PEARL TECHNOLOGY

STATE OF CYBER INSURANCE

Pearl Technology

Prepared By
Anthony Mini
President | CISO

2023

Introduction

There are striking similarities between cybersecurity and cyber insurance. The "ones and zeros" from binary to statistical modeling all merge into the overarching domain of risk management. The Key Risk Indicators (KRIs) published in the annual cybersecurity reports from Verizon and the FBI all illustrate that the emerging threats to cybersecurity are growing in frequency and cost.

The FBI noted an increase in cybersecurity incidents in the past four years—from 19,060 in 2016 to 26,074 in 2021. Verizon reported that data breaches nearly doubled in recent years, increasing from 2,260 in 2016 to 5,258 in 2021. Further, CrowdStrike Intelligence, a cybersecurity organization, observed an 82% increase in ransomware-related data breaches from 2020 to 2021. Costs associated with cybersecurity incidents both to the overall economy and to affected organizations are significant. However, cost estimates for these incidents vary widely. For example, in 2018 the Council of Economic Advisers estimated that malicious cyber activity cost the U.S. economy between $57 billion and $109 billion in 2016 (The Council). According to a 2018 RAND report, cyber incidents may have cost the economy more than $242 billion per year. A 2020 CISA study, based on data from several datasets published in 2015–2020, reported that the median cost of a cyber incident to a U.S. organization might range from $56,000 to $1.7 million.

As these trends continue to get worse, it is important that organizations seek to better understand the risk they are managing. Throughout this paper, we will address the state of cybersecurity from two vantage points: one being ***cyber assurance***, which are the processes, technologies, and efforts "left of boom" and are proactive in defending against an attack; and the latter being ***cyber insurance***, which are the processes, technologies, and efforts focused on the "right of boom," after the alert of a cyberattack.

A notable trend impacting the threat landscape and cyber insurance industry is the shift in victims. Traditionally, threat actors would target those organizations who had something worth taking, such as Personally Identifiable Information (PII), Protected Health Information (PHI), trade secrets, classified information, etc. However, with the evolution of ransomware attacks and the ability of the threat actor to halt an organization's production environment, hackers started targeting any company that had money to pay. This shift significantly leveled the playing field of new companies getting attacked.

Two Types of Cyberattack

There are two primary means in which a company can be "hacked" that will significantly impact the balance sheet. Fraudulent Funds Transfer (FFT) and ransomware were the biggest drivers of economic loss from cybercrime in 2022, accounting for more than 50% of insurance claims, according to figures from Corvus. Ransomware attacks are a type of malicious cyberattack where hackers use malicious code to target and gain access to a system. Once the hackers are inside, they encrypt data that renders the data unusable and then demand a ransom from the victim to release and provide access to the data. FFT, also known as Business Email Compromise (BEC), is a type of social engineering attack where scammers use deception and manipulation to take advantage of organizations and gain access to their financial accounts and transfer money. BEC frauds typically involve sending emails to companies that claim to be from a legitimate partner or customer. These emails use trust to gain access to sensitive information or initiate wire transfers of large sums of money. This type of attack is becoming increasingly popular as it is done with minimal risk and high reward. The 2022 Internet Crime Complaint Center received BEC complaints with losses exceeding $2.7 billion.

The Million Dollar Question

We know there is a problem, but what is the potential cost of damage to your organization? What is the ROI for assurance and insurance? IT managers struggle to demonstrate the likelihood of an attack, the cost, or the proportional protections required. Likewise, insurance actuaries struggle to understand the wicked problem of cyberattacks. If an organization does not have access to cybersecurity subject matter experts (SMEs) who can perform a Quantitative Risk Analysis (QRA), there are market benchmarks to consider.

Although the Federal Emergency Management Agency (FEMA) report points out the impact of natural disasters, the perceived downtime for these disasters is similar to the exposure of downtime experienced during a cyberattack. FEMA reported 40% of small- and mid-sized businesses (SMBs) never reopen after a natural disaster, and an additional 25% reopen but fail within a year. Also, the IBM "Cost of a Data Breach 2022" report shows the average ransom payment of $812,360. In addition, the total cost of a ransomware attack, $4.5 million on average, includes the entire cost of recovery. Lastly, the Deloitte Insights report tells us that the average company spends 10.9% of their IT budget on cybersecurity (average 0.48% of company revenue) and average $2,700 per full-time employee (FTE) on cybersecurity.

