Recorded Future®

# Managing Cyber Risk in the Age of Stakeholder Capitalism

*By Anna Iskenderian, Jesse Nuese, Jakob Wolk, and Levi Gundert*

# Abstract

Historically, cybersecurity investment has been viewed as a necessary evil that creates a drag on profitability in exchange for managing operational risk. When firms use traditional means of financial analysis to assess cybersecurity investments, the analysis suggests relatively low returns and high costs. However, this perspective creates near-sighted cybersecurity models that fall short of a comprehensive loss picture.

Even if organizations continue to rely on traditional financial metrics for cyber analysis, they should expect to observe overall future higher loss amounts. In response to continual data breaches, geopolitical instability, and social considerations, governments and international regulators are prioritizing cybersecurity for enhanced regulation. While possible, a cookie-cutter model of financial investment and returns fails to capture dynamic trends toward improved governance in cyberspace.

Alternatively, factoring social and reputational costs into risk management frameworks will create a more accurate and holistic understanding of cyber breaches' true costs. Stakeholder capitalism and environmental, social, and corporate governance (ESG) provide a new lens for calculating cybersecurity investment. ESG metrics are becoming increasingly popular, particularly with Generation Y and Generation Z driving expectations for good governance that extends beyond shareholders to customers, partners, and employees. National governments are beginning to respond by demanding transparency, codifying best practices, and creating larger incentives (primarily through punitive fines) for organizations with weak cyber risk management.

For the purpose of this paper, we focus on social and governance (the "SG") metrics, as they are most applicable and relevant in cybersecurity. Proactively focusing on social and governance standards will create a competitive advantage, specifically in operational risk management, due to a full accounting of stakeholders in an increasingly aggressive regulatory environment. Social and governance considerations reveal a new set of costs associated with cyber breaches.

To illustrate the value of proactive cyber risk management, we dissect over 400 public cybersecurity failure events over 7 years that resulted in a range of financial losses. We highlight instructive case studies and further illuminate patterns in loss types — namely, that a breach does incur an extended period of financial loss (even if relatively minor), but the loss is only a microcosm of the larger harm that companies experience. Finally, we discuss the future of good cyber governance and best practices in proactive risk management as the regulatory landscape continues to accelerate and evolve.

# Table of Contents

# Introduction

Potentially negative externalities that include climate change, social movements, complex supply chains, and ambiguous financial interdependence are challenging companies to adopt new risk assessment methodologies. As the potential for indirect costs mount, the contemporary business environment demands a dynamic risk framework that can accurately identify all facets of financial loss and codify commitments necessary to navigate this ever changing market landscape. To that end, environmental, social, and governance (ESG) metrics for corporate behavior have gained traction as a tool for benchmarking a stakeholder-centric approach to capital allocation.

Breaking from a singular focus on profit and shareholder value, ESG metrics underscore the importance of considering a variety of stakeholders, such as employees, suppliers, customers, and community, in evaluating investments. Cybersecurity represents an underappreciated component within this ESG paradigm shift — specifically in the social and governance categories — toward increased corporate responsibility. In this paper, we explain why cybersecurity investments using this model of stakeholder capitalism produce more holistic risk assessments that account for external costs and look beyond simple financial loss.

Before delving into the application of social and governance-informed cyber investment, we should look at how social and corporate considerations intersect with the cyber realm. Data responsibility is an essential first step in sound social and corporate governance. The exfiltration of personally identifiable information (PII) threatens the privacy, safety, and security of all stakeholders and erodes public trust.1 Threat actors continue to create vibrant markets for data stolen from security breaches, such as home addresses, phone numbers, online dating preferences, credit card information, passport identifiers, Social Security numbers, and even private health data.2 The public remains vulnerable to social engineering, identity theft, fraud, and other schemes that range from criminal monetization3 to intelligence-gathering by foreign governments.4 Lacking qualified professionals, tools, and training to properly assess and manage cyber risk, enterprises fail their social obligation to protect their customers' personal information.

---

1 The number of annual credential spill incidents nearly doubled between 2016 and 2020. Source: https://www.f5.com/labs/articles/threat-intelligence/2021-credential-stuffing-report

2 For example, underground marketplace SlilPP sold more than 80 million login credentials from over 1,400 companies since its inception in 2012. The portal was finally seized and shut down by the DoJ in June 2021. Source: The Record by Recorded Future. https://therecord.media/authorities-seize-slilpp-a-marketplace-for-stolen-login-credentials/.

3 Insikt Group reports that based on ease of use and low barrier of entry, dark web marketplaces will continue to be attractive destinations for threat actors to buy and sell PII, PHI, and other commodities for the foreseeable future. Source: https://go.recordedfuture.com/hubfs/reports/cta-2022-0217.pdf p.8

4 Insikt Group found that the volume of victims listed on extortion sites rose 110% from 2020 to 2021. The popularity of extortion sites that publish stolen credentials is partially due to its proven success in being a lucrative business model. For example, cybercriminal group Conti has received more than $200 million USD since it originated in 2017, capitalizing off of stealing and selling sensitive PII.
Source: Insikt Group, Annual Report — 2021 Malware and TTP Threat Landscape, https://support.recordedfuture.com/hc/en-us/articles/4416296400915.

Social and governance considerations gain utility as we anticipate consumer privacy and data protection will become a larger compliance priority as evidenced by recent legislation and regulatory changes, necessitating additional cybersecurity investment. Recent legislation includes the Strengthening America Cybersecurity Act5 and the Securities Exchange Commission's (SEC) new proposals for incident disclosure and cybersecurity risk management.6 Strong operational risk management via proper cybersecurity investment is a wise, proactive business decision in the context of this trend towards tighter data protection regulatory regimes. As social externalities play a greater role and drive more stringent regulations, social and governance metrics may be useful benchmarking tools for companies looking to proactively manage their brand reputations.

Beyond accounting for higher regulatory fines, companies have a reputational and ethical interest in creating greater corporate responsibility. Especially in the age of social media, the reputational consequences for a company that carelessly treats sensitive data can harm a firm's bottom line. Approaches to accurately assessing cybersecurity risk are often limited to attack surface size, security frameworks, or regulatory compliance, but proper risk assessments should incorporate social responsibilities to a firm's employees, customers, and suppliers. Using a stakeholder-based lens to make sense of the changing rules and regulations around cybersecurity, plus its reputational effects, can be instructive in ensuring the correct level of investment goes into risk mitigation.

5 https://www.securityweek.com/cyber-incident-disclosure-bill-passes-senate-amid-fears-russian-attacks

6 https://www.cnbc.com/2022/03/09/sec-votes-to-propose-new-cybersecurity-rules.html

# Analysis of Over 400 Cyber Events: Evaluating the True Cost of a Breach

We analyzed more than 400 cybersecurity events to build a broader understanding of how exactly a network breach affects an organization. Punitive fines for regulatory noncompliance are just one of many potential costs stemming from a data breach. Disrupted business operations, long-term legal liability, and reputational harm are a few examples of difficult losses to quantify. A financial-loss centric approach to assessing organizational cybersecurity posture that doesn't consider the nuance of these intangible losses will fail to comprehensively show potential breach externalities. We categorized the cyber loss events we analyzed into a high-level framework that includes **Loss Event Type**, **Initial Unauthorized Access Type**, and **Fines/Financial Loss** (if any) for each data breach. We explore these category nuances below.

