Sept. 10, 2015.
121 "Las Vegas Sands—2014 10-K"; SEC.gov.
122 "Update on Sony Investigation"; Federal Bureau of Investigation; Dec. 19, 2014.
123 "Bolton Confirms China was Behind OPM Data Breaches"; *FedSmith*; Sept. 21, 2018.
124 "U.S. Suspects Hackers in China Breached About 4 Million People's Records, Officials Say"; Wall Street Journal; June 5, 2015.
125 "Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea"; WhiteHouse.gov; Dec. 19, 2017.
126 "Chinese Military Personnel Charged with Computer Fraud, Economic Espionage and Wire Fraud for Hacking into Credit Reporting Agency Equifax"; U.S. Department of Justice; Feb. 10, 2020.
127 "Statement from the Press Secretary"; WhiteHouse.gov; Feb. 15, 2018.
128 "Foreign Office Minister condemns Russia for NotPetya attacks"; Gov.uk; Feb. 15, 2018.
129 "United States Condemnation of Russian Cyber-Attack on Georgia"; Op. cit.
130 "UK condemns Russia's GRU over Georgia cyber-attacks"; Gov.uk; Feb. 20, 2020.
131 "Joint Statement by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Office of the Director of National Intelligence (ODNI), and the National Security Agency (NSA)"; Cybersecurity and Infrastructure Security Agency; Jan. 5, 2021.
132 "FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government"; WhiteHouse.gov; April 15, 2021.
133 "HAFNIUM targeting Exchange Servers with 0-day exploits"; Microsoft; Marc 2, 2021.
134 "The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China"; WhiteHouse.gov; July 19, 2021.
135 "FBI Statement on Compromise of Colonial Pipeline Networks"; Federal Bureau of Investigation; May 10, 2021.
136 "FBI Statement on Network Disruption at Colonial Pipeline"; Federal Bureau of Investigation; May 9, 2021.
137 "JBS USA Cyberattack Media Statement—May 31"; JBS Foods; May 31, 2021.
138 "FBI Statement on JBS Cyberattack"; Federal Bureau of Investigation; June 2, 2021.
139 "REvil gang asks for $70 million to decrypt systems locked in Kaseya attack"; *The Record*; July 4, 2021.

While the time to achieve public attribution associated with significant cyberattacks from governments has been decreasing—as seen with the Solar Winds' Orion, Colonial Pipeline, and JBS cyberattacks—Wannacry and NotPetya each took months of investigation before public attribution from the United States and United Kingdom. In that timeframe, cyber claims may have been paid out, but the insurer may have wanted to or still want to invoke exclusions or deny the claim as a result of the findings from the public attribution. Additionally, the choice to invoke such exclusions creates uncertainty in the courts when it comes to whose evidence and definitions will be the primary evidence around the attribution. The incidents in Table 2 are examples with press releases and quotes from government officials, but there is very little information provided as to how those conclusions were arrived at.

Actuaries and the War Exclusion / Cyberterrorism

These coverage clauses and endorsements will be increasingly important for all stakeholders and for actuaries practicing in the cyber insurance space as the impact of potential systemic, war-related, and military-related cyber incidents will influence both the pricing and reserving of losses falling under cyber policies. When these unique events cross the line from cyberterrorism to acts of war and invoke exclusions under the policies, they will likely be litigated in the courts, as is the case in the *Mondelez International, Inc. v. Zurich American Insurance Company* property insurance suit. The uncertainty around payouts associated with these litigated coverage cases will add complexity to the overall reserving process. Further, actuaries would do well to have a clear understanding of the types of cyber event scenarios to exclude from their pricing analyses if the cyber incidents are outside of the purview of the written cyber policy based on the policy wording.

Over time, greater clarity from the cyber insurance industry around the ambiguities noted above is essential. In the interim, it is important that actuaries working in the cyber insurance space be aware of the nuances and uncertainties created by these coverage conditions and the nature of cyber incidents.

Autonomous Vehicles and Cyber Risk

Published June 2022

Summary

The line between cyber and auto insurance is blurring as sophisticated and often internet-connected autonomous vehicles (AV) become more prevalent. This section discusses the growth of AVs, their benefits, and their cyber risks, in addition to legislation and current regulations overseeing cyber insurance.

Introduction

According to one industry projection, the global market for automated vehicles is expected to grow[140] from 0.1% of vehicle registration share in 2021 to 12% or approximately 101 million units in 2030.