What Is Cybersecurity Insurance?

In the United States, the states and territories are the primary regulators of the business of insurance, including cyber insurance. The regulators seek to ensure that insurance policy provisions comply with state law, are reasonable and fair, and do not contain major gaps in coverage that might be misunderstood by consumers and leave them unprotected (GAO). Cyber insurance emerged from third-party liability to cover companies' duty to protect their clients' and employees' data and was rooted in errors-and-omissions insurance. Cyber insurance protects a

business against financial losses that are caused by incidents such as data breaches and theft, system hacking, ransomware extortion payments, and more. Depending on the industry that you work in, you may be required by your state to carry other types of insurance, most often general liability insurance. For businesses that offer services, such as those in real estate, insurance, or healthcare, you may need professional liability insurance (also called errors and omissions insurance) before you can get a license.

What Does Cybersecurity Insurance Cover?

Before we dive into the details of the coverage, it is important to highlight a couple of examples of companies that did not have cybersecurity coverage. The 2011 Sony PlayStation Network breach exposed the PII of 77 million PlayStation accounts. Due to the breach, Sony incurred over $171 million in costs. The court ruled that Sony's insurance policy only covered damage to physical properties. This left Sony the full amount of costs related to the cyber damages and the breach. In September 2017, Equifax, a credit reporting agency, was the victim of a data breach that exposed 147 million peoples' personal information. Equifax reached a settlement in 2019 with the U.S. Federal Trade Commission (FTC). The agreement Equifax made in the settlement was that they would spend $425 million to provide people with free credit reporting, cash payments, etc. These are just a couple of examples of high-profile cases that sparked the demand for cyber specific insurance coverage.

Cyber insurance may provide coverage or protection against unauthorized access, extortion, legal fees, victim notification, forensics experts, data recovery, repairing or replacing damaged computer systems, business interruption, reputational hardship, network security liability, privacy liability, regulatory proceeding liability, Payment Card Industry Data Security Standards (PCI-DDS), media liability coverage, and more.

First- & Third-Party Loss Policies

Various insurance policies cover first-party losses, but companies are starting to offer third-party liability/loss policies. First-party coverage protects your company when they incur expenses from a data breach. Third-party coverage provides protection when a customer, vendor, partner, or other party sues for allowing a data breach to occur. The gaining popularity of third-party insurance coverage can be anticipated by the rise of supply chain attacks.

For example, in May 2021, the Colonial Pipeline Company learned that it was the victim of a ransomware attack against its IT network. As a safety measure, the company disconnected certain industrial control systems, resulting in a temporary halt to all pipeline operations. This in turn led to short-lived gasoline shortages throughout the southeast United States. In July 2021, Kaseya—a provider of IT and security management solutions for managed service providers and small- to medium-sized businesses—reported that its tools were compromised and used to conduct ransomware attacks that affected about 1,500 organizations.

What Isn't Covered by Cybersecurity Insurance?

Business owners often assume that existing business owner's policy (BOP) coverage includes protection from data breaches, but there are likely gaps, similar to professional liability, medical coverage, and worker's compensation. Coverage can have sublimits or be limited to per-occurrence of aggregated claims. When the policy is active, a per-occurrence limit indicates the insurer will pay up to a set amount to cover any single claim. When the policy indicates an aggregate limit during the lifetime of the policy (usually one year), this means it is the set maximum the insurer will pay to cover claims during that year.

Certain policies exclude coverage when an incident was both preventable and caused by humans. Examples of exclusions are rooted in poor configuration management, careless mishandling of digital assets, cyber events initiated and caused by employees or insiders, infrastructure failures not caused by a purposeful cyberattack, preexisting or cyber events that occurred before the policy was active, and the cost to improve security systems. The Cybersecurity and Infrastructure Security Agency (CISA) in the United States operates under the Department of Homeland Security, CISA strongly encourages businesses, both large and small, to improve their cybersecurity in return for more coverage at more affordable rates.