## Dissection of Loss Categories

Loss categories represent financial loss in post-compromise ("right of boom") activities. We assessed 8 different types of financial loss events that stem from network breaches. The table below summarizes each loss event type category and its respective definition for our data.

| Loss Event Type | Definition |
|---|---|
| Extortion | The general act of cybercriminals demanding payment through threats or malicious activity against the victim.7 |
| Ransomware | A specific type of malware extortion that blocks access to a system, device, or file until a ransom is paid.8 |
| PII Theft | The theft of any information that permits the identity of an individual to whom the information belongs to be reasonably inferred by direct or indirect means.9 |
| Trade Secret Theft | Stealing or misappropriating a trade secret to the economic benefit of anyone other than the owner.10 |
| Communications Theft | Stealing or misappropriating plans, instructions, or correspondence to the economic benefit of anyone other than the owner. |

7 https://www.cisecurity.org/insights/blog/cyber-extortion-an-industry-hot-topic

8 Definition: https://www.cisecurity.org/insights/white-papers/security-primer-ransomware
Example: In April 2022, Conti ransomware gang launched ransomware attacks on several government agencies throughout Costa Rica. Conti operators breached and caused outages in platforms managing customs, taxpayer information, and other sensitive data. The ransom demanded is rumored to be at $10 billion. In 2021, Conti was identified among one of the most prolific ransomware-as-a-service (RaaS) operations by Insikt Group. Source: The Record by Recorded Future, https://therecord.media/conti-ransomware-cripples-systems-of-electricity-manager-in-costa-rican-town/. Insikt Group: https://support.recordedfuture.com/hc/en-us/articles/4416296400915

9 Definition: https://csrc.nist.gov/glossary/term/PII
Example: In November 2018, Marriott Hotels disclosed a data breach of their subsidiary, Starwood Resorts. Threat actors hacked into the network and accessed PII information of hotel customers, including names, mailing addresses, phone numbers, passport numbers, date of birth, and reservation dates. Source: https://support.recordedfuture.com/hc/en-us/articles/360013047893-Marriott-Discloses-Data-Breach

10 Example: Asurion, an electronics and home appliance insurance provider, paid USD $300,000 (AUD $448,000) in fees after former employee Nicholas Burks committed costly trade secret theft. Burks compromised a company laptop, stole private data from the company, and held it hostage for ransom. Burks threatened to leak stolen trade secret information to newspapers and competing companies. Source: https://app.recordedfuture.com/live/sc/7HngDOuXGztu

| Loss Event Type | Definition |
|---|---|
| System/Data Harm/ Destruction | The impairment or total deletion of sensitive data or a system.11 |
| Financial Fraud | Obtaining money, payment card information, or other financial assets through deception or criminal activity to initiate unauthorized transactions or extortion.12 |
| Data Impairment | The harm or misappropriation of data to undermine data integrity and trust.13 |

### *Brief Overview of Loss Events*

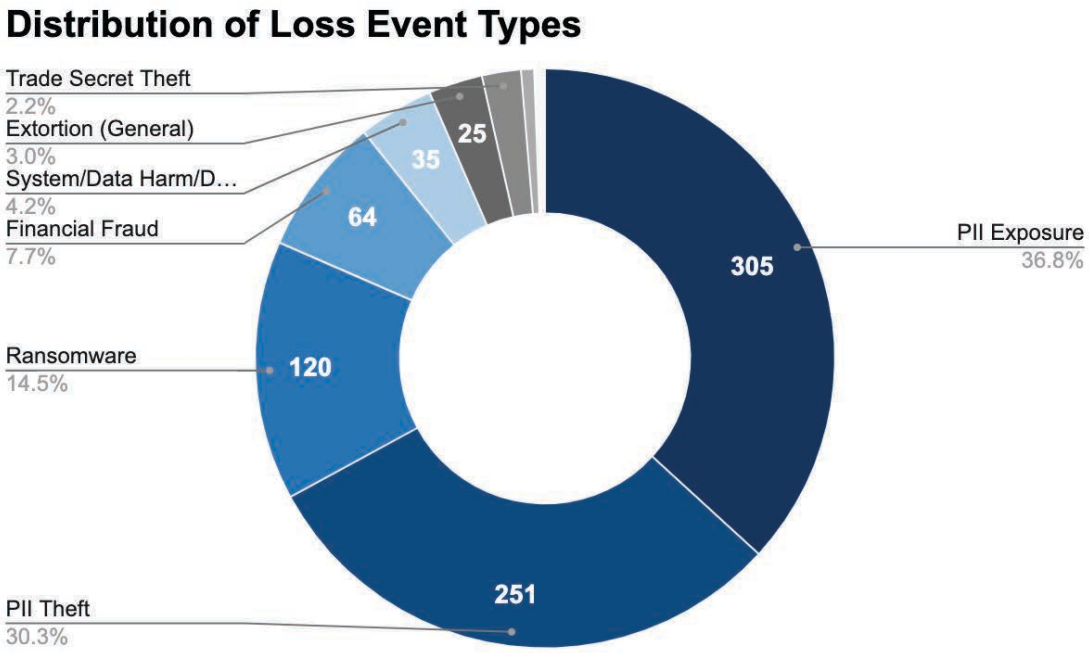
For every instance of a data breach, we identified its post-compromise loss event type. The pie chart below summarizes the distribution of loss events across our data. The top loss event types were PII exposure and PII theft, followed by ransomware. This result is consistent with other research on data breaches in recent years. For example, IBM's 2021 "Cost of a Data Breach Report" cites customer PII as the most common type of record lost, included in 44% of breaches.14 The least common loss event type in our data was communications theft and data impairment. This pie chart only refers to the counts of each loss event type in our data, meaning the frequency of a cyberattack within these loss event types.

11 Fallout from the NotPetya cyberattack caused crippling operational outages at Danish shipping and logistics company Maersk. The malware infection rendered the company unable to access the majority of its systems and applications, and wiped out access to almost all of its data. Source: https://www.i-cio.com/management/insight/item/maersk-springing-back-from-a-catastrophic-cyber-attack

12 https://www.visma.com/blog/what-is-financial-cybercrime-and-how-to-prevent-it/

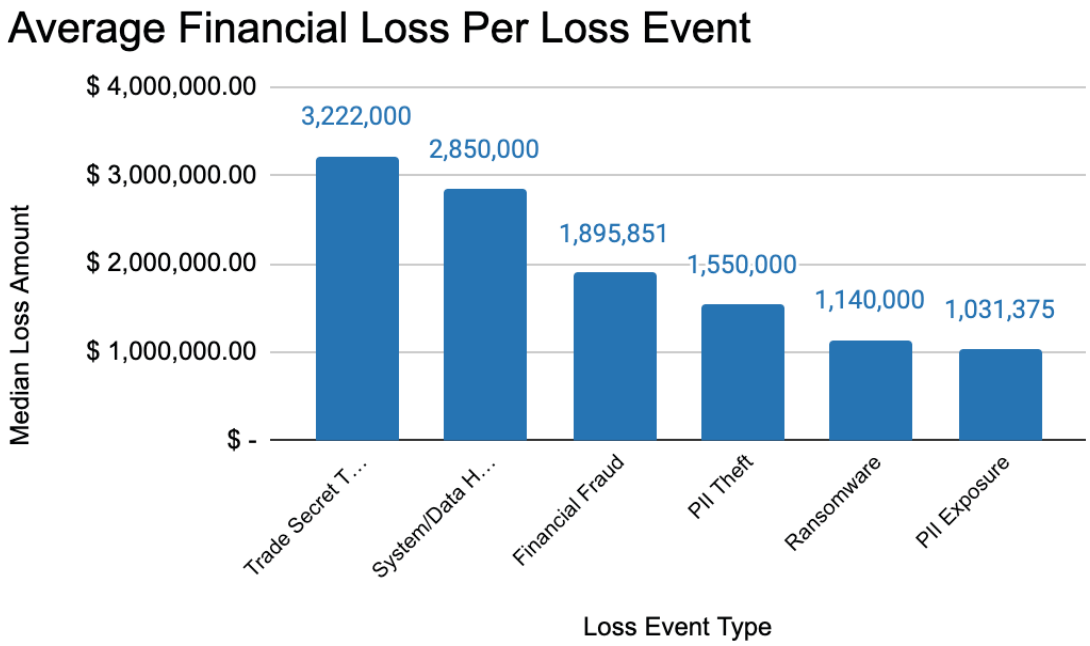
13 Example: In November 2021, hackers broke into the official FBI server and sent spam emails to a database of public email addresses, warning that someone was trying to steal the org's data. Though the email had several mistakes that undermined its authenticity, it was sent straight to the inbox of the recipients, rather than a spam folder. The fraudulent warning of an impending cyberattack from the official FBI email caused panic and confusion. Source: https://therecord.media/official-fbi-email-server-hacked-used-to-send-fake-threat/

14 https://www.ibm.com/security/data-breach




Some of the pitfalls of a financial loss approach are revealed when comparing our data against other cumulative cyber breach reports that consider tangible and intangible costs, such as the widely circulated IBM 2021 "Cost of a Data Breach Report".