The global autonomous commercial vehicle market is expected to grow from $5.59 billion in 2020 to $7.07 billion in 2021 at a compound annual growth rate (CAGR) of 26.5%. The market is expected to reach $13.41 billion in 2025 at a CAGR of 17%.[141]

Major players in the autonomous commercial vehicle market include Volkswagen, Daimler AG, Tesla, Denso, Continental, Waymo, BMW AG, Isuzu Motors Limited, General Motors, and AB Volvo.

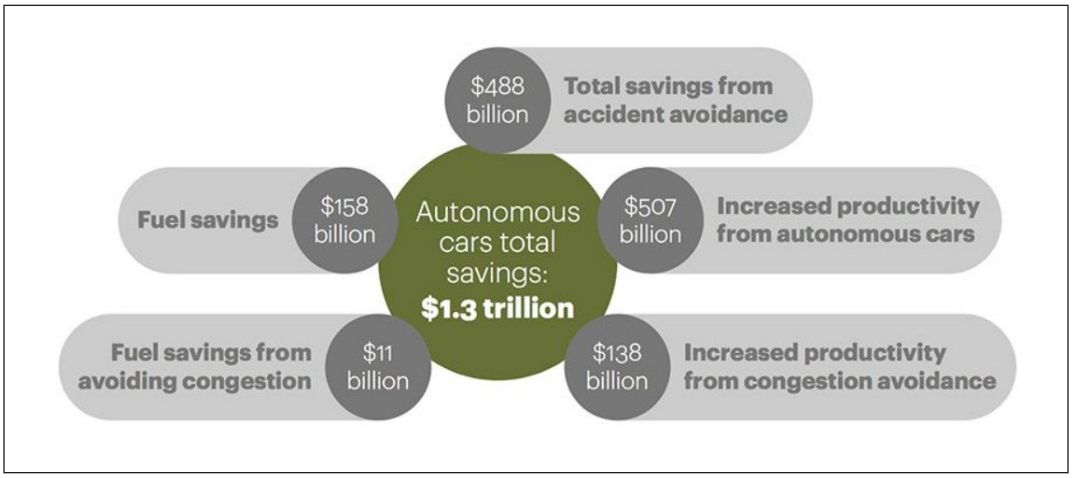
Benefits of Autonomous Vehicles

One industry survey, *The Road to Autonomous Vehicles—2018*,[142] found that 7 in 10 Americans (70 percent) believe autonomous vehicles will routinely navigate the nation's streets and highways within 15 years.

140 "Projected autonomous vehicle registration share worldwide between 2021 and 2030"; Statista; Aug. 5, 2021.
141 "Autonomous Commercial Vehicle Global Market Report 2021: Breakdown by Driver Assistance, Partial Automation, Conditional Automation, High Automation, Full Automation"; ResearchAndMarkets.com; Aug. 26, 2021.
142 "Americans Expect Self-Driving Vehicles to be Commonplace within 15 Years"; *ITS Digest*; June 4, 2018.

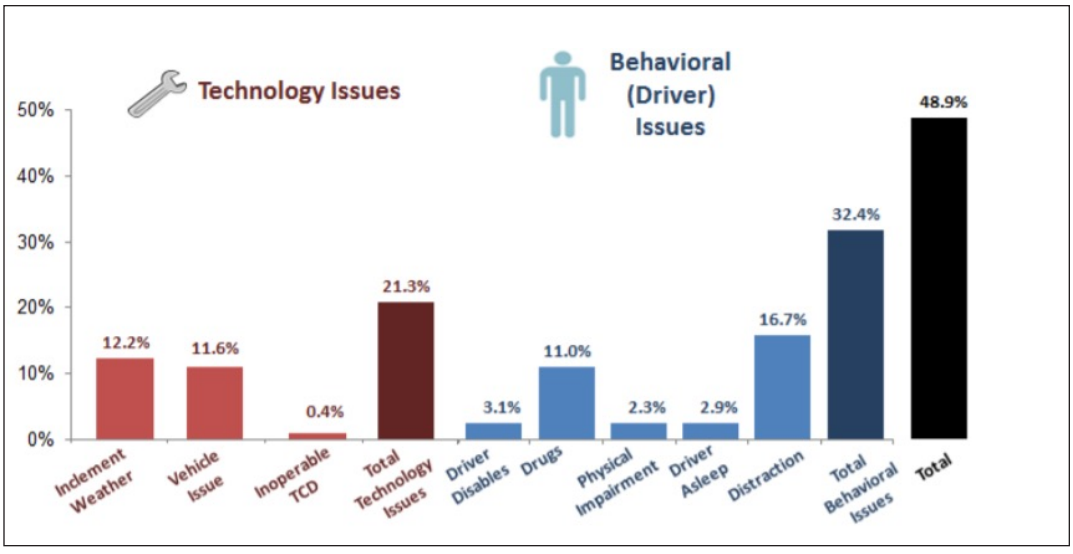
According to another industry study,[143] the growth of AVs could represent a $1.3 trillion boost to the U.S. economy. For comparison, the U.S. nominal GDP in 2021 was $20.5 trillion.[144]

