# How informative are cybersecurity risk disclosures? Empirical analysis of firms targeted by ransomware

Matthew Adams* and Tyler Moore
School of Cyber Studies
College of Engineering and Computer Science
The University of Tulsa
800 South Tucker Drive, Tulsa, Oklahoma 74104 USA
mla5406@utulsa.edu, tyler-moore@utulsa.edu

July 2025

**Abstract**

Public companies face escalating requirements to disclose cybersecurity risks and damages in regulatory filings. In theory, such disclosures should equip investors with knowledge required to make informed decisions, while also encouraging firms to adopt more robust strategies for managing cybersecurity risks. In practice, discussions are often embedded in disparate locations of long documents full of legalese, which hinders systematic examination. This paper examines the regulatory filings of 61 firms that experienced ransomware incidents between 2018 and 2021. We describe a process whereby 7,681 cyber-related statements were extracted from 314 10-K filings between 2018–23, then categorized using an iterative process inspired by grounded theory. We then perform quantitative and qualitative analysis of the statements, examining how firms discuss cybersecurity before and after experiencing an incident.

***Keywords—*** Cybersecurity metrics, security economics, cybersecurity regulation, 10-K disclosure

# 1 Introduction

Cybersecurity presents an important and growing risk for firms of all sizes. Cyber incidents have been shown to significantly affect firm financial stability (Gao et al., 2020; Schlackl et al., 2022; Woods and Böhme, 2021; Zhang and Smith, 2023), customer retention (W. Li et al., 2023; Woods and Böhme, 2021), and reputation (Gao et al., 2020; W. Li et al., 2023). Researchers agree that incidents continue to escalate in frequency (Eling et al., 2023; W. Li et al., 2023; Romanosky, 2016; Schlackl et al., 2022).

Against that backdrop, it is no surprise that investors and regulators are interested in improving how firm-level cybersecurity risks are presented and evaluated. Over the past decade and a half, the U.S. Securities and Exchange Commission (SEC) has placed increasingly substantial obligations on publicly-traded firms to

*Corresponding author.

Citation: Matthew Adams and Tyler Moore. How informative are cybersecurity risk disclosures? Empirical analysis of firms targeted by ransomware. *Computers & Security* (forthcoming), 2025.

disclose material cybersecurity risks and incidents. The rationale behind such regulatory action is to reduce information asymmetries by ensuring firms disclose substantial risks that might otherwise remain hidden from view. By doing such, investors are better able to assess risk, hopefully leading to the reallocation of capital towards more secure firms. Ideally, increased transparency should also encourage firms to improve their cybersecurity posture in order to better align with market expectations.

The efforts began in 2011 when the SEC released guidance clarifying that existing rules to disclose material risks in annual 10-K filings also cover cybersecurity risks (U.S. Securities and Exchange Commission, 2011). The guidance was expanded in 2018 (U.S. Securities and Exchange Commission, 2018), further specifying when and how cyber incidents and risks should be disclosed (Gao et al., 2020; H. Li, No, and Boritz, 2020). This regulation, along with an increase in cybersecurity risk, has had a noticeable effect on the increasing number of firms discussing cybersecurity risks within 'Item 1A', a section dedicated to the discussion of risk factors faced by the company (Gao et al., 2020). Most recently, the SEC issued a rule that led to the creation of 'Item 1C' in the annual 10-K filings, a section where companies are required to mention their risk management and governance policies related to cybersecurity (Katz and McIntosh, 2025; U.S. Securities and Exchange Commission, 2023, July). Item 1C became mandatory for all public companies starting in December 2023 (U.S. Securities and Exchange Commission, 2023, July).

What has the effect been of these growing disclosure requirements? Research suggests that such regulatory pressure, without rigid requirements, has resulted in declining levels of valuable information (H. Li, No, and Wang, 2018; Nelson and Pritchard, 2016). On the other hand, we know from other empirical research that proactive security investment results in fewer incidents (Gandal et al., 2023; Kwon and Johnson, 2014). Firms that proactively report the strategies they employ to mitigate cybersecurity incidents demonstrate transparency regarding the damages suffered from an incident, the loss of value caused by it, and the costs incurred to resolve it. They outline the steps they took in reaction to suffering an incident to minimize the compromise, providing useful information to investors and regulators. In this paper, we argue that statements made in regulatory filings can be used to measure cybersecurity posture at the firm level. In particular, we can deduce from the reports the degree of preparedness, transparency, and informativeness regarding the disclosure of cybersecurity incidents and mitigation strategies.

This firm-level behavior increasingly aligns with evolving regulatory expectations. The SEC's 2018 disclosure guidance, as well as changing guidance requirements and guidance from other regulators and stock exchanges, highlight the importance of transparent cybersecurity disclosure (Peng and C.-W. Li, 2022). Higher-quality disclosure can mitigate information asymmetries and, according to Campbell et al., 2014, can benefit the firm in various ways, such as reducing the cost of capital when disclosure decreases uncertainty. Furthermore, not following such requirements leads to potential legal liability due to the failure to disclose material risks to shareholders (Campbell et al., 2014).

An economic lens can provide useful information on cybersecurity decisions made by both attackers and defenders (Anderson, 2001; Anderson and Moore, 2006). Market failures, especially information asymmetries and externalities, help explain why cybersecurity investments often lag or are inefficient. In this context, SEC disclosure requirements are best characterized as a policy intervention designed to remedy the information asymmetry between stakeholders such as investors, consumers, governments, and the firms themselves. These disclosures create a record of the interactions between companies and attackers, as well as the precautions firms take to mitigate the threat of incidents. One can also observe the "moving target" nature of attacks, in which adversaries shift focus to firms exhibiting weaker security based on observable characteristics such as industry, size, and apparent technological sophistication. Firms with weaker cybersecurity postures have been shown to suffer more severely from ransomware incidents (Connolly et al., 2020), further highlighting the risks involved when firms under invest. Game-theoretic models can provide a meaningful way to study these strategic interactions between firms and adversaries (Tan et al., 2023). The disclosures considered here could present an opportunity to empirically validate the predictions of such models.

Public regulatory filings, such as 10-K filings, offer a source of information on the cybersecurity posture of companies (Berkman et al., 2018; Celeny and Marćhal, 2023, October; Cheong et al., 2021; Gao et al., 2020; Hajizada and Moore, 2023; H. Li, No, and Wang, 2018; W. Li et al., 2023). However, boilerplate disclosure often plagues these reports, with generic recycled text bloating regulatory filings, diminishing transparency, and reducing informativeness (Gao et al., 2020; H. Li, No, and Wang, 2018; Nelson and Pritchard, 2016). Boilerplate disclosure is generic recycled text, that companies repeat annually because they have been carefully screened by management and attorneys (Gao et al., 2020). Researchers disagree on boilerplate disclosure in 10-Ks; nonetheless, pursuing increased informativeness and transparency benefits investors and regulators.

We are not the first to utilize regulatory disclosures to measure cybersecurity. Other researchers have approximated cybersecurity effort through metrics such as the length of disclosure and frequency of cybersecurity-related phrases, using computational methods to quantitatively measure these filings (Berkman et al., 2018; Florackis et al., 2023; Wong et al., 2023). Alternatively, researchers have manually coded parts of the text to analyze the qualitative aspects of these disclosures, finding topics based on their findings (Wong et al., 2023).

In contrast, for this paper, we combine the two approaches using domain-specific attributes of cybersecurity. We conduct qualitative analysis of cyber-related statements to categorize what is being discussed, then apply the framework quantitatively to 7,681 cybersecurity-related statements made by 61 firms. Distinct from prior research, we have also focused on all U.S.-based publicly-traded companies that have been independently reported to the Critical Infrastructure Ransomware Attacks (CIRA) dataset to have experienced a ransomware attack between 2018 and 2021. This enables us to study how disclosures, and ultimately cybersecurity risk management, changes following an incident.