The bar chart shown below demonstrates variations in financial loss across loss event type in our data. The average loss amount for a cyber breach across all companies we recorded was **$1.5 million**. Although PII exposure and PII theft were the most common loss event types overall, they were not the most financially harmful. Trade secret theft was the most significant loss event type identified, averaging a **$3.22 million** loss for the company. PII theft averaged a **$1.5 million** loss per company. Interestingly, the ransomware category average was **$1.14** million, which is more than 3 times lower than IBM's figure for ransomware loss amounts at $4.62 million on average. We will explore this discrepancy (and other ones) more in detail in following sections, but suffice it to say that the cost-based vision falls short. Overall, there is a need to look deeper into the financial losses from post-boom fallout, which is why an approach that lends weight to economic externalities is better at capturing the true cost of these loss events.




### Dissection of Initial Unauthorized Access Categories

Below we build a more detailed picture of a data breach by taking into account the initial access methods used by threat actors. Understanding common tactics can shape high-impact cybersecurity risk governance and strategy. Below we outline the initial access categories used in our data and their associated definitions:

| Initial Unauthorized Access Mechanism | Definition |
|---|---|
| Social Engineering | Researching victims to understand them socially (profession, age, gender, and so on) and then using this social information to improve attack tactics. Common attack types include phishing, vishing, or deep fakes.15 |
| Credential Reuse | The use of legitimate compromised user credentials (username, password, and so on) to breach a network or system. Examples include brute forcing, credential stuffing, or OS credential dumping.16 |
| Known Vulnerabilities | A specific weakness in a system which threat actors can use to exploit a victim's deployment in that system.17 |

15 Insikt Group, "Threat Intelligence Glossary." https://support.recordedfuture.com/hc/en-us/articles/115003274173-Threat-Intelligence-Glossary

16 Mitre, "Tactic: Credential Access", https://attack.mitre.org/tactics/TA0006/

17 Insikt Group, "Threat Intelligence Glossary"

| Initial Unauthorized Access Mechanism | Definition |
|---|---|
| Zero-Day Vulnerabilities | An exploit disclosed publicly without prior notification to developers of affected software.18 |
| Misconfigurations | Using security controls that are incorrectly configured or left insecure to gain access into a system.19 |
| Protocol Hijacking | The malicious takeover of internet infrastructure (DNS/BGP) causing traffic misdirection.20 |
| Physical Tampering | Stealing, hiding, altering, or otherwise physically changing the state of the data or system of an organization. |
| Rogue Employee | An employee (or former employee) of an organization who breaks rules and policies by exploiting their access to a company's system. |
| General Unauthorized Access | Any logical or physical access gained without permission to the network, system, application, or other resource.21 |

### *Brief Overview of Initial Unauthorized Access Vectors*

Just like with loss events, we assessed the counts of initial unauthorized access events that are tied to financial loss (since we were not always able to associate a financial loss amount with all of our cyber events). The table below summarizes the top initial access categories that resulted in some amount of financial loss.

| Top Initial Unauthorized Access With Financial Loss | |
|---|---|
| **Initial Unauthorized Access Mechanism** | **Count** |
| Vulnerabilities | 158 |
| General Unauthorized Access | 114 |
| Social Engineering | 75 |
| Credential Reuse | 39 |
| Misconfiguration(s) | 28 |
| Physical Tampering | 18 |
| Rogue Employee | 14 |
| Protocol Hijacking | 4 |

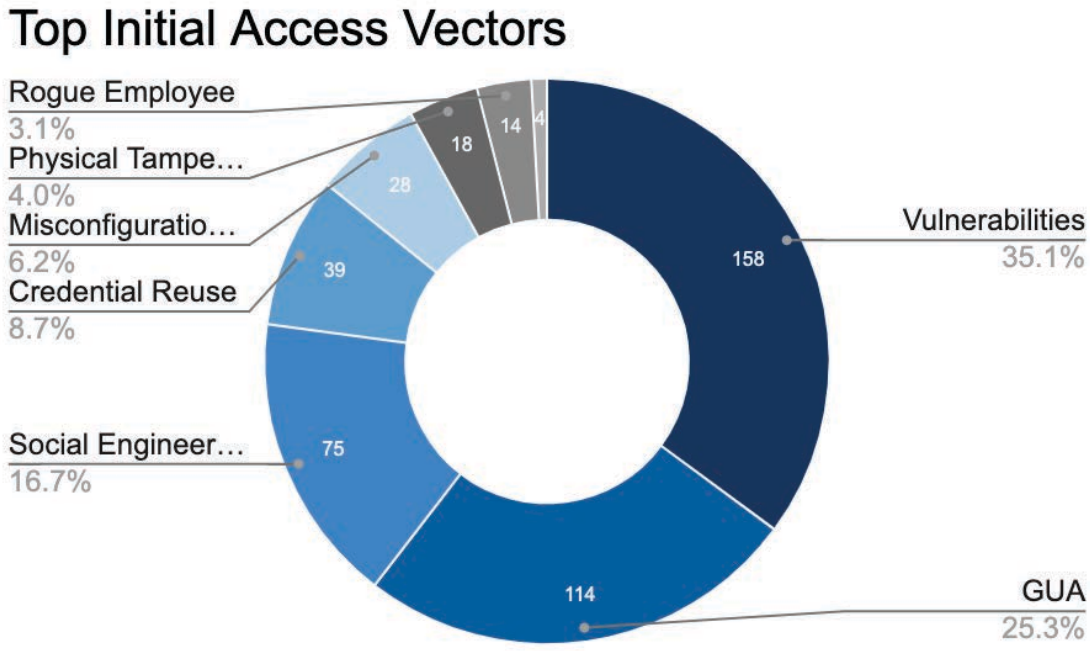
18 Insikt Group, "Threat Intelligence Glossary"

19 Nist, "Computer Security Resource Center", https://csrc.nist.gov/glossary/term/misconfiguration

20 https://csrc.nist.gov/glossary/term/protocol

21 https://csrc.nist.gov/glossary/term/unauthorized_access

**Vulnerabilities** (known and zero day) and **general unauthorized access (GUA)** were the top initial access mechanisms respectively with associated financial losses. Often, a finding of general unauthorized access can be attributed to uncertainty about the true nature of the initial access vector. We observed 114 cases of GUA tied to financial loss, which speaks to the complexity and ambiguity surrounding initial access. Social engineering and credential reuse were the third and fourth most prevalent initial access vectors respectively. The least common method for hackers to gain unauthorized access to a system/network initially was via protocol hijacking.




## Brief Industry Analysis

When sorting our data by industry, it becomes even more evident that the social costs of a network breach are not adequately captured by traditional financial analysis. We focused on three industries — finance, healthcare, and industrials — which regularly handle troves of sensitive data, are critical to supply chains and economic infrastructure, and suffer the brunt of reputational and external costs associated with poor social governance strategy should they suffer data breaches.[22] These three industries also have a dimension of social responsibility in that they all affect citizens at scale and play a significant role in our day-to-day lives.

Across all industry verticals, industrials suffered the largest average loss amount: **$15.2 million**.

Although the healthcare industry had the highest count of breaches with a confirmed loss amount, it had one of the lowest average loss amounts at **$1 million**. Given the social sensitivity of the private medical data that permeates the healthcare industry, this is an excellent example of how traditional financial analysis metrics fail to capture the true cost of a breach.

22 https://securityintelligence.com/posts/threat-actors-targeted-industries-2020-finance-manufacturing-energy/

According to SecurityIntelligence reporting, banking and financial services are identified as the second most costly industries hurt by data breaches.[23] Following a data breach, our data set found that the financial industry ranks firmly in the upper echelon of industries when sorted by the size of financial loss incurred. However, with demand for remote banking and services on the rise, coupled with the uptick in leaked credentials and credit card fraud, the finance industry is certainly a sector that will continue to be vulnerable to costly breaches as firms push digitalization.[24] The table below summarizes the average loss amounts from data breaches across all industries.

| Industry | Median of Loss Amount ($) | Count of Industry |
|---|---|---|
| Industrials | $15,200,000 | 22 |
| Energy | $10,600,000 | 5 |
| Consumer Staples | $4,662,500 | 17 |
| Information Technology | $4,625,000 | 54 |
| Finance | $2,750,000 | 63 |
| Government | $2,700,000 | 3 |
| Real Estate | $1,500,000 | 2 |
| Consumer Discretionary | $1,339,481 | 41 |
| Healthcare | $1,020,000 | 117 |
| Services | $457,059 | 74 |
| Communication Services | $300,000 | 15 |