Figure 11



In 2018, the Casualty Actuarial Society's Automated Vehicles Task Force published a paper[145] that presented an illustration of driver behavior as being the largest contributor to accidents, followed by technology issues (when extrapolated):

Figure 12



143 "US autonomous vehicle market could hit $560 billion by 2035"; Consulting.us.; July 25, 2019.
144 "GDP Ranked by Country 2022"; World Population Review; 2022.
145 Automated Vehicles and the Insurance Industry; Casualty Actuarial Society; 2018.

Based on this information, by eliminating the driver from the equation, autonomous cars can be expected to be safer, as the increase in potential technology issues is far outweighed by the removal of the behavioral issues.

This would in turn be expected to shift the liability from individual drivers to the vehicle manufacturers. The same paper calculates the insurance premium impact of this shift with assumptions, such as:

- Every vehicle is fully autonomous.
- Every vehicle is fully owned by the manufacturer.
- $1 million policy limits.
- Frequency remains the same.

The paper projects that the average premium would double or triple, caused mostly by dramatically increasing the coverage of each vehicle. However, the frequency is expected to decrease. Under different scenarios, the paper calculates a frequency reduction slightly above 50% is going to cause average premiums to decrease instead.

Some expect the biggest benefit of AV for long-haul trucks is doubling the asset utilization by eliminating the need for mandated truck stops. A second benefit is mitigating the shortage of drivers available, which has historically been the highest-cost line item in the industry.[146]

Cyber Risks in Autonomous Vehicles

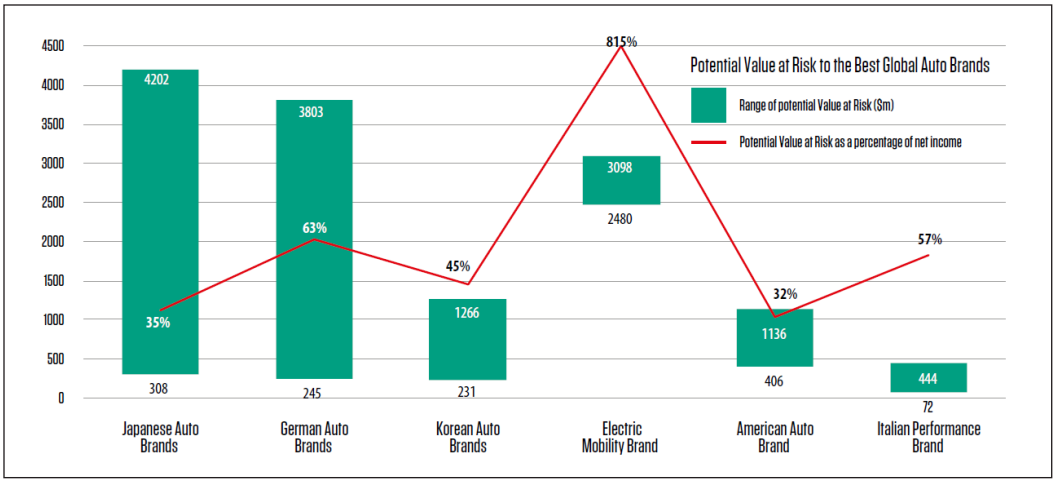
The integration of motor vehicles with electronic systems slowly turns them into connected devices. Several vehicle manufacturers even provide over-the-air (OTA) updates, while others are equipped with Wi-Fi for their passengers. Turning cars into connected devices adds new cyber risks including exposure, theft, and tampering.

Therefore, the level of security required to protect these vehicles extend far beyond the entry points of the vehicle itself, both wired and wireless. To accomplish this, OTA updates need to use the appropriate encryption methods; data warehouses used by the manufacturers to receive and transmit vehicle data need to be safeguarded; and standards need to be created that articulate best practices in the industry.

146 "Autonomous commercial vehicles: ready for the road?"; Kearney.