The lack of common definitions in policy language and vastly different risk assessments result in varying coverage from one provider to another. When choosing a policy, companies should dig into the details to ensure it contains the necessary protections and provisions. The companies should take note of any exceptions or expectations of recurring security controls.

The Application Process

Typically, most providers require that you complete an application to start the process of obtaining cybersecurity insurance. The applications tend to collect the total number of employees, amount of annual sales/revenue, and the amount of annual revenue from online sales or services they have in the United States, Canada, and other countries. They will take into consideration your inventory of hardware and software, number of records, amount of record transactions, and the safeguards you have in place to protect your information. Some additional considerations are legal expenses, forensic expenses, Incident Response (IR), and customer notification expenses. Depending on what kind of business is applying for a cyber insurance policy, they could have any regulatory fines and penalties covered if they are subject to industry-governing authorities, i.e., General Data Protection Regulation (GDPR), Payment Card Industry

Data Security Standard (PCI DSS), Federal Trade Commission (FTC) Safeguard Rule, etc. When choosing a cybersecurity insurance policy, the pricing is based on the insured entity's yearly revenue and the industry. To apply for cybersecurity coverage, a business must submit to a security audit or provide documentation assisted by an assessment tool. At the time of this publication, there is no standard cybersecurity risk assessment across providers or for all insureds, and some assessments are more comprehensive than others. The Federal Financial Institutions Examination Council (FFIEC) does provide a free helpful assessment tool. The results from the audit or the assessment tools will factor into the coverage and cost of the premiums. While many carriers do run vulnerability scans and assessments, there are still carriers in the marketplace that do not. Some rely just on an application, some (for small firms with low limits) don't require hardly any information beyond the type of business and revenue. For small firms, some carriers offer the option of tacking small limit cyber coverage onto other policies, like business owners' policies or professional liability.

What Are Insureds' Responsibilities?

Once a person or business gets cybersecurity insurance, they hope they never need to use it. Guarding against an attack does require due diligence on the part of the insured. They need to keep their devices and data protected. There are several minimum-security controls and expectations from the insurance provider, including multi-factor authentication (MFA), endpoint protection and response (EDR), encryption, backups, awareness training, patch management, e-mail filtering, access controls, network segmentation, BCP/DR/IR plans (written and assessed), and more. Some cyber insurance companies are providing access to cyber assurance security tools to help prevent the likelihood of an attack.

Trends & Case Studies

Perhaps most significantly, the case law that has shaped the financial sector, through thousands of cases that have been tried and ruled on for a couple hundred years, simply has not taken place yet in cyber. The legal aspects are not simplified nor codified by any one governing organization. Simply put, we do not know what to expect.

-Mondelez and Zurich Reach Settlement

In October 2022, the Mondelez International Food Company and Zurich American Insurance reached a settlement in court to end their multi-year legal battle. This battle started because Mondelez filed a $100 million claim for the damage caused by the NotPetya cyberattack back in 2017. Zurich initially refused to cover the damages to Mondelez, whose court documents showed they lost more than 1,700 servers and 24,000 laptops to the malware. The case between Mondelez and Zurich was complicated because Mondelez never expressly took out a cyber insurance policy, but they did take out a policy that they argued covered cyberattacks. According to Billy Gouveia, chief executive of the incident response business Surefire Cyber, “The settlement between the two companies will fuel growth for the cyber insurance market.” (The Record)

-Act of War Exclusions

Excluding war perils has been a feature of insurance for centuries. However, the act of war clause has stirred up considerable debate as it attempts to define territory that the United States and cyber professionals have argued for decades, defining a cyber activity that is “an act of war.” Indeed, to exclude "all war" remains a fundamental requirement of compliance for policies.

This concept is unique in comparison to other professional insurance coverage. Consider how vulnerable organizations are to the fingertips of well-funded enemies using the cyber domain for theft of intellectual property, strategic posturing, and theft to fund military operations.