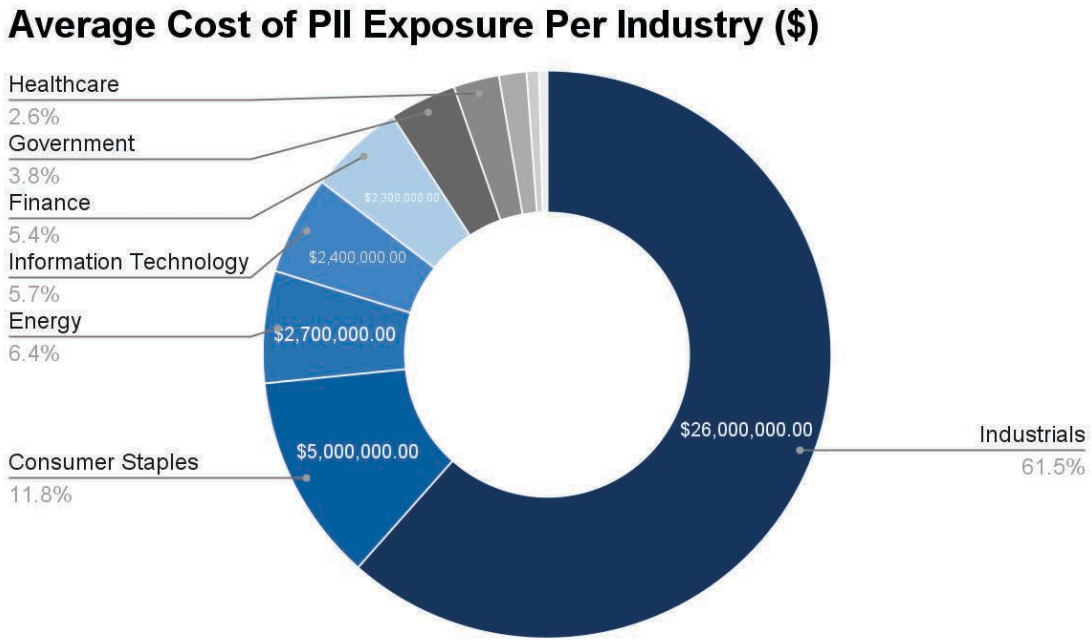
### *Industry Verticals — Loss Events*

We observed further complexity when we sorted the financial loss within each industry by loss event type. Certain industries experienced different amounts of financial loss, dependent on the type of loss event at hand. This reflects the wide range of stakeholders subjected to the costs of a breach in different industries. For example, the theft of PII carries a higher social cost in the healthcare industry, where the PII gathered by organizations is much more sensitive than that of, say, firms selling consumer discretionary goods, as well as regulated by HIPAA, which exposes firms to regulatory penalties. Indeed, dissecting the industry verticals by loss event type reveals the shortcomings of the traditional financial approach to assessing cyber risk.

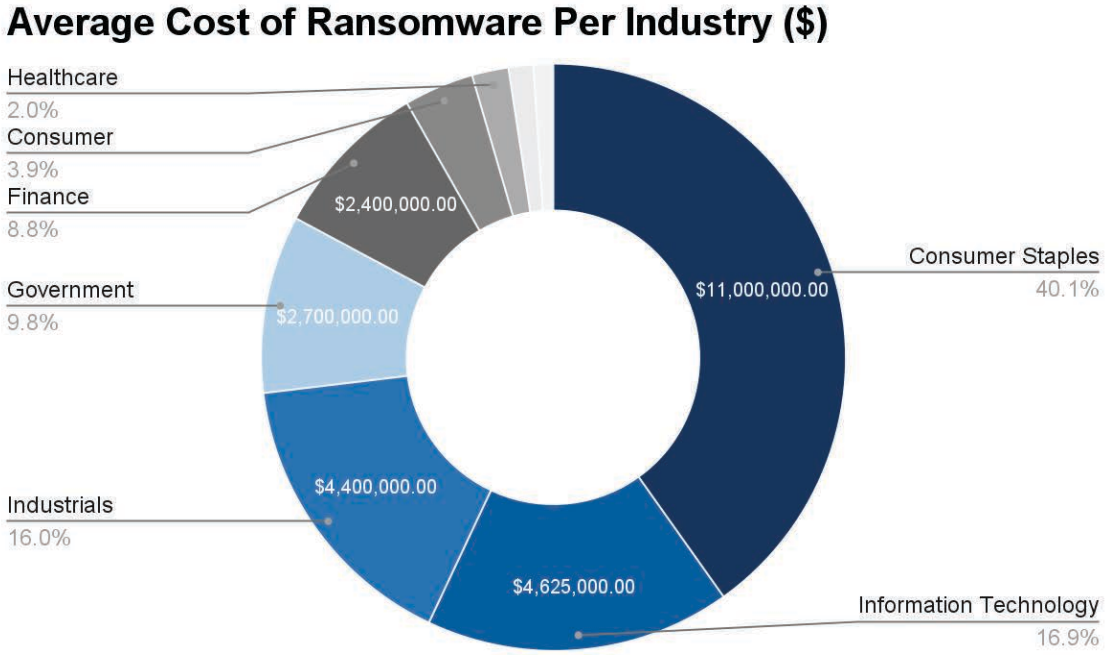
For example, industrials suffered the highest financial loss from PII exposure in particular, at an average loss of $28 million. Although the energy industry experienced one of the highest overall financial losses, it only experienced an average loss of $2.7 million through PII exposure. The pie chart below visualizes the differences across industries pertaining to financial loss for PII exposure.

23 https://securityintelligence.com/articles/banking-finance-data-breach-costs-risks/

24 https://securityintelligence.com/articles/banking-finance-data-breach-costs-risks/




Consumer staples experienced the highest loss average when it came to ransomware, at **$11 million** per ransomware breach. This industry encompasses non-cyclical goods that are needed year-round, such as foods and beverages, household goods, and personal products.[25] Following consumer staples, information technology and industrials had similarly high average losses associated with ransomware, **$2.4 million** and **$2.7 million** respectively per incident.




25 https://www.investopedia.com/terms/c/consumerstaples.asp

Given the increasing frequency that threat actors combine ransomware attacks with sensitive healthcare information harvesting, it may come as a surprise that the healthcare industry ranks relatively low in terms of financial loss.26 However, once again we stress that the figures in our data are produced solely from a financial loss standpoint. The costs associated with operational outages, restoring from backups, and reputational fallout (all common byproducts of ransomware attacks) are not factored into our loss amounts.

Once again, we compare our data to other reports that do factor in some hidden costs to reveal the difference in loss amounts. According to IBM, the typical cost of a healthcare breach rose to $9.4 million in 2021, $2 million more than the previous year.27 Recorded Future reporting identifies ransomware as a top threat currently facing the healthcare industry.28 In our data, the healthcare industry only comprises 2% of all financial losses associated with ransomware. However, it is essential to note that ransom payments are not always disclosed. Additionally, personal data theft, which could be used for future monetization opportunities, lacks a uniform standard for quantified loss. From the industry level to individual firms, a purely financial approach to assessing loss fails to reveal the true cost of network breaches.

An additional loss event that has become more prominent in recent years is business email compromise (BEC). We did not create a specific category for this social engineering attack, instead categorizing it under the umbrella of financial fraud. We did, however, note when this specific loss event occurred. Across all financial fraud we recorded, 14% were specifically tied to successful BEC campaigns.29 The Record notes that factors such as the COVID-19 pandemic, advanced phishing tactics, and the use of cryptocurrency have all contributed to BEC proliferation30, while a 2022 FBI report estimated that BEC drove over $43 billion in losses over the last five years. In our own data, financial fraud cost an average of $1.9 million across all industries. For the financial sector specifically, financial fraud cost firms an average of $6.9 million. This elevated figure may be attributed to the 57 loss event instances (a relatively low sample size).

### *Why Did Our Data Yield Low Average Loss Amounts?*

Reviewing the loss figures tied to the attack vectors and loss events in our data is underwhelming. The picture becomes even less clear when we compare our data to previous reporting on cyber breaches. Singling out individual industries only underscores the point that financial losses fail to capture the full impact of negative externalities from breaches. Self-reported financial losses are notoriously difficult to verify, allowing for breach cost obfuscation. The past 7 years of public reporting on cyber breaches was decided largely by internal corporate stakeholders, since there were few defined regulatory guidelines on public disclosure requirements. Moreover, concrete numbers for loss amounts are rare, and the numbers that are available are often clouded by ambiguity about certain aspects of the breach or the loss event. Even those most informed about a cyber event often lack a clear understanding of the financial loss associated with the breach. As a result, the harm caused by operational disruption and the breach itself ends up being largely underestimated.31

---

26 Insikt Group asserts that healthcare entities have been "disproportionately impacted" by ransomware attacks in the past couple of years, as threat actors exploit COVID-19 to create coronavirus-related campaigns and domain infrastructure. Source: https://support.recordedfuture.com/hc/en-us/articles/360045157834--Threats-to-the-Healthcare-Sector-Amid-Global-COVID-19-Pandemic.