# 2 Background and related work

## 2.1 Firm-level cybersecurity measurements

Research has shown that cybersecurity incidents have lasting impacts on financial stability (Gao et al., 2020; Schlackl et al., 2022; Woods and Böhme, 2021; Zhang and Smith, 2023), customer retention (W. Li et al., 2023; Woods and Böhme, 2021), and brand reputation of firms (Gao et al., 2020; W. Li et al., 2023). Despite such escalating claims about cyber-incident risks and inconsistent demonstrations of the efficiency of security interventions, cyber-risk management has been viewed as "more of an art than a science" (Woods and Böhme, 2021), signaling a need for systematic approaches to quantifying cyber risk, as "the main problem to solve is data availability" (Woods and Seymour, 2023).

However, acquiring relevant data to evaluate cybersecurity risks has long been recognized a persistent challenge (Anderson and Moore, 2006). Firms fear that openly discussing cyber incidents could damage their reputation. They also may not collect relevant data internally due to its impracticality, such as implementing security controls on one portion of their environment but not another to observe effectiveness. Furthermore, ethical and legal risks inhibit data collection and sharing (Moore et al., 2019), notably privacy concerns arising from inherent use of personally identifiable data (Grier et al., 2010).

Despite these headwinds, efforts to gather relevant data persist. The Cyberspace Solarium Commission recommended establishing a Bureau of Cyber Statistics in the United States to overcome the data gap (King and M. Gallagher, 2020, March). On the academic side, Woods and Seymour, 2023 emphasize the need for publicly available datasets containing variables of interest. These variables will inspire researchers to build upon it and search for relevant data. They continue to state that a publicly available database revolving around the details of ransomware victims could improve companies controls (Woods and Seymour, 2023), allowing for research to better improve firms' cybersecurity posture.

Some empirical research has indeed made progress on measuring how firm investment in cybersecurity defenses can reduce risk. Using survey data from Israeli companies, Gandal et al., 2023 demonstrated that companies adopting more security controls experienced a significantly lower chance of suffering an incident. Kwon and Johnson, 2014 finds that, within the healthcare sector, proactively investing in security controls reduces both the cost of security measures and the failure rate of such controls. The challenges in cybersecurity risk assessment are further highlighted by the reliance on publicly reported data, often resulting in biases such as the lack of significance of harms and the over-representation of large organizations in cybersecurity incident studies (Cheong et al., 2021; Woods and Böhme, 2021).

Measuring firm-level cybersecurity posture is a prominent topic. Nagle et al., 2017 examines the number of open ports in firms' networks and identifies a correlation between such and cyber incidents stemming from botnets. Liu et al., 2015 similarly focused on firms' networks, gathering data on the number of misconfigurations and malicious activities that originate from said networks. The researchers used this data to construct a model that identifies whether an incident will be reported. Sarabi et al., 2016 collected similar data, adding novelty in business sectors and types of breach. This information helped identify which industries were more susceptible to specific risks. Due to the ransomware spreading both socially and technically, a highly trained staff and secure network is required to combat it (Connolly et al., 2020). When looking at the cybersecurity posture of 50 firms based on preparedness of procedures and diligence of maintaining security standards, Connolly et al., 2020 find that the severity of ransomware incidents is independent of size or sector. Most related to our research, Berkman et al., 2018 creates a measure of firm-level cyber awareness to examine its impacts on the firm's market value. This measure is based on the length and relevance of the disclosure within 10-K filings, using a self-developed dictionary based on the National Initiative for Cybersecurity Careers and Studies (NICCS) glossary to calculate relevance.

## 2.2 Regulation and informativeness

The basis for reporting requirements from the SEC is *materiality*, defined as information for which "there is a substantial likelihood that a reasonable person would consider it important" (U.S. Securities and Exchange Commission, 1999). Publicly-traded companies are required to inform investors of all material risks they face and discuss how they plan to manage them. In theory, such disclosures should help investors make informed judgments on whether to buy or sell stocks in listed firms.

The cybersecurity-specific guidance issued by the SEC starting in 2011 continued in this vein, requiring firms to discuss any material cybersecurity risks, both prospective and actualized. The guidance made by the SEC in 2011 and 2018 heavily emphasized the need for specific and informative content (Gao et al., 2020; H. Li, No, and Wang, 2018), marking a pivotal shift in how companies disclose their risk (Cheong et al., 2021). Both Cheong et al., 2021 and H. Li, No, and Wang, 2018 note that this increased pressure caused a gap between regulatory intent and corporate response, as it led to firms disclosing more cybersecurity risk without them necessarily adequately capturing their actual level of risk (Peng and C.-W. Li, 2022). According to Cheong et al., 2021, these practices lead to diminished transparency, hindering investors' ability to make informed decisions. Additionally, firms display strategic behavior in their cybersecurity disclosures, particularly post-cyber incident (Cheong et al., 2021; Gao et al., 2020), with research finding a weakening correlation between the disclosure in 'Item 1A' and subsequent cybersecurity incidents weakening following the 2011 guidance, indicating a decline in the informational value of these disclosure (H. Li, No, and Wang, 2018; Nelson and Pritchard, 2016). Boilerplate disclosure carefully balances satisfying compliance requirements and obscuring potentially harmful information, this is done mainly though the repetition of statements that have been carefully screened by management and attorneys (Gao et al., 2020).

Despite the SEC's attempts to guide firms towards transparent reporting through repeated guidance, 10-K fillings are still characterized by boilerplate disclosure (Gao et al., 2020), which, due to it being both

generic and recycled, is less meaningful to investors and regulators (Nelson and Pritchard, 2016). However, some researchers suggest that boilerplate disclosure is obsolete (Berkman et al., 2018; Campbell et al., 2014; H. Li, No, and Wang, 2018). Campbell et al., 2014 found that risk factor disclosure was incorporated into post-disclosure market measures, suggesting that said disclosure is informative for investors. While H. Li, No, and Wang, 2018 found that a higher length of cybersecurity disclosure is positively associated with increased cybersecurity incidents. Berkman et al., 2018 echoes such findings, providing evidence that following the 2011 SEC guidance, disclosure reflects cybersecurity awareness and thus is not just a boilerplate. However, Campbell et al., 2014 continues to state that "our results do not necessarily imply that critics who call for improvements to risk factor disclosure are wrong." For the benefit of investors and regulators, more informative and less generic disclosure of cybersecurity incidents should be pursued.

Firm-level cybersecurity disclosure practices are increasingly driven by evolving regulatory requirements and guidance. The SEC's 2018 guidance, along with similar requirements from stock exchanges and other regulatory bodies, reflect a growing belief that cybersecurity risks can be material and should be transparently disclosed (Peng and C.-W. Li, 2022). These developments highlight a broader recognition that cyber threats now rival other national security concerns (Campbell et al., 2014), and should be crucial for shareholders' decision-making process. The cybersecurity disclosure should convey the material risks and uncertainties that could affect the performance of the companies (Campbell et al., 2014), and therefore should be readily available to potential and current shareholders. The omission of these risks and the opaque language that minimizes them could result in legal liability (Campbell et al., 2014; Nelson and Pritchard, 2016).

Weighing the potential cost of transparency, namely reputational damage, against the possible risk of regulatory enforcement, such as legislative action, is a potential strategic choice that firms take when disclosing 10-Ks (Cheong et al., 2021). Boilerplate disclosure runs counter to the goal of transparency by satisfying regulatory requirements without informing investors. Disclosure that is regularly updated and easily understood benefits investors and mitigates information asymmetries (Nelson and Pritchard, 2016). Enhanced disclosure can improve investors' ability to assess risk and, according to empirical research Campbell et al., 2014, may lower a firm's cost of capital by reducing information asymmetry, perceived uncertainty, and risk correlation with the broader market-ultimately benefiting both investors and the firm.