On August 16, 2022, Lloyd's of London announced that, beginning March 31, 2023, it would require all cyber insurance policies to specifically exclude coverage for losses related to state-backed cyberattacks. The requirement, would preclude coverage during costly cyberattacks by equating state-backed cyberattacks with kinetic hostility from an insurance perspective. It increases uncertainty, since it can often take months (if not years) for experts to attribute attacks to specific groups of threat actors and those findings are rarely conclusive. Additionally, adversaries are pivoting their affiliations and attributions to avoid being identified and blocklisted from receiving their ransoms.

In January 2022, pharma giant Merck & Co., Inc. awarded a $1.4 billion insurance win against insurer Ace American Insurance Co. The presiding judge ruled that the War or Hostile Acts exclusion was inapplicable in the Merck claim, which had parallels with the Mondelez claim.

-Responsibilities to Report

In March 2022, President Biden signed into law the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). Enactment of CIRCIA marks an important milestone in improving America's cybersecurity by, among other things, requiring CISA to develop and implement regulations requiring covered entities to report cyber incidents and ransomware payments. These reports will allow CISA to rapidly deploy resources and render assistance to victims suffering attacks, analyze incoming reporting across sectors to spot trends, and quickly share that information with network defenders to warn other potential victims. The regulation to

report cyberattacks will put a tremendous amount of pressure on organizations to increase their cyber assurance and insurance programs.

Additionally, the Securities and Exchange Commission ("Commission") is adopting new rules to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incidents by public companies that are subject to the reporting requirements of the Securities Exchange Act of 1934. Specifically, we are adopting amendments to require current disclosure about material cybersecurity incidents. We are also adopting rules requiring periodic disclosures about a registrant's processes to assess, identify, and manage material cybersecurity risks, management's role in assessing and managing material cybersecurity risks, and the board of directors' oversight of cybersecurity risks. Lastly, the final rules require the cybersecurity disclosures to be presented in Inline eXtensible Business Reporting Language ("Inline XBRL") (SECURITIES AND EXCHANGE COMMISSION).

-Cyber Insurance Market

GlobalData predicted that the cyber insurance industry would grow to $8.92 billion in 2021 and then grow up to $20.6 billion by 2025 (Field Effect). Over the course of 2022, insurance companies drastically increased their premiums for cyber insurance policies after multiple attacks and action taken by the government increased demand for products. According to the National Association of Insurance Commissioners, direct-written premiums collected in 2021 by the biggest U.S. insurance companies swelled year-over-year by 92%. It was reported that the increase reflected higher rates and not that insurers expanded the amount of money they were willing to cover. Increasing the premium cost helped the cyber insurance industry in the U.S. trim down its direct loss ratio, which is the percentage of their income that it pays to people who file claims with them, to 65.4% in 2021. In 2020, before getting their ratio trimmed down, it was at a record high of 72.5%. These numbers are still incredibly high compared to 2019's record low

of 47.1%. Alongside the rise in premium prices, insurance companies cut what their cyber insurance policies would cover (WSJ).

What Does the Future Hold?

The landscape of cybersecurity insurance will be ever-changing due to the speed and creativity of cybercriminals. Insurance companies will need to adapt and provide quality coverage but will also have to put greater focus on consumer protection and paying out claims.

It is imperative for an organization to understand the risk they manage and document what they are avoiding, reducing, transferring, and accepting. Outside of all the geeks and squeaks of cybersecurity, it is important to have a fundamental awareness of the business impact analysis. It's critical to understand where your crown jewels are, how you secure them, and practice contingency plans to be comfortable with response procedures. We often experience a company's tendencies to skirt cyber assurance best practices because of the short-term inconveniences. Unfortunately, these short-term conveniences typically lead to costly attacks. Therefore, it is important to highlight the potential cost associated with not using e-mail filters, enforcing awareness training, conducting phishing tests, and using MFA tools.

Overall, insurers will reduce their exposure through policy limits, raising premiums, requiring cyber hygiene, and adding exclusions. Therefore, companies will need to balance their risk appetite, bundle their insurance policies, and consider paying the annual premium upfront for cost savings. Lastly, organizations stakeholders need to become more intimate in their business impact analysis (BIA), which is the process to determine and evaluate the potential effects of an interruption to critical business operations because of a disaster,

accident, attack, or emergency. A good BIA will drive the business decisions that manage risk with assurance and insurance.