27 IBM, "Cost of a Data Breach 2021" report

28 https://support.recordedfuture.com/hc/en-us/articles/360045157834--Threats-to-the-Healthcare-Sector-Amid-Global-COVID-19-Pandemic

29 Of all 57 financial fraud events, 8 of them were specified as BEC scams. (8/57 = ~0.14)

30 https://therecord.media/fbi-business-email-compromise-attacks-led-to-more-than-43-billion-in-losses-since-2016/

31 https://www.sungardas.com/en-us/blog/the-consequences-of-a-cyber-security-breach/

The extended timeline of cyber events presents another challenge to properly contextualizing our data set. Companies report direct financial losses from a network breach, only to face regulatory penalties or class action lawsuits years later. For example, UK-based multinational firm Dixons Carphone suffered a breach stemming from server vulnerabilities between July 2017 and April 2018. Dixons did not disclose the related financial fraud and PII exposure until June 2018.32 It was not until January 2020 that the UK's Information Commissioner's Office (ICO) levied a regulatory penalty of £500,000 on the UK conglomerate.33 Between the 9-month period where the malicious software went undetected and the lengthy legal processes, Dixons is an example of a larger trend where companies are susceptible to protracted timelines before a complete financial loss disposition is achieved. The timeline below illustrates the segmented, extended life cycle of a network breach and its associated costs. Given this pace of regulatory regimes and legal enforcement, it should come as no surprise that quarterly and annual financial reporting fails to capture the full scope of loss and risk stemming from network breaches.

Time and time again, network breaches incur significant external costs that financial loss analysis fails to fully articulate. This is due to a variety of factors, including extended timelines, a lack of regulatory regime, and amorphous operation outages. This dynamic necessitates a new, more comprehensive approach for analyzing risk.

32 https://www.theguardian.com/business/2020/jan/09/dixons-carphone-fined-500000-for-massive-data-breach

33 https://www.theguardian.com/business/2020/jan/09/dixons-carphone-fined-500000-for-massive-data-breach

# A Risk-Based, Analytical Approach: The New Standard

Cyberattacks pose a growing threat to the industries we depend on to sustain our way of life, as evidenced by the aftermath of cyberattacks triggering extended outages in critical energy sectors, disrupting food supply chains, and enabling bank fraud from financial institutions. Not only are cyberattacks crippling society's critical sectors and challenging social stability, but they are becoming increasingly easy to accomplish. Cybercriminals have access to underground markets, advanced technology, cross-collaboration, even sometimes state-backed resources. The increasing scale of potential cost emanating from cyberspace looms over governments and regulatory bodies as they consider the first tranche of cybersecurity-specific legislation.

As a result, cybersecurity regulation in Western markets is at an inflection point. Misalignment between the significant capabilities of threat actors and the lackluster incentives for firms to institute strong cyber risk controls has created an environment where social costs outweigh financial costs. However, this is likely to change in the immediate and near-term future as regulators attempt to catch up by levying larger fines for poor cyber controls. As we saw in our data outlined above, the current cyber risk approach fails to mitigate the cost of a breach for companies and stakeholders alike. This dynamic, in concert with rising consumer awareness of data and privacy issues34, points to change on the horizon.

A competitive advantage can be generated from a proactive data governance strategy that emphasizes stronger cyber risk mitigation strategies. A stakeholder-conscientious approach presents a keen awareness of the escalating cyber climate, and builds trust with a diverse public audience, from consumers to regulators. It is no longer enough for compliance to be a responsive check-the-box exercise. Instead, a risk-based, analytical approach that exceeds present compliance frameworks will be the new standard in cybersecurity governance.

To start illustrating the competitive advantage of a risk-based approach to cybersecurity, we start by outlining shifting expectations as they are codified in regulatory frameworks. Even within compliance frameworks, the effects on a variety of stakeholders, rather than just shareholders, is being considered, often for the first time. We believe two trends are emerging in the legal ecosystem that place renewed emphasis on cybersecurity and risk management: more stringent reporting requirements, and increasingly punitive fines for data privacy violations. Aware that cybersecurity threats are currently outpacing mitigation strategies, governments and international regulators are looking at cybersecurity as an area that demands a stricter set of guidelines. We will start by taking a closer look at some of these guidelines to build a better understanding of this rapidly evolving legislative landscape.

34 https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative

### Stringent Reporting Requirements

In the European Union, the General Data Protection Regulation (GDPR) regulates digital privacy and defense. The GDPR requires that companies disclose breaches to the individual EU state's supervisory authority without "undue delay", and where feasible within 72 hours after becoming aware of an incident.35 The content of the notification is also regulated under GDPR. The notification itself must contain a description of the nature of the breach, likely consequences of the breach, the contact details of the relevant data protection authority, and measures taken or proposed by the controller to mitigate the damage caused by the breach.36 Every notification must prove that proper controls were in place before the breach to avoid hefty EU fines. This common reporting standard sets an expectation that companies disclose all-encompassing details of breach. Like all frameworks, GDPR is a work in progress, as legislators continue to discuss how reporting can be enforced and standardized across companies of various sizes and maturities.37 However, the GDPR has been considered a successful overarching reporting mechanism that holds EU states accountable for providing concrete, timely notifications to shareholders affected by cyber events.

The United States government is also beginning to demand greater transparency and promptness in reporting. As the public gains awareness that cyber breaches have deep implications for its personal data, it is demanding an overhaul of best practices. This puts bodies like the Federal Trade Commission, which oversees a federal approach to cyber reporting in the US, in the spotlight. Where the FTC may have taken a more vague stance in the past, recent language signals that failure to implement timely patching, and to publicly disclose and report patches, will be grounds for future legal fines.38 The more aggressive stance comes in a January 2022 Log4j vulnerability report, where the FTC stresses that companies must report their patches for Log4j and all "similar known vulnerabilities" in their systems.39 Further, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) is setting stricter limits and conditions around personal health information (PHI) in the healthcare sector. At the time of writing, HIPAA is developing new policy updates on the speed and methods by which people can access PHI, fees that may be charged for lack of transparency, and more.

One of the most significant strides in the US cybersecurity landscape came in March 2022, when the Securities and Exchange Commission (SEC) proposed a set of changes to its existing cybersecurity rules. The SEC aims to protect US investors through enforcing laws and overseeing securities markets. The proposed amendments look to "enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incident reporting by public companies."40 By proposing the amendments, the SEC signals an aim to give investors better insight on public companies' cybersecurity risk management procedures. The proposal can be separated into two main points: mandatory cybersecurity incident reporting, and obligatory disclosures on a company's risk management and governance strategy framework.

35 https://www.perkinscoie.com/en/news-insights/gdpr.html

36 https://globaldatahub.taylorwessing.com/article/data-security-and-breach-reporting-under-the-gdpr-and-nisd

37 https://www.isaca.org/resources/isaca-journal/issues/2019/volume-1/reporting-on-gdpr-compliance-to-the-board

38 https://www.lmgsecurity.com/the-latest-us-cybersecurity-regulations-crackdowns-trends/

39 https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2022/01/ftc-warns-companies-remediate-log4j-security-vulnerability

40 https://www.sec.gov/news/press-release/2022-39

The first part of the proposal would mandate companies to report a cybersecurity event no later than 4 days after the event is determined by the company to be a "material cybersecurity incident".41 The SEC outlines the criteria for materiality as information where "there is a substantial likelihood that a reasonable shareholder would consider it important" in making an investment decision, or if it would have "significantly altered the 'total mix' of information made available."42 This once again underscores how federal organizations are evolving their legislation to account for the far-reaching social effects of privacy violations and lax data management practices.