## 2.3 10-K cybersecurity disclosure

Analysis of 10-K documents is plentiful, dating back almost two decades (F. Li, 2008). The authors used EDGAR and 10-Ks to measure firms' risk sentiment based on the frequency of words related to risk and uncertainty within the filings. According to their findings, risk sentiment can be used to predict future returns with firms with a greater frequency change related to negative sentiment suffered from negative returns in the following year (F. Li, 2008), showing the potential usefulness of analyzing 10-K filings. This frequency-based methodology has become the standard for analyzing 10-Ks. Future research adopted a textual analysis approach, akin to a Bag-of-Words (BOW) methodology, focusing on metrics such as frequency of words, length of cybersecurity risk disclosure, and the presence of said risk disclosure (H. Li, No, and Wang, 2018). Likewise, other research has used computational linguistics to create a measurement that provides weight to words frequently found based on their predictive ability to ascertain future attacks (Jamilov et al., 2021).

The following papers are the ones most closely related to our objective. Florackis et al., 2023 develop a cybersecurity risk measure using textual analysis on Item 1A Risk Factors section. This analysis spans from 2007 to 2018 for the authors to capture a broad spectrum of cybersecurity risk disclosure and related cyber-attack incidents. These disclosures were compared to disclosures of firms that had experienced a significant cyber attack, using data from the Privacy Rights Clearinghouse to form a training sample. This measure used cosine and Jaccard similarity scores to estimate the degree of similarity between the training

sample and the sampled firms (Florackis et al., 2023). Likewise, Peng and C.-W. Li, 2022 uses Vector Space Modeling (VSM) to calculate the change in disclosure modification before and after a cybersecurity incident based on similarly extracted text from 10-K fillings, specifically looking at how firms alter their disclosures following a cybersecurity attack. This research looks at firms that suffered cybersecurity incidents between 2013 and 2016, finding that firms disclose more information once they have suffered an incident. However, they do not find any evidence of the quality of the disclosure changing post-incident (Peng and C.-W. Li, 2022). Finally, Wong et al., 2023 analyze how companies make disclosures in the face of confusing and ever-changing privacy legislation and resulting regulation legible to potential and current investors. This study focuses on nine large technology companies and examines disclosures between 2015 and 2020. Our paper follows a similar methodology to theirs, as they implement a thematic analysis process where two coders read 10-K documents and iteratively work through them, adding a qualitative layer to this process.

Our research intends to synthesize and expand upon these related works. In the next section, we describe a methodology inspired by grounded theory designed to integrate qualitative analysis with quantitative metrics. We analyze a sample of 61 companies, each having suffered a ransomware attack, to quantify how their disclosures change over time in relation to the incident. While this research does quantify statements, the goal is to move away from a frequency-based methodology, which can lose rich information and where observably boilerplate recycled statements may undermine metrics based on simple counts. Additionally, the manual process of analyzing and categorizing all 7,681 statements has allowed for the creation of qualitatively created categories and subcategories that, interestingly, echo the factors present in the causal model espoused by Woods and Böhme, 2021.

# 3 Categorizing cybersecurity disclosure text

We describe how the data is collected, followed by the process for constructing categories and the resulting descriptions.

## 3.1 Data collection methodology

The population under investigation is all U.S.-based publicly traded companies that suffered ransomware incidents between 2018 and 2021. These companies were identified as having suffered an incident by the CIRA dataset maintained at Temple University Aunshul Rege, 2025, The CIRA dataset recorded 946 ransomware incidents between 2018 and 2021. However, most of these incidents did not affect firms who were obligated to disclose that they have experienced an incident. Only public companies based in the United States are required to file 10-K annual reports, and only these firms are required to discuss how they manage cybersecurity risks and report incidents. After removing duplicates and any organizations not subject to disclosure rules (i.e., non-profit organizations, private companies and international firms), we were left with 61 distinct public companies. While the number may appear small, it actually quite comprehensively identifies nearly all companies who experienced ransomware and filed annual reports with the SEC. Below, we compare the CIRA to another dataset to evaluate the comprehensiveness of its coverage. Within these 61 public companies, 314 10-K fillings were accessed. During our time period many companies either became publicly traded, became privately traded, or merged with other companies, thus they did not have all six 10-K's available.

The available 10-Ks were downloaded from the SEC EDGAR website and subsequently parsed through a Python script, which extracted paragraphs related to cybersecurity based on the following keywords: 'cyber', 'ransomware', 'breach', 'malware', 'phishing', and 'unauthorized'. These keywords were selected based on a manual review of the cybersecurity risk section from approximately half of the 10-K filings, capturing the most prominent cybersecurity-related terms.

We focus exclusively on companies that experience ransomware incidents as outlined above. Initially, ransomware incidents primarily threatened availability by scrambling firm data, but the threats have evolved to also target confidentiality since criminals often publish stolen data when ransoms are not paid. Notably, ransomware attacks do not as directly impact integrity, the third aspect of the so-called CIA triad fundamental to cybersecurity. Despite this, our study examines the broader cybersecurity strategies of firms both before and after a ransomware incident. Hence, we anticipate the disclosures to cover all aspects of cybersecurity, including integrity. Hence, that is why our keyword search is broader than ransomware, covering terms such as 'breach', 'malware' and 'phishing'. Such terms could certainly appear in the context of a ransomware attack, but may also be relevant for cybersecurity threats more broadly.

We collect data in this way for several reasons. First, we anticipate that experiencing a ransomware incident should alter a firm's overall cybersecurity strategy. Second, a firm's broader cybersecurity posture should impact its likelihood of falling victim to ransomware. Third, ransomware is a very serious threat to many firms that rose rapidly in prominence during the 2018–2021 period under study. Fourth, compared with other threats such as data breaches, ransomware attacks harm companies directly and do not exhibit externalities to the same extent as other threats. Hence, we expect rational firms to take cybersecurity precautions before and after experiencing an event (Telang, 2021).

To further assess the suitability of the Temple CIRA dataset, we compared it to another data source, the Cyber Events Database maintained by the University of Maryland (Harry and N. Gallagher, 2018). This database tracks all public reports of cyber incidents, not just ransomware, affecting any organization. We leverage this database to evaluate the coverage of the CIRA, and to identify what kinds of attacks public companies experience besides ransomware.

Unfortunately, the Cyber Events Database does not identify when an affected organization is a publicly-traded company. Of the 5,067 incidents occurring between 2018–2021, we found 138 affecting public companies based in the United States. 38 of these incidents were ransomware attacks (as determined by searching for the term "ransom" anywhere in the description).

Of the 61 ransomware incidents from CIRA, 29 were also found in the Cyber Events Database. 32 appeared only in CIRA, while 9 ransomware incidents appeared only in the Cyber Events database. This confirms that the CIRA is a very comprehensive record of ransomware incidents.

Furthermore, this reinforces the fact that ransomware is a substantial attack type affecting publicly-traded companies. Most of the 100 non-ransomware incidents found in the Cyber Events Database describe data breaches or other thefts of personal or corporate information. 84 of these incidents are categorized as "Exploitive", which is the category assigned to data breaches. 11 are classified "Disruptive" (suggesting a denial-of-service attack), while 4 are classified as "Mixed". We therefore conclude that the CIRA dataset is reasonably comprehensive and appropriate for studying public-company discussions of cyber risks.