How about the level of cyber risk faced by the auto industry? A 2021 industry report produced by a digital services consulting firm[147] quantifies the value at risk in this way:

Figure 13



Invisible Tech—Real Impact: The Industry View

Some recent cyber-attacks illustrate the potential of future impacts:

- Two researchers have displayed how a zero-click exploit[148] could be used to hack Tesla—and possibly other cars—remotely, using a drone. The researchers showed how to take full control of the infotainment system (although not the drive control itself). While Tesla has patched this vulnerability, the vulnerable component is widely used in the auto industry, which means that other cars could be vulnerable.

- One of Honda Motor Company's internal servers was attacked[149] by a case of Ekans ransomware in 2020, affecting its production, sales, and development activities. Ekans uses RSA[150] encryption to lock up impacted machines and will go on a "process killing rampage, terminating any system that could become a barrier to the malware's activities and deleting shadow copies in the process to make it more difficult to recover files."[151]

147 *Invisible Tech—Real Impact*; Infosys; 2021.
148 "Tesla Car Hacked Remotely From Drone via Zero-Click Exploit"; *SecurityWeek*; May 3, 2021.
149 "Honda's global operations hit by cyber-attack"; BBC News; June 9, 2020.
150 Rivest, Shamir and Adleman (RSA) algorithm, a public key encryption technique.
151 "This is how EKANS ransomware is targeting industrial control systems"; *ZDNet*; July 2, 2020.

- During a test drive in 2019 using Tesla's Navigate on Autopilot feature, a staged attack[152] caused a car to suddenly slow down and unexpectedly veer off the main road. Researchers "found that 'spoofing' attacks on the Tesla GNSS receiver could easily be carried out wirelessly and remotely, exploiting security vulnerabilities in mission-critical telematics, sensor fusion, and navigation capabilities."[153]

- A hacker named "EvanConnect" developed a device in 2020 that can break into any luxury car that uses a wireless key fob system. It is being sold for $12,000. One security expert said that the "keyless repeater technology is commonly known in the field."[154]

Clearly, as vehicle systems become increasingly interconnected, more potential cyber exposures will exist, and therefore stronger cybersecurity measures will be necessary for the manufacturers of autonomous vehicles. It is equally important for the vehicle owners to ensure software updates are done on time.

Federal and State Legislative and Regulatory Outlook

There is currently no comprehensive federal or state-level regulatory structure for AV vehicles in the United States.[155] Traditionally, both federal and state agencies work together to regulate the safety of passenger vehicles.

A congressional bill H.R. 3711,[156] also known as the Self Drive Act, would have prescribed the safety standards for highly automated vehicles. Two attempts to pass the bill in 2017 and 2020 both failed due to concerns about the language. However, key federal lawmakers have recently noted they intend to enact legislation to create federal safety and security standards for autonomous vehicles.[157]

In *Automated Driving Systems: A Vision for Safety*,[158] the National Highway Traffic Safety Administration (NHTSA) laid out voluntary guidance, technical assistance to states with respect to federal and state roles, best practices for consideration in legislating in this area, as well as "best practices for state highway safety officials."

152 "How Hackers Can Take Over Your Car's GPS"; *Claims Journal*; June 19, 2019.
153 "Tesla Model S and Model 3 vulnerable to GNSS spoofing attacks"; GPS World; June 28, 2019.
154 "Hacker creates new device that can unlock any luxury car"; The Economic Times; Feb. 17, 2020.
155 *Autonomous Vehicles: Legal and Regulatory Developments in the United States*; Jones Day; July 2021.
156 *H.R.3711—SELF DRIVE Act*; Congress.gov; June 4, 2021.
157 "Congress makes renewed push on self-driving cars bill"; *The Hill*; Feb. 17, 2021.
158 *Automated Driving Systems 2.0: A Vision for Safety*; U.S. Department of Transportation; September 2017.

In June 2020, the Department of Transportation (DOT) launched the AV TEST initiative, a cooperative effort between the DOT, 52 companies, state governments, and associations with the purpose of "coordinating and sharing information in a standard way."