CITATIONS

Bateman, et. al, Systemic Cyber Risk: A Primer (Carnegie Endowment for International Peace and the Aspen Institute: Washington, D.C., 2022). Although there is not a commonly accepted definition for systemic cyber incidents, this definition, offered by the authors of this report broadly covers other definitions offered by the cybersecurity and insurance industries. For example, the report reviews CISA's definition, which is as follows: "Systemic risk occurs when risk is spread across interdependent systems so that a failure of one component has consequences system wide, amplifying the impact of the incident. In this context, [CISA] is looking to identify and understand the ways that cyber risks or incidents in individual pieces or components of critical infrastructure or National Critical Functions could create far-reaching cascading impacts, leading to system-wide functional degradation or failure." CISA, Systemic Cyber Risk Reduction Venture, https://www.cisa.gov/sites/default/files/publications/FS_Systemic-Cyber-Risk-Reduction_508.pdf, last accessed on May 23, 2022.

Carnegie, acts of war, including cyber war, can have cascading consequences across entire systems. One federal statutory definition of "act of war" is any act occurring in the course of (1) declared war; (2) armed conflict, whether or not war has been declared, between two or more nations; or (3) armed conflict between military forces of any origin. 18 U.S.C. § 2331(4); however, contractual definitions of "act of war" vary. "Act of war" exclusions are generally found in policies issued in most lines of insurance, including cyber.

CISA. Cybersecurity and Infrastructure Security Agency, 2021 Trends Show Increased Globalized Threat of Ransomware, AA22-040A (Washington, D.C.: February 2022). In a written response, CISA explained that the increase in cyber incidents may be partially attributed to organizations' improvements in detecting incidents.

Corvus Insurance, sublimits refer to limitations on how much coverage is available for a specific type of loss. For example, a policy may have an overall limit of $100,000 in coverage but may limit ransomware coverage to $50,000. Coinsurance requires policyholders to share a defined percentage of the claim cost with the carrier. For example, a policy can stipulate that a policyholder must pay a certain percentage of a ransomware claim. The Council of Insurance Agents & Brokers, Commercial Property/Casualty Market Index: Q4/2020 (Washington, D.C.: 2021).

Crowdstrike, 2022 Global Threat Report. Data breaches can occur when criminal groups steal an organization's data as part of a ransomware attack and threaten to make the data publicly available unless the victim organization pays a ransom.

(CSO) Burgess, C. (2022, November 3). Mondelez and Zurich's Notpetya cyber-attack insurance settlement leaves behind no legal precedent. CSO Online. https://www.csoonline.com/article/3678970/mondelez-and-zurich-s-notpetya-cyber-attack-insurance-settlement-leaves-behind-no-legal-precedent.html#:~:text=Multinational%20food%20and%20beverage%20company,the%20Mondelez%20network%20and%20infrastructure.

Field Effect. Filipkowski, B. (2023) What is the future of cybersecurity? Field Effect. Available at: https://fieldeffect.com/blog/what-is-the-future-of-cyber-security (Accessed: 06 June 2023).

Government Accountability Office. (2022) Cyber Insurance: Action Needed to Assess Potential Federal Response to Catastrophic Attacks, Available at: https://www.gao.gov/products/gao-22-104256

Jamie MacColl, Jason R. C. Nurse, and James Sullivan, Cyber Insurance and the Cyber Security Challenge (London, U.K.: Royal United Services Institute, June 2021).

The Council of Insurance Agents & Brokers, Commercial Property/Casualty Market Index: Q2/2021 (Washington, D.C.: 2021).

The Council of Insurance Agents & Brokers, Commercial Property/Casualty Market Index: Q4/2021 (Washington, D.C.: 2022). The Council also reported this was the first time after September 11, 2001 that premiums for a line of business increased more than 30%.

The Record. Mondelez and Zurich reach settlement in NotPetya Cyberattack Insurance suit (2022) The Record from Recorded Future News. Available at: https://therecord.media/mondelez-and-zurich-reach-settlement-in-notpetya-cyberattack-insurance-suit (Accessed: 06 June 2023).