## 3.2 Grounded theory process

Grounded theory is an iterative research approach in which data is collected and analyzed to develop theories and hypotheses inductively. This research took inspiration from grounded theory, ensuring a valid interpretation of the text statements and limiting the amount of bias within the categorization. The iterative process began with taking a random, unique, representative sample of the statements, resulting in a sample of 595 statements. These statements were analyzed by three researchers, the two co-authors and an additional researcher, where three rounds of iterative coding and discussions were completed. During the coding session, each coder would independently analyze a portion of the statements and assign one of the categories to them. During the discussion phase, problematic statements were identified and discussed. Discussion led to either a realization of the coder's mistake during categorization or the adaptation of the definitions to more accurately capture the statements. After the third round the following four categories were realized: 'Inci-

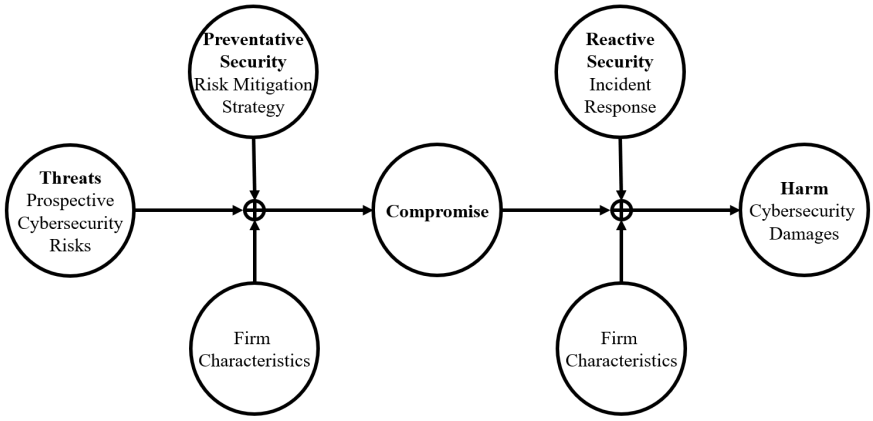


Figure 1: Causal model (Woods and Böhme, 2021) mapped to identified categories.

dent Response (IR)', 'Cybersecurity Damages (CD)', 'Prospective Cybersecurity Risks (PCR)', and 'Risk Mitigation Strategy (RM)'. After these initial discussions, two coders analyzed the entire 595 statements. The reliability between raters was evaluated using Cohen's Kappa. The unweighted kappa was $\kappa = 0.69$, 95% CI [0.65, 0.74], indicating a substantial agreement (Landis and Koch, 1977). The weighted kappa, accounting for the degree of disagreement, was $\kappa = 0.65$, 95% CI [0.58, 0.72].

## 3.3 Category descriptions

**Prospective Cybersecurity Risks (PCR)** is defined as "statements that are forward-looking statements describing how and what could go wrong with cybersecurity". Theoretically, this category aligns with the 'Threat' latent factor within the causal model espoused by Woods and Böhme, 2021. (Figure 1 shows the mapping of each category onto the model.) An example of a PCR statement is: "Despite our security measures, our information technology infrastructure may be vulnerable to attacks by hackers or breached due to employee error, malfeasance or other disruptions." This statement captures the company's expectations of threat and uncertainty.

**Risk Mitigation Strategy (RM)** is defined as "statements that explain company strategies to mitigate the impact of a future cybersecurity incident." Theoretically, this category aligns with the 'Preventative Security' latent factor within the causal model. An example of an RM statement is: "We proactively evaluate the cybersecurity risk of third-party IT providers and solutions by utilizing a repository of risk assessments and an external monitoring solution that includes threat intelligence to better inform us during contracting and vendor selection processes." This statement captures the proactive strategies used by the company to reduce the potential for compromise.

**Incident Response (IR)** is defined as "statements that explain the steps companies took to limit the impact caused by an experienced incident directly" and was initially referred to as 'Corrective Plan of Action.' An example of an IR statement is: "Upon learning of the AMCA Incident, the company promptly stopped sending new collection requests to AMCA and stopped AMCA from continuing to work on any pending collection request from the Company." This statement captures the company's response once it discovers the incident to reduce the compromise's further impact.

**Cybersecurity Damages (CD)** is defined as "statements that describe damages caused by cybersecurity incidents and any other results of such damage." An important clarification is that, as this is the result of suffering an incident, statements referring to companies who are reimbursed by their cybersecurity insurance, as well as other positive outcomes, are also included, as they are consequences of the incident. An

| Subcategory | Definition |
|---|---|
| **Prospective Cybersecurity Risks (PCR) & Cybersecurity Damages (CD)** | |
| Legal Costs | Statements that speak about legal consequences and proceedings stemming from a cyber-attack. |
| Business Disruption | Statements that speak about interruption of business operations stemming from a cyber-attack. |
| Reputation | Statements that speak about reputational damages stemming from a cyber-attack. |
| Third Party | Statements that mention that a cyber-attack is due to a related third-party incident or may affect related third parties. |
| Unauthorized User | Statements that speak about damages caused by users with falsified access (such as hackers). |
| Information | Statements that speak about the loss or compromise of confidential data due to a cyber-attack. |
| Financial Loss | Statements that speak about monetary losses stemming from a cyber-attack. |
| **Risk Management (RM)** | |
| Due Diligence | Statements that suggest the organization is employing all mechanisms to prevent cyber-attacks. |
| Program | Statements that mention the creation of or an existing system to resolve cyber-attacks. |
| Compliance | Statements that mention the resulting regulations that must be followed to resolve a cyber-attack. |
| Assessment | Statements that mention the company's actions to get an overview of their cybersecurity defense system. |
| Committee | Statements that mention the creation of or an existing group to oversee cyber defense. |
| Third Party | Statements that mention the use of third-party services. |
| Training | Statements that mention a program designed to educate or spread awareness of cybersecurity. |
| Investment | Statements that mention increased resources being used to support cyber defenses. |
| NIST Framework | Statements that mention the use of the NIST framework. |
| **Incident Response (IR)** | |
| Reporting | Statements that mention notification to affected parties, stakeholders, and regulatory bodies. |
| Legal | Statements that mention interaction with the judiciary or law enforcement in relation to the incident. |
| System Shutdown | Statements that mention the company deliberately took their systems offline. |
| Experts | Statements that mention interaction or consultation with professionals in the related field. |
| Monitoring | Statements that mention that the company monitored the system's security levels. |

Table 1: Subcategory definitions.

example of CD statements is: "We have incurred legal, settlement and other costs in connection with cyber incidents that have impacted us." This statement captures the consequences suffered by the company that resulted from the cybersecurity incident.

In addition, this dataset tracks the following: 'Ransomware' - a boolean variable describing if the statement mentions the term ransomware within it and 'Immaterial' - a boolean variable describing if the statement refers to the harms sustained from cybersecurity incidents as immaterial, as well as subcategories within the primary categories.

Various subcategories emerged within each of the primary categories. Due to overlapping thematic elements, PCR and CD are grouped together allowing for a direct comparison between prospective risks and the realized impacts. They were developed and analyzed using the same approach as the primary categories. Table 1 provides definitions for each subcategory. These definitions are derived from terminology used within the 10-K fillings and may not align with standard terminology used in other domains. For example, while Financial Loss is often a consequence of Legal Costs (such as a settlement expenses), Legal Costs is a separate subcategory as it is often mentioned independently within the textual statements as seen in the following example.