### Potentially More Punitive Fines Around Privacy Violations

As legislators begin to tackle the full scale and complexity of cyber regulation, it is becoming clear that privacy and strong data control is of central importance to a variety of stakeholders. With the ideals of social responsibility shifting attitudes in policymaking, growing concern around data responsibility is driving more punitive fines for privacy violations. Companies who fail to keep pace with regulatory changes, or fail to demonstrate due diligence, will find themselves facing even greater financial penalties in the future.43

Continuing with the amendments to the SEC's cyber rules mentioned above, one section of the proposed rules would mandate companies to give timely and accurate information on cybersecurity risk management and strategy. This proposed item relates back to the SEC's goal in providing better transparency for shareholders and investors. The requirement extends to pertinent topics such as fraud, extortion, violation of privacy laws, and reputational risk.44 When pairing enhanced cybersecurity strategies and increased incident disclosures, the SEC believes companies' "susceptibility" to cyberattacks and other incidents will ultimately decrease. Firms that fail to institute cyber controls against these types of risk will expose themselves to further risk of regulatory penalties.

As GDPR enters its fourth year, fines for privacy violations are increasing in frequency and size. In the last year, GDPR enforcement has demonstrated an emphasis on transparency, prioritizing honest and detailed security breach notices. The message is clear: Stakeholders deserve to know the exact nature and scope of a privacy violation. GDPR fines for Q3 2021 alone topped €984.47 million — a figure three times higher than the €306.3 million imposed across the entirety of 2020.45 One infamous example was the €50 million fine ($57 million) that the French National Commission on Informatics and Liberty (CNIL) imposed on Google in January 2019.46 The premise of the fine was that Google failed to provide users with transparent information regarding the use of their personal data. Where in the past, tech giants like Google, Facebook, and Microsoft may have been able to write their own data use policies, GDPR is setting a new, stricter standard for data privacy laws.

41 https://www.sec.gov/rules/proposed/2022/33-11038.pdf

42 Ibid

43 According to the GDPR Fines and Data Breach Survey by International law firm DLA Piper, fines increased nearly sevenfold from January 2021 in the EU, to USD 1.2 billion. https://www.dlapiper.com/en/us/insights/publications/2022/1/dla-piper-gdpr-fines-and-data-breach-survey-2022/#:~:text=Data%20protection%20supervisory%20authorities%20across,international%20law%20firm%20DLA%20Piper.

44 Ibid

45 https://finbold.com/gdpr-fines-q3-2021/

46 https://finbold.com/gdpr-fines-q3-2021/

With the UK now separate from the EU, the UK Information Commissioner's Office (ICO) has been left to develop its own privacy protections. It has certainly indicated that it plans to do so. The world took notice as British Airways was fined £20 million by the ICO when hackers harvested personal data of over 400,000 staff and customers, including banking and payment information, names, and addresses.47 The ICO also fined Uber for £385,000 and Marriott Hotels for £18.4 million, both for failing to uphold safety measures that would safeguard user privacy.48 These fines signal a no-nonsense tone for the ICO, urging other countries to take a similar approach.

Taking a look at Western societies specifically, governments and regulators are preparing to adopt a stronger posture when it comes to how firms maintain their own cybersecurity and manage their customers' data.

## Case Studies: How Poor Security Management Impacts Firm Performance

The lackluster financial reporting and future tightening of regulations are not the only reasons why an approach that focuses on present-day compliance fails firms and stakeholders alike. Where social and governance considerations are concerned, expectations for good governance extend to the "under the surface" costs of a breach, and mitigating those intangible losses beforehand to the best of a firm's abilities. To further illustrate the shortcomings of a strictly compliance-based approach, we discuss a few case studies below.

### *Ransomware: Cognizant*

Ransomware has become more prevalent over the last few years as companies all over the world suffer from locked up networks and extortion requests at the hands of criminal ransomware gangs. Within our data set, ransomware was the third most common type of loss event, with our research revealing over 120 breaches that involved a ransomware component. The frequency of ransomware attacks is rapidly increasing, with one prolific criminal group, LockBit taking credit for more than 70 ransomware incidents in May 2022 alone.49 The breach of one firm, Cognizant, stood out as particularly instructive to the multifaceted governance and financial risks that can stem from ransomware.

In April 2020, Cognizant, one of the largest publicly traded managed IT services firms in the world, disclosed that its networks had been breached and that unencrypted data had been extracted from its systems. Customer and employee drivers' licenses, Social Security numbers, and financial information were all stolen by the Maze Ransomware gang, which in turn threatened to publish the stolen, sensitive data unless Cognizant paid a significant ransom. Not only was sensitive data extracted from the firm's networks, but the ransomware also locked up the internal work from home software being used by Cognizant employees. As an IT service provider, Cognizant was also forced to reach out to its customers and advise them to disconnect from Cognizant services lest they also be breached, incurring a significant hit to the firm's reputation as a reliable provider. Additionally, Cognizant was compelled to suspend its billing systems, hurting its ability to collect on accounts receivable. These types of costs, stemming from operational downtime, reputational damage, and paying for credit monitoring for affected customers, are notoriously difficult to quantify, but by assessing the firm's SEC filings, both quarterly and annual, from the year of the breach, we can begin to glean the effect of the ransomware attack on Cognizant's bottom line.

47 https://www.lexology.com/library/detail.aspx?g=4a4818a6-2540-4582-81a7-592be99c85b2

48 https://finbold.com/gdpr-fines-q3-2021/

49 https://therecord.media/ransomware-tracker-the-latest-figures/

According to Cognizant's 10-Q quarterly report[50],

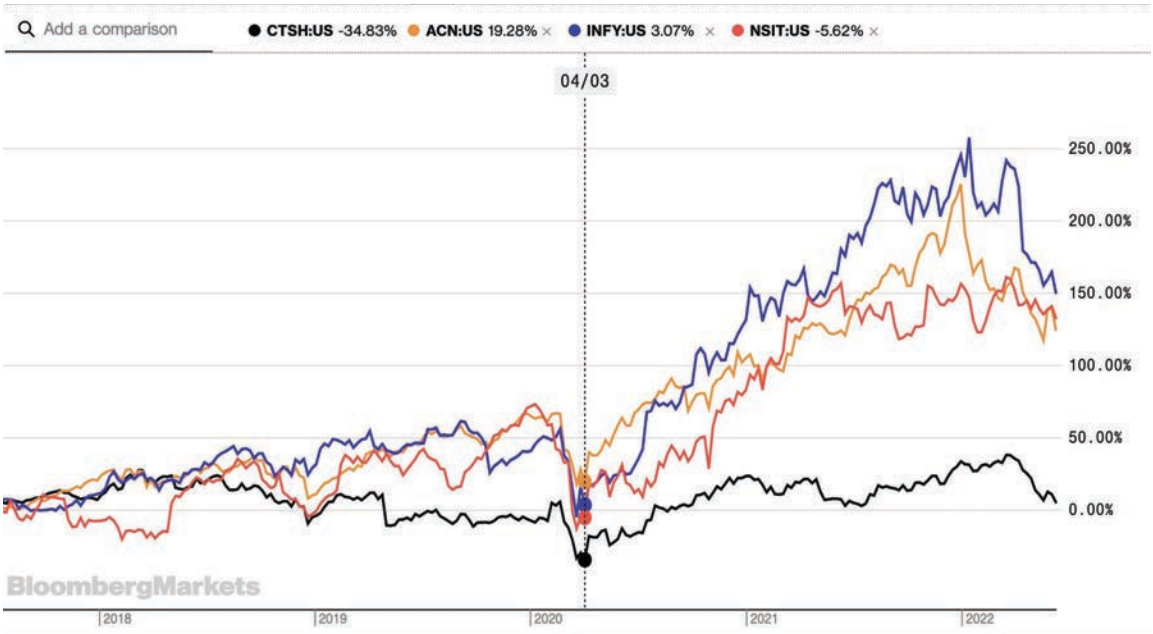
> As a result of fulfillment challenges caused by the ransomware attack, our year over year revenue growth for the second quarter was reduced by approximately 90 basis points … Additionally, in the second quarter of 2020, we incurred $24 million in costs related to the ransomware attack and we will continue to incur significant incremental costs for the remediation of the security incident and investments to enhance our overall security environment. The lost revenue and containment, investigation, remediation, legal and other costs may exceed our insurance policy limits or may not be covered by insurance at all. Other actual and potential consequences include, but are not limited to, negative publicity, reputational damage, lost trust with customers, regulatory enforcement action, litigation that could result in financial judgments or the payment of settlement amounts and disputes with insurance carriers concerning coverage.

