UPDATED FEBRUARY 2023

An Introduction to Cyber
CYBER RISK TOOLKIT

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

American Academy of Actuaries
ACTUARY.ORG

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

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

American Academy of Actuaries

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

An Introduction to Cyber

Updated February 2023

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 cyber-attacks. Other papers 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

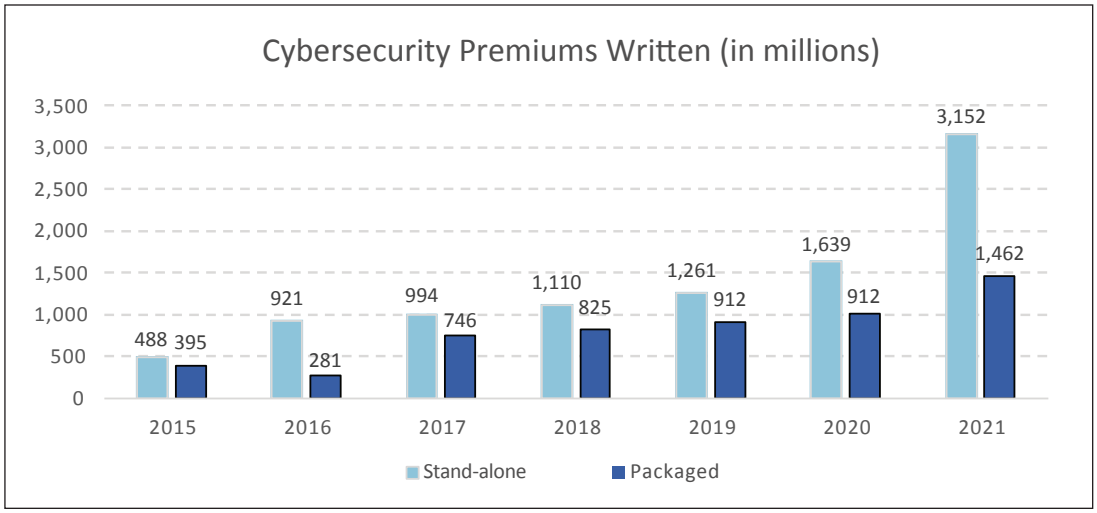
The National Association of Insurance Commissioners (NAIC) Cybersecurity Insurance and Identity Theft Coverage Supplement has been used to gather information about cybersecurity and identity theft insurance since 2015. Our paper focuses on statistics from cybersecurity coverage and not identity theft 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 $4.6 billion U.S. market in 2021 and have more than doubled since 2019. This comprised of approximately 0.6% of the total direct premiums written in the U.S. property & casualty P/C) market. On average, 63% of cybersecurity coverage premiums written consist of the stand-alone product. However, a larger proportion (74% in 2021) of carriers are writing cybersecurity policies on a packaged basis.

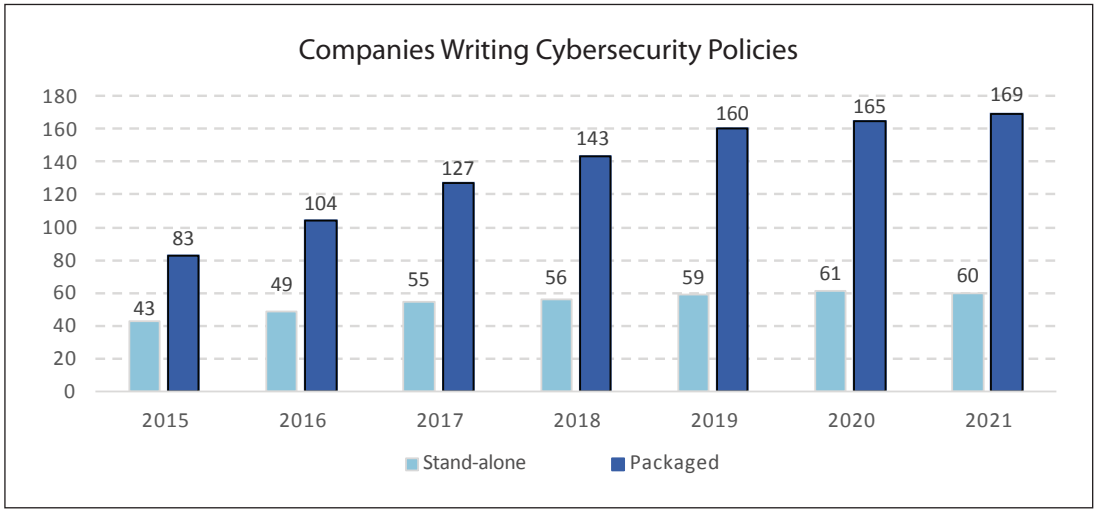
2 "Cybersecurity," National Association of Insurance Commissioners (NAIC); May 27, 2021.