> Any security breach involving the misappropriation, loss, or other unauthorized disclosure of confidential information, whether by us or our vendors, could result in significant legal and

| Subcategory | Chart of Accounts |
|---|---|
| **Prospective Cybersecurity Risks (PCR) & Cybersecurity Damages (CD)** | |
| Legal Costs | 6.3.9 Fines And Penalties (Dr) & 5.2.2 Selling, General And Administrative (Dr) |
| Business Disruption | 5.2.1 Cost Of Sales (Dr) & 5.2.2 SG&A (Dr) & 6.2.8 Other Gains And Losses (Dr / Cr) |
| Reputation | 6.2.8 Other Gains And Losses (Dr / Cr) |
| Third Party | 2.4.3 Other Provisions (Cr) & 7.3.2 Intercompany And Related Party Expenses (Dr) |
| Unauthorized User | 6.2.7 Impairment Loss (Dr) & 5.1.2 Employee Benefits (Dr) |
| Information | 6.2.8 Other Gains And Losses (Dr / Cr) & 5.2.2 SG&A (Dr) |
| Financial Loss | 6.2.8 Other Gains And Losses (Dr / Cr) & 1.2.1 Accounts Receivable (Dr) |
| **Risk Management (RM)** | |
| Due Diligence | 5.2.2 SG&A (Dr) |
| Program | 5.1.3 Services (Dr) & 1.7.2 Computer Software (Dr) |
| Compliance | 6.3.3 Direct Tax And License Fees (Dr) & 5.2.2 SG&A (Dr) |
| Assessment | 5.2.2 SG&A (Dr) |
| Committee | 5.2.2 SG&A (Dr) |
| Third Party | 5.1.3 Services (Dr) & 7.3.2 Intercompany And Related Party Expenses (Dr). |
| Training | 5.1.2 Employee Benefits (Dr) & 5.1.3 Services (Dr) |
| Investment | 1.1.2 Financial Assets (Investments) (Dr) & 1.7.2 Computer Software (Dr) & 5.1.3 Services (Dr) |
| NIST Framework | 5.2.2 SG&A (Dr) & 5.1.3 Services (Dr) |
| **Incident Response (IR)** | |
| Reporting | 5.2.2 SG&A (Dr) & 6.1.2 Other Expenses (Dr) |
| Legal | 6.3.9 Fines And Penalties (Dr) &5.2.2 SG&A (Dr) |
| System Shutdown | 5.2.1 Cost Of Sales (Dr) & 6.2.8 Other Gains And Losses (Dr / Cr) |
| Experts | 5.1.3 Services (Dr) |
| Monitoring | 5.1.3 Services (Dr) & 1.7.2 Computer Software (Dr) |

Table 2: Subcategories mapped to Chart of Accounts.

> remediation expenses, severely damage our reputation and our customer relationships, harm sales, expose us to risks of litigation and liability, and result in a material adverse effect on our business, financial condition, and results of operations.

With that in mind, Table 2 presents a simplified mapping of our subcategories to the Chart of Accounts (COA), a standardized list of financial accounts used under IFRS and the US GAAP. This is done to relate existing financial terminology to the subcategories discovered during our data collection. For example, in the Financial Loss subcategory: direct monetary impacts (such as stolen funds or ransom payments) would be recorded in the income statement under 6.2.8 Other Gains and Losses (Dr), while a disrupted contract resulting in uncollectible receivable would be recorded as a bad debt expense under 1.2.1 Accounts Receivable (Dr).

# 4 Analysis

We now analyze the categorized statements in order to study variation by firm and in response to incidents. This analysis focuses on the overall proportion of firms that make cybersecurity statements delineated by category, as well as the median number of statements made in each category. In addition, this analysis will also capture how these disclosures change in relation to the incident. This analysis compares various subcategories and tags given to specific statements, based on specific words and phrases being used.

| Year | 2018 | | 2019 | | 2020 | | 2021 | | 2022 | | 2023 $\overline{1C}$ | | 2023 1C | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | % Firms | Median # statements | % Firms | Median # statements | % Firms | Median # statements | % Firms | Median # statements | % Firms | Median # statements | % Firms | Median # statements | % Firms | Median # statements |
| Prospective Risk (PCR) | 98 | 9 | 96 | 9 | 98 | 12 | 100 | 12.5 | 100 | 14.5 | 100 | 16 | 100 | 16.5 |
| Incident Response (IR) | 4 | 0 | 13 | 0 | 39 | 0 | 46 | 0 | 42 | 0 | 36 | 0 | 44 | 0 |
| Risk Mitigation (RM) | 53 | 1 | 58 | 1 | 61 | 1 | 72 | 1.5 | 75 | 2 | 72 | 1 | 96 | 19 |
| Damages (CD) | 38 | 0 | 44 | 0 | 68 | 2 | 96 | 4 | 92 | 3 | 90 | 3 | 96 | 4 |
| TOTAL | 98 | 11 | 96 | 12 | 98 | 17 | 100 | 21 | 100 | 21.5 | 100 | 24 | 100 | 44 |

Table 3: Primary Categories by Year

## 4.1 How have cybersecurity disclosures changed over time?

Table 3 reports how cybersecurity-related disclosures in annual reports have changed over time. We can see that discussions involving cybersecurity steadily increased in the time period. The median number of statements observed has steadily risen from 11 in 2018 to 24 in 2023 (excluding statements in the newly required Section 1C Cybersecurity, which was added in 2023). What firms discuss has also changed. While nearly all companies have discussed prospective risks since 2018, the other categories have steadily increased to varying degrees. For example, whereas in 2018–19, fewer than half of firms discussed cybersecurity damages, by 2021 the share rose to 96%, remaining high in subsequent years. The share of firms discussing risk mitigation strategies rose more modestly, from approximately half of the companies early on to approximately 3 in 4 in later years. The 'Total' row was calculated by combining all four of the other categories for the relative year. While the percentage of firms captures this combination correctly, due to rounding, the median statements are slightly higher than they would be summed. Finally, we observe that most discussion focuses on prospective risks, with between 9–16.5 median statements. By contrast, most companies do not discuss incident response or risk mitigation strategies as much.

As mentioned above, the SEC recently issued guidance to firms asking that they complete a new section entitled "1C Cybersecurity" for any disclosures submitted after the 18th of December 2023 (Katz and McIntosh, 2025; U.S. Securities and Exchange Commission, 2023, July). Item 1C is a new requirement for companies to address their risk management and governance policies in relation to cybersecurity. Within our sample, 38 of the 61 companies have implemented Item 1C. This is due to companies publishing 10-Ks at different points in the year, with 38 of them publishing the report for 2023 after the SEC issued guidance.

The final two columns reflect the difference between the exclusion and inclusion of Item 1C within the 10-K documents. All primary categories increase with the inclusion of Item 1C. Notably, risk mitigation has the largest increase, where almost all the firms now address risk mitigation within their disclosures. Additionally, with a median of 19 statements, risk mitigation is now the most widely discussed category. Risk mitigation is an important category to address in a disclosure as it will help investors understand firm defensive strategy. However, the content of Item 1C is still new and only became mandatory starting in 2024. We defer analysis of 1C statements to future work, once more time has passed. For this paper, we exclude all 1C statements from subsequent analysis.

| Year | -3 | | -2 | | -1 | | 0 | | 1 | | 2 | | 3 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| # Firms | 14 | | 39 | | 49 | | 55 | | 56 | | 53 | | 38 | |
| | % Firms | Median # statements | % Firms | Median # statements | % Firms | Median # statements | % Firms | Median # statements | % Firms | Median # statements | % Firms | Median # statements | % Firms | Median # statements |
| Prospective Risk (PCR) | 93 | 7.5 | 97 | 10 | 98 | 11 | 98 | 11 | 100 | 13 | 100 | 15 | 100 | 16 |
| Incident Response (IR) | 0 | 0 | 0 | 0 | 3 | 0 | 55 | 1 | 45 | 0 | 42 | 0 | 34 | 0 |
| Risk Mitigation (RM) | 36 | 0 | 51 | 1 | 57 | 1 | 67 | 1 | 70 | 1 | 74 | 1 | 76 | 2 |
| Damages (CD) | 21 | 0 | 36 | 0 | 35 | 0 | 87 | 5 | 95 | 4 | 91 | 3 | 92 | 3 |
| TOTAL | 93 | 9 | 97 | 11 | 98 | 13 | 98 | 21 | 100 | 21 | 100 | 21 | 100 | 23.5 |

Table 4: Comparing Categories Relative to Incident

## 4.2 How do firm disclosures change following an incident?

Following a ransomware attack, we would expect firms to address the incident in their regulatory filings. Table 4 follows the same structure as Table 3 but orients time relative to when the incident occurred. The columns with negative years are pre-incident, while columns zero and above are the year of the incident and the following years. The 'Total' row was calculated by combining all four of the other categories for the relative period. While the percentage of firms captures this combination correctly, due to rounding, the median statements are slightly higher than they would be summed.