There are six levels of self-driving according to a standard setter:[159]

1. Level 0—No Driving Automation
2. Level 1—Driver Assistance
3. Level 2—Partial Driving Automation
4. Level 3—Conditional Driving Automation
5. Level 4—High Driving Automation
6. Level 5—Full Driving Automation

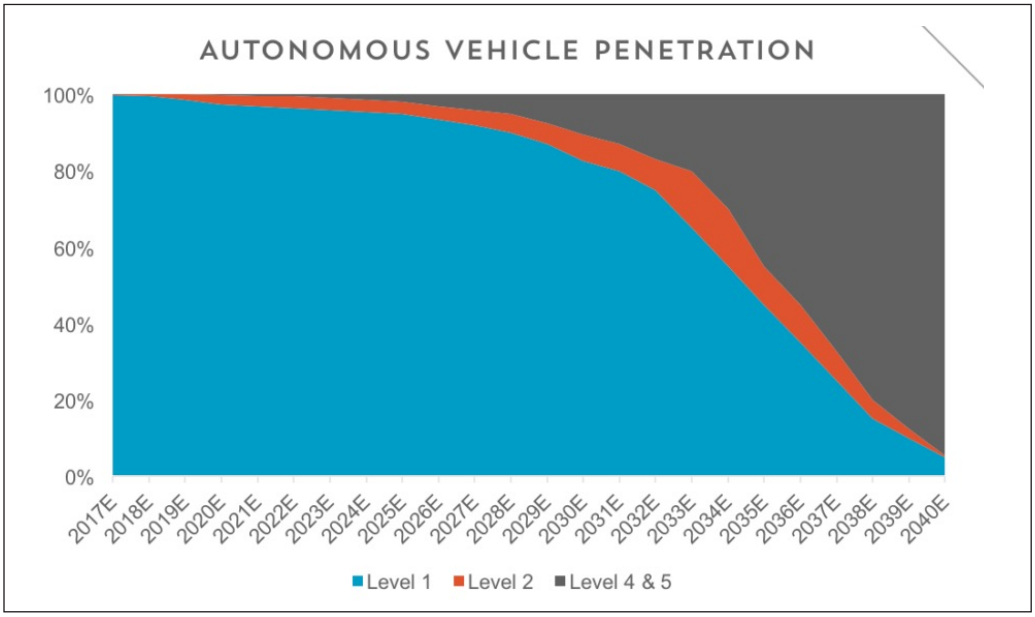
In 2020, NHTSA published an advance notice of proposed rulemaking to "obtain public comments on the development of a framework for Automated Driving Systems (ADS) safety."[160] The framework's intent is to "objectively define, assess, and manage the safety of ADS performance while ensuring the needed flexibility to make further innovation." It had a comment period that ended in April 2021.[161]

In November 2020, the FCC split the 5.9 GHz band between dedicated ranges for Wi-Fi and C-V2X (Cellular-Vehicle-to-Everything) in order to "enhance automobile safety."

159 *Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles*; SAE International; April 2021.
160 *Framework for Automated Driving System Safety*; National Highway Traffic Safety Administration; Nov. 19, 2020.
161 "Framework for Automated Driving System Safety; Extension of Comment Period"; National Highway Traffic Safety Administration; Jan. 29, 2021.

One industry source[162] projects the following market penetration by self-driving level in the next 20 years:

Figure 14



Source: Loup Ventures

According to the National Conference of State Legislatures,[163] as of 2020, 29 states had enacted laws related to autonomous vehicles. However, as of 2021, 37 states and D.C. have some kind of AV-related regulation.[164]

More could be done on this front, especially when we consider other countries: The United Kingdom (UK)[165] and Germany,[166] for example, have enacted laws to address liability issues.

In June 2020, 53 countries adopted a United Nations regulation[167] for jurisdictions that adhere to it that would require national regulators to guarantee vehicles are adequately protected against potential cyber security attacks. The regulation also would require manufacturers to ensure that suppliers include cyber security protection such as forensic technology able to decipher cyber-attacks.

While the U.S. participated in discussions in the development of the regulatory agreement, it did not vote and has not implemented the regulation. However, those that sell vehicles in jurisdictions where the cyber security regulation has been implemented must comply.

162 *Auto Outlook 2040: The Rise of Fully Autonomous Vehicles*; Loup Ventures; Sept. 6, 2017.
163 "Autonomous Vehicles State Bill Tracking Database"; National Conference of State Legislatures; March 16. 2022.
164 *Autonomous Vehicles: Legal and Regulatory Developments in the United States*; Op. cit.
165 *Automated and Electric Vehicles Act 2018*; Legislation.gov.uk.; 2018.
166 "Gesetz zum autonomen Fahren tritt in Kraft"; German Federal Ministry for Digital and Transport; July 27, 2021.
167 "U.N. Announces New Cyber Security Regulation for Connected Vehicles"; IEEE.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.[168]

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,[169] 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.

168 "Cybercrime To Cost The World $10.5 Trillion Annually By 2025"; *Cybercrime Magazine*; Nov. 13, 2020.
169 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

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