In its 10-K annual filing[51], Cognizant disclosed even more harrowing and long-term details of the ransomware attack. While it reported that the company managed to "contain the attack," its net income fell **24%**, and the firm's revenue from business operations dropped nearly **14%**. Amid the COVID-19 pandemic and overall economic turbulence, the April 2020 ransomware attack is unlikely to be the sole cause of this financial downturn. However, it is undeniable that the original financial cost of the data breach, coupled with the post-boom losses, significantly hurt the company's ability to generate revenue for months after the original cyberattack. It remains to be seen how this ransomware attack will affect Cognizant's long-term performance, but it shows that recovery from cyber events is a lengthy process that can incorporate a broad array of financial loss.

To understand how a network breach acts as a long-term headwind in the face of a firm's overall performance, we decided to compare the performance of Cognizant's (**CTSH**) stock with its primary competitors in the industry, Accenture (**ACN**), Infosys (**INFY**), and Insight Enterprises (**NSIT**).

50 2020 Cognizant Q2 Report (10-Q) https://cognizant.q4cdn.com/123993165/files/doc_financials/2020/q2/cognizant-2q2020-10q.pdf

51 2020 Cognizant Annual Report (10-K) https://cognizant.q4cdn.com/123993165/files/doc_financials/2020/ar/385766(1)_14_Cognizant_AR_WR.pdf




While the ransomware attack is surely not the sole driver of Cognizant's underperformance, it likely played a significant role in the firm's loss of market share.

### *Credential Reuse: Uber*

Another major theme in our data set was the exploitation of credential reuse to gain unauthorized initial access into a network or system. The far-reaching repercussions of this type of technique were seen in the 2016 Uber data breach, when threat actors used stolen credentials to infiltrate Uber's network. These credentials were exposed by Uber engineers via a back-up file stored on Amazon's S3 storage service.52 The credentials to access the storage bucket had been left on GitHub, a web-based code sharing and development platform,53 where they were exposed to the public. The hacker was then easily able to view multiple Uber S3 buckets, accessing 57 million accounts of its riders and drivers around October 2016.54 Once credentials were accessed by the hacker, they used credential stuffing to escalate privileges into the network. This means compromised username and password pairs were injected into websites until they matched with an existing account.

Perhaps even worse than the breach itself was the way that Uber mishandled the outcome. The breach was only disclosed in November 2017, after Uber attempted a cover-up. The then-CEO sought to pay off the hackers by funneling the payoff through a bug bounty program, which arranges payment to hackers who point out security issues without actually compromising data.55 Once the details of the breach and cover-up became public, the real pain for Uber began. The loss of business, reputational damage, and fines increased the already hefty financial costs of the breach. Multiple lawsuits against Uber were filed in the US and Europe, including a $148 million settlement reached with all 50 US states in September 2018.56

52 https://www.cnbc.com/2018/11/27/uber-fined-more-than-1-million-dollars-by-uk-and-dutch-authorities.html.

53 https://www.bankinfosecurity.com/uber-fined-12-million-by-eu-for-breach-disclosure-delay-a-11730 (code repo collection/alerting)

54 https://www.databreachtoday.com/uber-no-justification-for-breach-cover-up-a-10637

55 https://www.bankinfosecurity.com/uber-fined-12-million-by-eu-for-breach-disclosure-delay-a-11730

56 https://www.reuters.com/article/us-uber-databreach/uber-to-pay-148-million-to-settle-data-breach-cover-up-with-u-s-states-idUSKCN1M62AJ

### *Class-Action Lawsuits: Capital One Financial Corporation*

Litigation fees are another added expense not always considered in a simplistic financial-loss approach to assessing cyber risk. According to research done by senior policy researcher Sasha Romansky, lawsuits regarding privacy violations have been increasing dramatically since 2005, and especially since 2009.[57] The reality of cyber breaches is that the actual breach is just the beginning — the litigation fees are where the true consequences of privacy and data fallout are brought to bear.

The Capital One Financial Corporation data breach provides an example of large amounts of financial loss due to both regulatory penalties and class action lawsuits. In July 2019, the company disclosed that the personally identifiable information (PII) of over 100 million individuals was illegally obtained by an unknown threat actor. The FBI found that the threat actor gained access through a misconfiguration of a firewall on a web application.[58] According to court documents, 140,000 Social Security numbers and 80,000 bank account numbers were stolen in the breach.[59] Other data, including "credit scores, credit card limits, credit card balances, credit card payment history, and fragments of transaction data", was also stolen in periods from 2016 through 2018.[60]

The data breach led to significant financial losses for Capital One. The US Office of the Comptroller of the Currency (OCC) placed an **$80 million** fine on the company, "based on the bank's failure to establish effective risk assessment processes" as well as the firm's "failure to correct the deficiencies in a timely manner."[61] Concurrently, Capital One faced a large class-action lawsuit from affected customers. In December of 2021, the company would ultimately agree to settle the lawsuit for **$190 million**.[62] The combined loss figures, when adding together the OCC penalty and the class-action lawsuit settlement, totaled **$270 million**.

The litigation surrounding the Capital One breach, in concert with the regulatory penalty, combined to accrue significant financial losses to the firm. However, this is only a single instance of network breach-related litigation costs. Zooming out to assess the overall landscape of breach-related lawsuits reveals a landscape increasingly fraught with risk for firms with each passing year. Privacy and data related lawsuits are occurring more frequently, with only 7 occurring in 2006 but "increasing dramatically … since 2009, reaching as many as 150 suits per year [in 2014]"[63]. Indeed, the majority of all lawsuits related to cyber breaches are civil actions filed in federal courts[64] — pointing to the ever increasing likelihood that consumers whose data has been compromised will seek legal redress from the firms that failed to institute proper cybersecurity controls. Taken as a whole, the Capital One breach and subsequent lawsuit points to the significant legal risk taken on by firms that neglect cybersecurity investment, and the expanding likelihood of privacy litigation in turn illuminates a significant source of risk for companies around the world.

---

57 Romansky, "Examining the cost and causes of cyber incidents"

58 https://www.nytimes.com/2019/07/29/business/capital-one-data-breach-hacked.html

59 https://www.reuters.com/article/us-usa-banks-capital-one-fin/capital-one-to-pay-80-million-fine-after-data-breach-idUSKCN2522DA

60 https://bergermontague.com/wp-content/uploads/2021/05/09-Capital-One-Second-Amended-Representative-Complaint-10-23-20.pdf

61 https://www.washingtonpost.com/national-security/capital-one-fined-2019-hack/2020/08/06/90c2c836-d7f3-11ea-aff6-220dd3a14741_story.html

62 https://www.seattletimes.com/business/capital-one-to-pay-190m-settlement-in-data-breach-linked-to-seattle-woman/

63 Romansky, "Examining the cost and causes of cyber incidents"

64 Ibid.

# Most Common Causes of Security Events

### Solving for Legal Compliance Doesn't Necessarily Equal Good Governance

The prevailing wisdom supposes that it is sufficient due diligence to satisfy best practices as determined by a majority of competitors within the industry. In other words, it is just important to meet the status quo of compliance measures, and no more or no less than that amount. This common practice acts as a hindrance for novel, preemptive policies and practices in the cybersecurity space. And yet companies around the world are scoring extremely well on compliance but still suffering from cyberattacks. This existing pattern reveals the harsh reality: There are several flaws with the "legal compliance" logic that deems it an inadequate framework for a risk-based, analytical approach to cybersecurity.

First, treating cybersecurity as a "check-the-box" exercise underestimates the potential for security events that introduce operational risks that exceed regulatory compliance. Although an organization measures well on compliance, a security event could still cause major financial losses. There are countless examples of companies scoring well on compliance yet still being hit with devastating data breaches with harmful ripple effects to stakeholders and the market at large.

Another issue with the due diligence approach is that cyber policies are becoming less reliable for overarching coverage. As cyberattacks become more costly and common, improved policy articulation on covered events will likely bump up out-of-pocket costs for organizations themselves. Especially with the emergence of ransomware as a service (RaaS) as a successful monetization model for cybercriminals, the insurance market is tightening its approach to coverage. Insikt Group identifies ransomware as a "commoditized market", wherein the average ransom demanded of a company is 0.15% of the victim's annual revenue numbers.65 With ransomware evolving into an increasingly prevalent business model, it will become much more difficult for companies to write and maintain policies that do not have specific terms for ransomware.66 Even aside from ransomware, mounting insurance industry losses are driving the insurance market to aggressively contract as insurers exit the market.67 As the rising costs to insurance companies jostle many insurance firms out of the market, underwriting will become a common mitigation strategy for the insurance companies still available.68 Underwriters will likely demand detailed proof of clients' cybersecurity measures and procedures in more ways than ever before. Companies must adjust sooner rather than later to adopting more stringent policies to mitigate costly cyber risk.