Figure 1



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

Figure 2

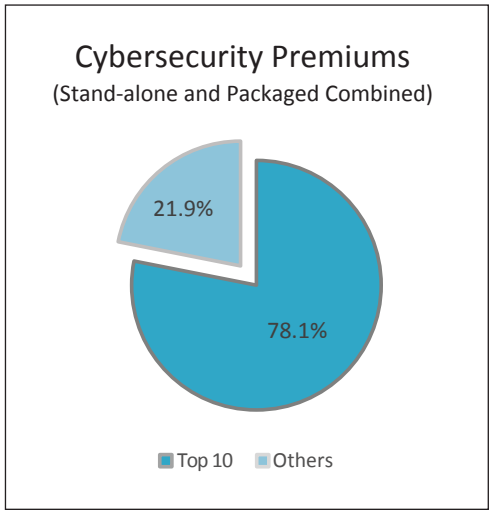


*The figures shown in the graphs are limited to information reported to NAIC by insurance carriers.

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 2020 was more than 75%, with a decrease to 72% in 2021.

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



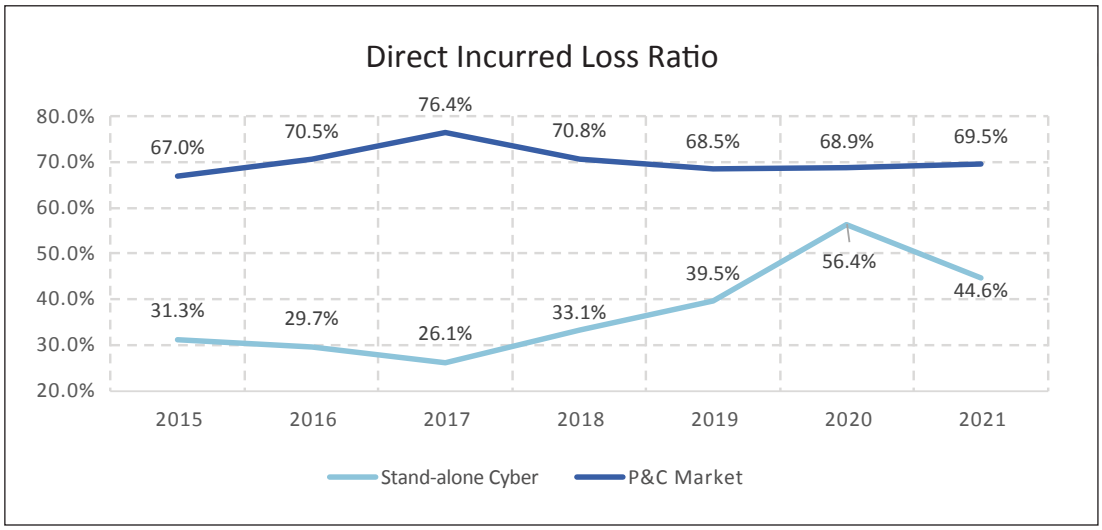
*The figures shown in the graphs are limited to information reported to NAIC by insurance carriers.

The cybersecurity insurance market has observed relatively lower loss ratios compared to the performance of the overall P&C market. Between 2015 and 2019, the calendar year loss ratio for stand-alone policies has hovered between 26% to 40%. However, loss experience has deteriorated to 56% and 45% for 2020 and 2021 respectively. In addition, cyber claims closed with a payment increased 200% in the last three years.[6] Packaged policy loss ratios have been excluded in figure 4 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 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.

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.
6 "Rapid Cyber Premium Growth by Fairfax, Tokio Marine Increased Share of the Market," *Insurance Journal*, May 9, 2022.

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 cyber-attacks and ransomware demands 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 47%[7] 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[8], the vast majority of third-party coverage for standalone cybersecurity policies continue to be written on a claims-made basis.