Overall, firms roughly double the number of cybersecurity statements from the years before an incident (11 - the mean of the total median statements for all years pre-incident) to the years afterwards (21.6 - the mean of the total median statements for all years post-incident). Prior to incidents, most firms discuss prospective cybersecurity risks. Discussion of prospective risks increases steadily, from 7.5–11 statements before and to 11–16 in the years following incidents. This corroborates previous theory that cybersecurity disclosure is expanding, both due to expanding cybersecurity sections within 10-K disclosure (Brown and Tucker, 2011), as well as the increasing risk surrounding cybersecurity (Romanosky, 2016; Schlackl et al., 2022).

In contrast, a smaller share of firms disclose their risk mitigation strategies. 57% of firms discuss risk mitigation strategies in the year before an incident, rising steadily to 76% three years after an incident. Even when they do discuss risk mitigation, they disclose relatively little, the highest median of two statements appearing in each annual report. Such modest change suggests that firms disclosure of their risk mitigation strategies is not influenced by suffering an incident, and is likely more a reflection of increased regulatory and societal pressure to constantly be upgrading their layers of defense.

Incident response statements discuss incident response plans and the steps undertaken to contain the compromise and reduce continued impact of the incident. Such statements are even more rare than those outlining general risk mitigation strategies. As expected, most firms do not make such statements prior to an incident occurring (those that do are referring to prior incidents unrelated to the ransomware events we studied). More surprisingly, only 55% of firms with incidents do discuss incident response in their filings even after the attack has taken place.

The incident impacts firm in many ways, such as business disruption, financial loss, and lawsuits. Compared to relatively extensive discussion of prospective cybersecurity risks, firms make fewer cybersecurity

| | PCR | IR | RM | CD | Total |
|---|---|---|---|---|---|
| Ransomware | 57% | 13% | 5% | 59% | 75% |
| Legal Costs | 90% | 11% | 15% | 43% | 93% |
| Immaterial | 3% | 0% | 0% | 31% | 34% |
| Insurance | 72% | 5% | 30% | 26% | 79% |

Table 5: Variables by Category

damage (CD) statements. In the years following a ransomware attack, most but not all firms (87–95%) do explicitly discuss the damages incurred. The median number of such statements is 5 for the year of the incident, slightly declining in later years. A key question is whether firms consistently disclose the types of risks they face before experiencing an incident and the impact they disclose afterwards. We examine this in more detail next.

## 4.3 Do firms discuss risk consistently before and after incidents?

Given that all firms in our sample experienced a ransomware attack, a natural starting question is how many disclose this fact. Table 5 reports that 75% of firms mention ransomware at least once across all 10-K reports. It is somewhat surprising that the share is not higher, given SEC disclosure guidance.

Next, it is worth noting *where* ransomware is mentioned. Most often, ransomware is discussed in PCR statements (57%) and in CD statements (59%). Very few mention it within their incident response plans and even fewer regarding how they proactively plan to mitigate such risk.

In addition to disruption and the ransoms themselves, legal costs can be a major consequence of ransomware attacks. 93% of firms mention litigation, legal procedures and how cybersecurity risks are manifested in the law. Typically, these are discussed as a prospective risk. However, less than half of the firms mention the resulting impact of such litigation (usually in the form of punitive cases or regulated practices). Within both incident response and risk mitigation disclosure, firms discuss legislation and regulation far less. These results echo those of Wong et al., 2023 which find that new regulations and, importantly, cybersecurity incident reporting requirements, are viewed as cybersecurity risks and are viewed similarly to prospective risks.

The SEC Cybersecurity guidance requires firms to discuss "material" cybersecurity risks. While exactly one firm explicitly admits to a risk or event rising to the level of materiality, roughly a third do the opposite. 34% of firms make statements about the immateriality of cybersecurity risks, with fully 31% of firms qualifying CD statements by stating that they are immaterial. By contrast, *not stating* that the damage is immaterial is an implicit admission of materiality, since the guidelines state that material risks must be disclosed. We dig deeper into why firms might voluntarily disclose immaterial cyber risks in Section 4.6.

We also observe that 79% of firms mention cyber insurance in their disclosures. The vast majority of these disclosures are found within the prospective risks section, often stating that, in the case of a potential incident, their insurance may not be able to cover all of the damages. Surprisingly, only 30% of the firms discuss insurance as part of their risk mitigation strategies. By contrast, the majority of firms do discuss insurance in their potential risks. Similarly in percentage, 26% of firms mention insurance when discussing cybersecurity damages. These statements capture the firms who suffered damages despite insurance coverage. However, due to the definition of CD, these statements also capture the firms who benefited from insurance payouts. We return to the role of insurance in mitigating damages in Section 4.5.

We next consider *when* risks and damages are discussed. Do firms change how they talk about risk and damages after an incident occurs? Table 6 seeks to answer this question. The first two columns capture

| | Ransomware | Legal Costs | Business Disruption | Reputation | Third Party | Unauthorized User | Information | Financial Loss | Average |
|---|---|---|---|---|---|---|---|---|---|
| Pre-Incident Risk (PCR) | 18% | 78% | 94% | 90% | 65% | 78% | 92% | 86% | 82% |
| Post-Incident Risk (PCR) | 59% | 90% | 100% | 97% | 86% | 95% | 98% | 95% | 90% |
| Damages (CD) | 61% | 44% | 78% | 27% | 42% | 59% | 49% | 78% | 54% |
| Pre-Incident Risk & Damages | 14% | 41% | 76% | 27% | 27% | 47% | 47% | 65% | 47% |
| Pre-Incident Risk & No Damages | 4% | 37% | 18% | 63% | 37% | 31% | 45% | 20% | 36% |
| No Pre-Incident Risk & Damages | 49% | 6% | 4% | 2% | 14% | 12% | 4% | 14% | 8% |
| No Pre-Incident Risk & No Damages | 33% | 16% | 2% | 8% | 22% | 10% | 4% | 0% | 9% |

Table 6: Comparing pre-and post-incident risk to the reporting of damages by subcategory.

ransomware and legal costs, comparing how they change pre- and post-incident, as well as how often they are mentioned in CD statements. The goal of the bottom half of the table is to tease out the timing more clearly so we can determine whether statements of prospective risks made in the years prior to a ransomware event accurately reflect the impact of the incident.

Before an incident only 18% of firms discuss ransomware as a prospective risk. Afterwards, 59% do, with 61% mentioning ransomware as a source of cybersecurity damages. The bottom half of the table makes the distinction more precise. Only 14% of the firms discuss the potential for ransomware and later report the resulting impact. An additional 4% discuss the potential of ransomware beforehand but do not mention any impact of the incident.