Finally, the due diligence approach hardly accounts for black swan events, or rare and difficult to predict yet disproportionately consequential events. The legal compliance frameworks (and therefore the companies who subscribe to them as well) assume that these high profile and costly cyberattacks are too rare to be concerned about. However, people are generally terrible at estimating "likelihood of occurrence," meaning black swan events occur much more frequently than our bias leads us to believe. The big-name cyber events like Wannacry, Notpetya, and SolarWinds have all happened within a relatively short, and recent, window of time. It is impossible to predict when exactly the next black swan event will happen, but with the level of interconnectedness and digital dependence in today's economy, it is inevitable. Excluding black swan events from any cyber policies is a logical non sequitur, and it means that when these events occur, the effects are even more devastating and far-reaching.

65 https://www.recordedfuture.com/2021-malware-and-ttp-threat-landscape/ , p.6

66 https://doi.org/doi:10.7282/t3-cqb3-4741

67 Gundert, "New Cyber Insurance Model" https://www.recordedfuture.com/new-cyber-insurance-model-continuous-control-validation/

68 Levi's book

# The Competitive Advantage of a Stakeholder Approach

With the shifting regulatory landscape in mind, coupled with an understanding that legal regulations are only the beginning of what it takes to create a robust cybersecurity program, it becomes clear that companies must take proactive steps for better cyber risk controls. As previously stated, it is no longer enough for compliance to be a responsive, status quo exercise. Instead, an approach that exceeds present compliance frameworks sets the new standard in cybersecurity governance. Proactively adopting social and governance frameworks in tune with standards will generate a competitive advantage, due to a fully accounting for stakeholders in an interconnected, real-time business environment where reputation plays a massive part in a firm's bottom line.

### Reputation Management in the Social Media Landscape

The rising influence of consumers and stakeholder behavior can be partially attributed to the rise in social media, and the voice it gives to users all over the world. The emergence of social media as a valid tool for business management points to several opportunities, but also threats, for a firm's reputation. Users can easily edit, share, and circulate content with vast numbers of people in seconds. If a company is seen acting in ways that violate stakeholder criteria, users can easily take to social media platforms to vocalize their dissatisfaction. When companies suffer a breach, and especially if they attempt to obfuscate the true nature of the breach, they lose credibility in the eyes of the public. This social currency is difficult to build up but extremely easy to lose in a competitive marketplace with safer and more secure alternatives.69 Social media presents a way for stakeholders to band together and hold companies accountable for upholding safe cybersecurity practices. Meanwhile, for companies this means that factoring in cybersecurity to stakeholder-centric initiatives is more important than ever.

Even ransomware operators pay attention to reputation, both their own and the ways that they can weaponize the power of reputation to coerce company targets into paying ransoms. For example, RansomHouse Group, a cybercrime operation emerging in December 2021, openly shames companies on their website whose networks they have managed to infiltrate.70 Similarly, the ransomware group Industrial Spy, active in early June 2022, posted their ransom notes on their victims' public-facing websites, enabling virtually anyone to see that the company was compromised. These name-and-shame tactics have greater weight in a social media landscape than ever before. Even within underground forums, ransomware operators rely on their reputation to generate sales, or else the credentials and other exfiltrated information receives little attention from buyers. Reputation, whether it pertains to legitimate or illegitimate business models, has a place in generating favor in the eyes of the public.

69 https://www.itpro.co.uk/security/data-breaches/357941/how-much-will-a-data-breach-really-damage-your-organisations

70 https://www.bleepingcomputer.com/news/security/new-ransomhouse-group-sets-up-extortion-market-adds-first-victims/

## The Business Case

The competitive advantage of robust cyber risk control rests on the superiority of a proactive, rather than reactive, approach to gaining customers and market share. Strong cyber risk control allows the firm to look forward into the future, using their human, technological, and financial resources to improve internal processes, innovate new products, and upsell to existing customers. On the other hand, lax cyber risk management forces firms to adopt a reactive posture.

A cyber breach is much more likely to occur under conditions of bad cyber risk management, and the costs associated with such a breach can be long lasting and substantial, as we have outlined in the case studies above. On top of paying for credit monitoring, incident response, and even potential fines and legal fees, customer retention may become more difficult and churn may increase. Trust is an essential component of any business transaction, and a breach may damage your reputation as a trustworthy partner to both the firm's customers and vendors. Protecting intellectual property and proprietary business information can also help maintain a firm's competitive advantage. A network breach could degrade a firm's ability to compete if it results in an adversary or competitor gaining access to this type of information, and indeed, in 2012, NSA Chief Keith Alexander asserted that the loss of industrial information and intellectual property through cyber espionage constitutes the "greatest transfer of wealth in history" with US companies losing over an estimated $250 billion to intellectual property theft propagated through hacks and network breaches. Effective cyber risk controls can prevent this type of drag on the firm's competitive advantage and allow its most important resources — human, technological, and financial — to remain proactive and focused on serving customers and beating competitors in the open market.

# Conclusion

Our data set of over 400 network breaches revealed a bevy of below-the-surface costs stemming from a cyberattack. These externalities include reputational harm, legal and regulatory penalties, and operational downtime, to name a few. All of these externalities hurt a firm's ability to compete for market share following a cyberattack. A traditional means of assessing financial returns on cyber investment fails to capture these nuanced, dynamic, and sometimes long-term losses that firms incur. Today's business environment demands a dynamic risk framework that can accurately identify all facets of financial loss and codify commitments to contemporary social and governance standards. We advocate for the utility of social and governance metrics in guiding organizations' approaches to calculating and managing cyber risk.

Organizations daily face increasing negative externalities that act as headwinds to proactive strategic management and financial growth. Cyber risk stands out as one of the most prominent and wide-ranging of these external threats to firms. The potential for direct and indirect costs stemming from network breaches is ever present, and firms must be prepared to institute thoughtful cyber risk controls in order to mitigate such costs. A breached network can affect a broad range of firm stakeholders, from customers, to vendors, to employees. A more comprehensive model of cyber risk analysis that transcends traditional financial risk is a better method for properly assessing how a breach will affect the ability of a firm to compete for market share. A dynamic risk framework that emphasizes stakeholders can more accurately identify all potential vectors of financial loss and codify the investment in cyber risk management. We highlight that social and governance considerations are useful in an environment characterized by rapid market and regulatory changes.

In addition to the shifting expectations as they are codified in regulatory frameworks, we underscored the competitive advantage that can be generated by adopting a proactive data governance strategy that emphasizes stronger cyber risk mitigation strategies. We used case studies to underscore the shortcomings of a strictly compliance-based approach, and the social and economic fallout that companies have suffered when compliance is a check-the-box exercise. We also highlight some of the logical fallacies with a due diligence approach, touching on shortcomings of bandwagoning behavior in the marketplace, cyber insurance, and the misleading notion of black swan events. Our data, case studies, and the high-level trends we drew out all point to one common theme: The cyber risk framework that best suits the modern threat landscape exceeds legal compliance and evaluates harm to multiple stakeholders.

Anna Iskenderian is a Threat Intelligence Analyst on Insikt Group at Recorded Future. She earned her Bachelors of Arts in International Relations at American University, and lives in Boston, Massachusetts.

Jesse Nuese served as an infantryman and a paratrooper in the US Army for four years, before separating from the service to pursue an education. He completed one year at Community College of Denver before transferring to Columbia University, which he graduated from in 2021 with a BA in International Affairs and a focus on US-China relations. He is currently a graduate student at the Fletcher School of Law and Diplomacy of Tufts University, where he studies International Business with an emphasis on Strategic Management, Finance, and Cybersecurity. He also serves as a Senior Business Fellow with the Warrior Scholar Project.

Jakob Wolk is a graduate student at New York University, pursuing a Master of Science in Global Affairs with a concentration in Transnational Security. He graduated magna cum laude from Arizona State University with a B.S. in Political Science.

Levi Gundert is the Senior Vice President of Global Intelligence at Recorded Future, where he leads the continuous effort to measurably decrease operational risk for clients. Levi has spent the past 20 years in both the public and private sector, defending networks, arresting international criminals, and uncovering nation-state adversaries. He's held senior information security leadership positions across technology and financial startups and enterprises. He is a trusted risk advisor to Fortune-500 companies, and a prolific speaker, blogger, and columnist.