Commercial insurance across all lines had an average rate increase of 6% overall during the first quarter of 2022 but cyber insurance rates increased 19.75% on average.[9]

Willis Towers Watson reports that cyber insurance is getting more expensive, and renewals are taking longer to process. For those looking to purchase cyber insurance additional concerns include:

- Coverage from excess carriers is not aligned with primary coverages
- Carriers may require supplemental applications for ransomware coverage
- The number of underwriting questions has increased[10]

Cyber insurers are increasing prices and reducing coverage by increasing retentions, reducing overall policy limits, incorporating new coinsurance provisions and introducing other exclusions, Cyber insurers are also requiring greater cyber security from their policyholders. The majority of cyber insurers now require enterprise-wide multifactor authentication, written strategy of data-backup processes and a privileged access management tool to protect user credentials, among other criteria. Conditions for policy binding may also stipulate that the applicant institutionalize protection monitoring and response tools and establish a 24/7 security operations center (SOC).[11]

7 *Cyber Insurance: Insurers and Policyholders Face Challenges in an Evolving Market*; Government Accountability Office; May 20, 2021.
8 "Report on the Cybersecurity Insurance and Identity Theft Coverage Supplement"; NAIC and the Center for Insurance Policy and Research; Sept. 12, 2019.
9 "Rates Up Again in Q1 as Signs May Pont to 'Stronger Increase': Market Scout"; *Insurance Journal;* April 7, 2022.
10 "Commercial Insurance Price Hikes Drop to Single Digits but Cyber Triples"; *Carrier Management*, April 11, 2022.
11 "25 Years: The Journey of Cyber Insurance"; Insurance Journal; July 6, 2022.

Silent Cyber[12]

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 explicitly recognizing cyber exposures. They either explicitly include coverage for some aspects of cyber-related losses or clearly exclude any such losses.

Policy Coverage Definitions / Services

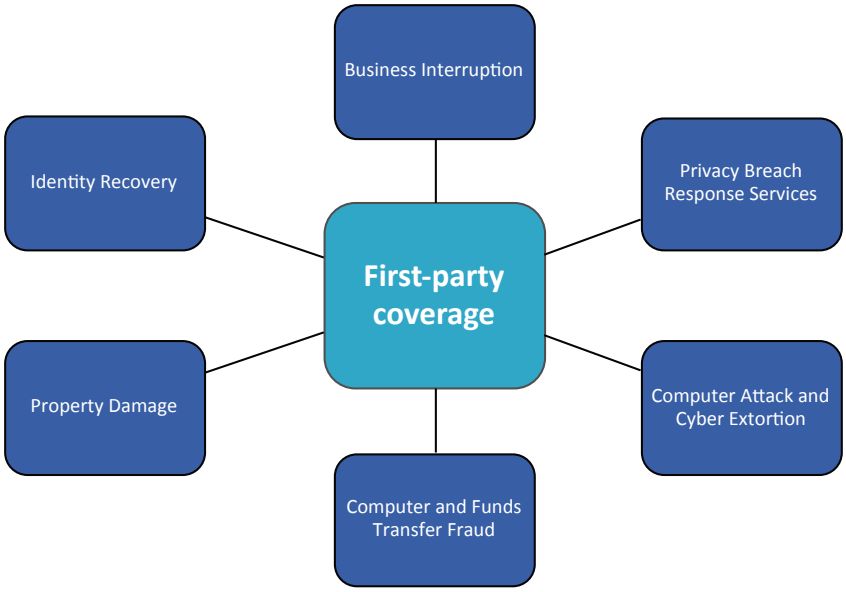
This analysis relies upon publicly available rate and rule filings submitted to state Departments of Insurance. The information from these filings was gathered and compiled, in order to compare the cyber policies being offered and the coverage definitions.

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.

12 Details on this topic are further described in a separate 2021 paper from the Academy on silent cyber.

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:
        i. Expenses must necessarily continue during the period of restoration; and
        ii. 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:

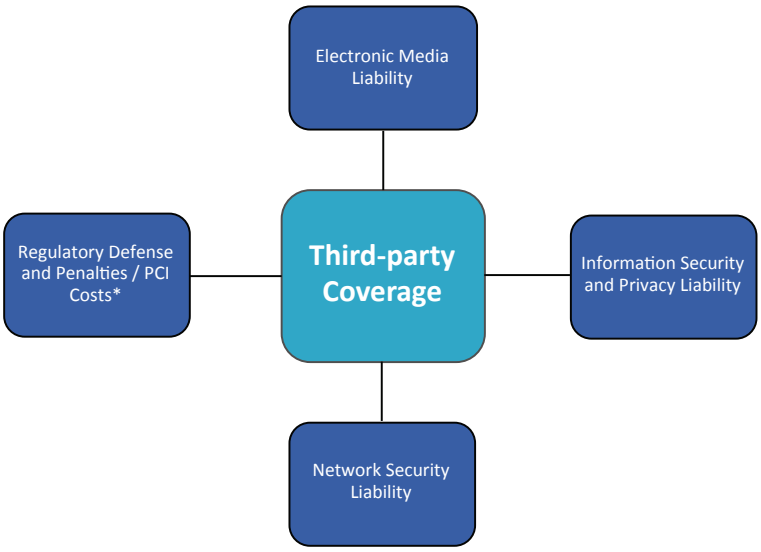
1. Case management services; and/or
2. Expense reimbursement.

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. uch 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:
    a. The alteration, corruption, destruction, deletion, or damage to data stored on computer systems.
    b. 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.
    c. 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[13,14,15,16,17] include:

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. Cyber-attack 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.

13 "Loss Mitigation for Cyber Policyholders"; Chubb.
14 "Protect Your Business before a Cyber Threat"; Travelers; 2021.
15 "Confidence to Thrive in the Digital World"; At-Bay; 2021.
16 "Coverages"; Coalition; 2021.
17 "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 cyber-attacks, 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.

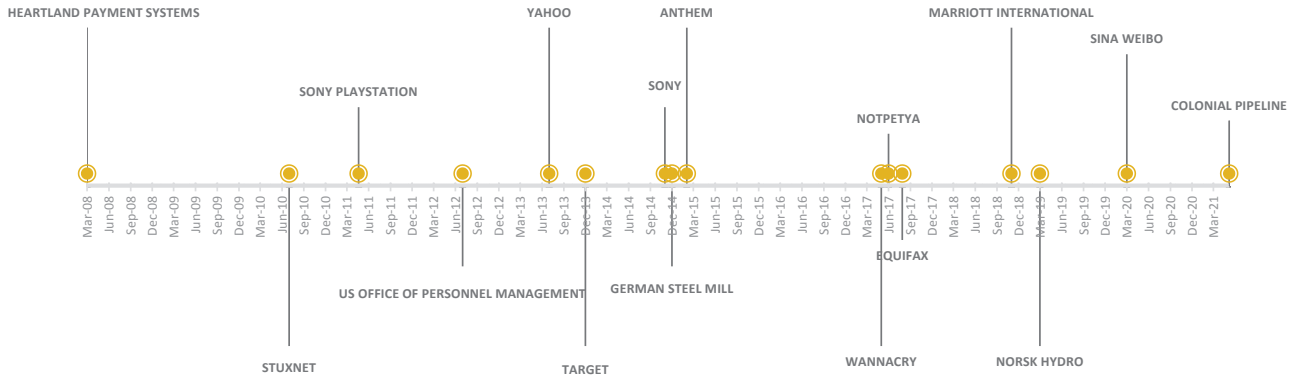
Zurich Insurance has denied Mondelez's claim for losses suffered in the 2017 NotPetya attack due to Zurich's "hostile or warlike action" clause in the property policy. As of November 2022, Mondelez has settled its lawsuit against Zurich Insurance but did not publicly reveal the settlement position.

In addition, a New Jersey court awarded Merck $1.4 billion from Ace American with a similar claim due to NotPetya.*

* "Merck's $1.4 Billion Insurance Win Splits Cyber From 'Act of War'"; Bloomberg Law; Jan. 19, 2022.

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[18] 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.[19]

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[20] 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[21] 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[22] 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.

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

German Steel Mill[23]

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[24] cyber-attack 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."

Colonial Pipeline[25]

The Colonial Pipeline Company was forced to take its pipeline offline in May 2021 as a result of a ransomware attack. The pipeline supplies about half of the United States East Coast's gasoline. To avoid a prolonged disruption, $4.4 million worth of bitcoin was paid to the hackers, of which approximately $2.3 million was subsequently recovered according to the Department of Justice.

23 "A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever"; *Wired*; Jan. 8, 2015.
24 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.
25 "The Biggest Cyberattacks in History"; HistoryHit; March 24, 2022.

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