By contrast, 49% of the firms did not discuss ransomware as a prospective risk prior to the incident but did so when they disclosed subsequent CD statements. Hence, these firms did not accurately identify cybersecurity risks in advance. A further 33% of firms fail to mention ransomware in either their prospective risks before the attack or in their impact disclosure. There are two possible explanations. Either these firms were not substantially affected by ransomware attacks or they are not sufficiently transparent in disclosing the risk or impacts experienced.

We observe that there appears to be little relationship between disclosing a particular risk before an incident and whether or not CD statements are later reported. Overall, a slightly greater share of firms report risks before an incident and later disclose the impact of the incident (47% to 36%). But the share is similarly split for those that do not disclose risks in advance of an incident and those that just do not disclose risks (8% vs 9%). Broadly speaking, the same story holds true for particular subcategories indicated in the table's columns. These subcategories were observed in both PCR and CD statements. While there is some variation, a chi-squared test indicates no statistically significant difference in proportion.

One takeaway from this analysis is that a minority of firms are not being sufficiently transparent in discussing cybersecurity threats. 9% of the time, there are no PCR or CD statements disclosed. A much larger share discuss only one side of the issue, either the risk or the impact of the incident, but not both. Given that all of these companies have been confirmed to have experienced ransomware, this is troubling.

Some types of risks are discussed more than others. 94% discuss business disruption risk prior to an incident, compared to 65% discussing third-party risks before an incident. After suffering an incident, all subcategories are discussed more frequently as a prospective risk, with all 61 firms mentioning the risk

| Category | Total | | Pre-Incident RM | | No Pre-Incident RM | | Post-Incident RM | | No Post-Incident RM | | Incident Response | | No Incident Response | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | # | % | # | % | # | % | # | % | # | % | # | % | # | % s |
| Immaterial | 19 | 31 | 10 | 53 | 9 | 47 | **18** | **95** | **1** | **5** | 12 | 63 | 7 | 47 |
| No Immaterial | 42 | 69 | 20 | 49 | 22 | 51 | **29** | **71** | **13** | **29** | 22 | 51 | 20 | 49 |
| $ Damages | 14 | 23 | 4 | 29 | 10 | 71 | 13 | 93 | 1 | 7 | **13** | **93** | **1** | **7** |
| No $ Damages | 47 | 77 | 26 | 55 | 21 | 45 | 34 | 72 | 13 | 28 | **21** | **66** | **26** | **34** |
| Legal Costs | 26 | 43 | 11 | 42 | 15 | 58 | 23 | 88 | 3 | 12 | **19** | **73** | **7** | **27** |
| No Legal Costs | 35 | 57 | 19 | 54 | 16 | 46 | 24 | 69 | 11 | 31 | **15** | **43** | **20** | **57** |
| Insurance | 16 | 26 | 7 | 44 | 9 | 56 | **15** | **94** | **1** | **6** | **15** | 94 | **1** | **6** |
| No Insurance | 45 | 74 | 23 | 51 | 22 | 49 | **32** | **71** | **13** | **29** | **19** | **42** | **26** | 58 |

Table 7: Comparing Risk Mitigation Disclosure

of potential business disruptions. However, there is greater variation in terms of CD subcategories. The most common types are financial losses (78%) and business disruption (78%). This makes sense, given that almost all firms these a prospective risks after suffering an incident. By contrast, while 97% of firms discuss reputational damage as a risk post-incident, only 27% of firms acknowledge damage to their reputation in the filings. Similarly, while 98% of firms discuss information risks post-incident, just 49% acknowledge experiencing the same type of damages from the incident. This is surprising given that ransomware attacks quite commonly harm confidentiality and integrity of enterprise data.

It is worthwhile to note the differences between ransomware and the subcategories. On average firms are able to disclose risks related to the subcategories the 82% of the time, only 18% of firms were aware of ransomware prior to to the incident. This discrepancy highlights a blind spot to the threat of ransomware. This result is consistent with other research showing the notable rise in ransomware during the 2020–2021 period (Hajizada and Moore, 2023).

## 4.4 Does disclosing cyber risk management strategies in advance affect outcomes post-incident?

We know from Table 4 that firms make much fewer statements about their cyber risk management strategies compared to discussions of prospective risks. 57% of firms include a statement about their risk mitigation strategies before a ransomware incident, steadily rising to around 76% in the years following an incident. RM statements are useful because they often indicate good cybersecurity posture and proactive investment following an incident. Table 7 summarizes the number of firms that mention RM strategies pre- and post-incident, and compares them to other variables of interest. The table also includes the incident response (IR), a particular form of reactive risk mitigation, in relation to the same variables.

Immaterial captures the firms which specifically mention that the impact suffered were "not material" in

their effects. As seen in the table, 19 of 61 firms (31%) report that the incident suffered was immaterial. Of those 19, 10 of them mention RM pre-incident. One might anticipate that firms who undertake better risk mitigation ahead of an incident are less likely to suffer a material loss. To explore relationships between the categorical variables, we relied on Fisher's Exact Test as the counts were too low for Pearson's Chi-squared tests. Results were considered statistically significant at the 10% level. Surprisingly, in this case we observe no statistically significant difference.

Interestingly, 18 of those 19 firms report on RM post-incident. This suggests that firms that state that the incident was not materially relevant, include RM statements post-incident to justify why the incident was immaterial. This is logical when considering that companies want to inform investors and regulators about how they successfully overcame the incident and how they plan to continue improving on their risk mitigation strategies. When analyzing the association, Fisher's Exact Test indicated a significant association between the variables ($p = 0.045$).

Interestingly, only one firm mentions that an incident had a material impact on the firm, but some firms do discuss the monetary damages suffered. The $ Damages variable indicates firms that disclose a monetary loss caused by the incident. 14 firms state specific monetary damages relating to an incident, while 47 do not mention any monetary damages. Over half (26 of 47) of companies reporting no damages also disclosed RM pre-incident, compared to just 4 of the 14 companies who suffered damages. Perhaps firms that proactively disclose risk mitigation strategies also tend to suffer less monetary damages than those who do not disclose their risk mitigation strategies beforehand. Of the same 14 firms that disclose damages, 13 disclose RM post-incident. When looking at the same firms, 13 of them disclose their incident response plan. In the same grouping, 26 of the 47 companies, those who do not state any monetary damages, also do not disclose any incident response plans. When analyzing the association, Fisher's Exact Test indicated a statistically significant association between the presence of monetary damages and the presence of incident response disclosure ($p = 0.0016$). Taken together, these results suggest that the firms that disclose damages alter their disclosure patterns in a manner that reflects the severity of said damages, with a significant increase in IR disclosure and a notable increase in RM disclosure.

As seen in the table, 26 of the 61 firms report legal costs directly arising from incidents. 19 of the 26 companies who discuss legal costs also disclose incident response. While, 20 of the 35 companies who do not discuss legal costs also fail to discuss incident response. This difference is statistically significant according to Fisher's Exact ($p = 0.022$). These results suggest that engaging legal advice may alter the way in which firms discuss incident response, which is consistent with the findings of other research Woods, Böhme, et al., 2023.

Finally, we consider firms that discuss insurance. While only 16 firms do so, nearly all of them (15 of 16) discuss risk management and incident response after the incident. By contrast, among those not discussing insurance, just 70% mention RM and 42% mention incident response. This makes sense, given that incident response services are often provided to policyholders. Each of these differences were statistically significant according to Fisher's Exact Test.

Even though incident response is disclosed by the fewest firms (as shown in both Tables 3 and 4), when such statements do appear they are powerful. It is evident from the results just presented that companies that disclose IR statements are more transparent about monetary damages, legal costs, and insurance. There are several plausible explanations why. One possibility is that because monetary damages, legal costs, and insurance link directly to suffered impact, firms that disclose such feel compelled to also discuss an incident response plan. Another is that firms with cyber insurance policies are more likely to receive guidance and support on incident response, especially after experiencing an incident, as all companies in our sample have. Regardless, both investors and regulators benefit from IR statements since they are directly related to the incident. They naturally stand out as positive examples of informative disclosure, especially when compared to boilerplate prospective risks so prevalent elsewhere.

## 4.5 Does insurance and legal costs help quantify damages?

Cyber insurance transfers risk from firms to carriers, but it also can reduce risk of an attack occurring and mitigate the impact of incidents afterwards. Additionally, insurers can even help to better quantify risk through claims data generated by covering losses. We see strong evidence of this in the disclosures. Only 14 of the 61 companies disclose specific monetary damages, 9 of those have insurance while 5 do not. Meanwhile, of the 47 companies that do not disclose specific monetary damages, 40 of them also do not disclose insurance. This difference is statistically significant ($p = 0.00067$). It stands to reason that companies who experience incidents and then file claims are much more likely to know what the incident costs due to their insurer footing all or part of the bill. Companies that do not have insurance, or whose insurance does not cover the incident, have not quantified the financial losses and thus do not share them in the disclosures.

Legal costs arising from incidents can also quantify the losses experienced. 43% of firms (26 of 61) discuss legal costs arising from incidents. However, of those 26, 11 (42%) report monetary damages. By contrast, only 3 of 32 (9%) of disclosures without legal costs mention damages. Hence, like insurance, legal costs appear to be a driver for manifesting quantifiable financial losses associated with cyber incidents ($p = 0.00432$). Moreover, insurance is associated with legal costs, with 13 of 16 firms carrying insurance also mentioning legal costs (81%) compared to 13 of 45 firms (29%) reporting legal costs but not insurance. This difference is statistically significant ($p = 0.00038$).

## 4.6 Why do firms disclose "immaterial" cybersecurity risks?

Firms have been instructed to disclose all material cybersecurity incidents. Thus, if a cybersecurity incident is disclosed in a 10-K, it is reasonable to assume it is material. Yet firms do sometimes disclose incidents but go out of their way to state that the incident was "immaterial". Why disclose at all? A company might anticipate that an incident may become public anyway and seeks to assure investors that it was not impactful enough to be considered material.

For the 14 firms that did disclose damages, we compared the reported loss in the first year mentioning damages to the total firm revenue that year. We might expect that smaller losses are more likely to be flagged as immaterial, and larger losses to not be. In fact, there is little difference between the groups for the total losses experienced or when normalized by company revenue. The median loss reported for immaterial incidents is \$17.9 million, compared to \$44.5 million for material ones. This difference is not significant according to a Wilcoxon test. As a share of company revenue, the median loss reported for immaterial incidents is 0.49%, compared to 0.81% for material ones. Again, this difference is not statistically significant.

We do observe that the largest losses tend to be material incidents. Only 1 of the 6 immaterial losses exceeds 1% of company revenue, while 4 of 8 material incidents do. So while the overall differences are indistinguishable, it does appear that more of the biggest losses tend to be material.

We also checked whether immaterial losses were more or less likely to also discuss insurance, legal costs or monetary damages. In each case, there were no statistically significant differences.

What are the implications of the fact that immaterial disclosures are mostly indistinguishable from material ones? First, it suggests that assertions of immateriality are not particularly informative to investors. Instead, assertions of immateriality may be more usefully understood as a strategy to minimize the importance of the incident while satisfying regulators that the firms are not hiding anything.

To better understand the implications of immateriality, we must examine both how it was captured within our data and how it is defined with regards to regulatory expectations. As shown in Table 5, only 3% of firms mention immateriality with PCR statements. This figure is misleading as it does not capture the qualitative context of these statements. While not reflected in any tables, we find that 89% of firms reference

the *potential* for material harm in their PCR statements. Yet these statements tend to be vague, high level, and lacking in substance. For example:

> Any significant breach in our data security infrastructure could result in a materially adverse effect on our operations.

Such statements fulfill minimal regulatory requirements while providing little actionable insight. Even more detailed disclosures, such as:

> Likewise, our customers, suppliers, subcontractors and partners face similar cybersecurity threats, and a cybersecurity incident impacting us or any of these entities could materially adversely affect our business operations and financial performance.

These statements still serve primarily as safeguarding disclaimers. These examples reference specific hypothetical consequences, that are much better aligned with subcategories such as financial loss, business disruptions, and third party. These forms of disclosure fall under boilerplate disclosure: generic, recycled language. These statements formally comply with regulation but do little to reduce information asymmetries and provide little help to investors aiming to make informed decision (Campbell et al., 2014; Gao et al., 2020).

Katz and McIntosh, 2025 state that material disclosure must offer timely, transparent, and specific information in order to benefit the decision making process. These qualities are notably in contention with the standard boilerplate disclosure found within our sample. The growing gap between regulatory intent and corporate practice suggest a misalignment; strategic ambiguity and boilerplate language is only enforcing such.

These tensions become particularly apparent when we return to the 31% of firms in Table 5 that explicitly classify incidents as immaterial. Within the analysis of these statements, we find evidence that immateriality is deployed not as a reflection of incident severity but rather a label to satisfy compliance requirements. Table 7 presents our only statistically significant association involving immateriality. Its positive correlation with RM disclosures post breach implies that firms labeling an incident as immaterial are more likely to increase their RM disclosure, justifying their classification by emphasizing their proactive governance and technical defenses. In contrast, firms that make no claims of immateriality have no incentive to frame their RM posture.

Thus, our analysis highlights the need for rigorous definitions and enforcement of transparent cybersecurity disclosure. The goal of SEC regulation is to reduce information asymmetry. To do such regulators must engage with how easily firms can satisfy formal requirements while providing boilerplate disclosure.

# 5 Case studies

This section will analyze 5 different corporations, based on the informativeness and the quantitative summaries of their statements. In order to ensure that they are all comparable within their 10-K disclosures, only companies that suffered incidents in either 2020 or 2021 and have all six 10-K's available, as well as having the year of the incident in the CIRA dataset, were eligible for this analysis. These limitations are required to keep the amount of disclosure before and after the incident consistent to allow for an apt comparison.

## 5.1 Informative disclosure

We have identified CIK 0000021175 CNA FINANCIAL CORPORATION as having one of the most informative disclosure practices. CNA reported that it suffered an incident in March 2021, as seen in the

following: "We sustained a sophisticated cybersecurity attack in March 2021 involving ransomware that caused a network disruption and impacted certain of our systems." This statement captures transparency by providing both the cause of the ransomware, a word that only 59% of firms mention, and when the attack took place. CNA also clearly explains the impacts they have suffered:

> Our investigation into the incident revealed that an unauthorized third party copied some personal information relating to certain current and former employees, contract workers and their dependents and certain other persons, including some policyholders.

On the other hand, they notably fail to mention any specific monetary amounts or how much personal information (or which information) was exposed.

CNA also shows transparency within their incident response plans:

> Upon detection, we undertook steps to address the incident, including engaging a team of third-party forensic experts and notifying law enforcement and key regulators. We restored network systems and resumed normal operations.

This is also in: "In July 2021, we provided notifications to the impacted individuals and regulators, by applicable law." These statements show they are more open than most firms with incident response plans. CNA also refers to their cybersecurity insurance coverage:

> Although we maintain cybersecurity insurance coverage insuring against costs resulting from cyber-attacks (including the March 2021 attack), we do not expect the amount available under our coverage policy to cover all losses.

Although this suggests that it was not enough to cover their financial losses, the fact that they had proactively taken such insurance suggests greater awareness of the present threats. They also disclose their strategies to promote their defenses and how much investment is due to the recent attacks: "Some of these investments are a direct result of the March 2021 cybersecurity attack, described in the immediately following risk factor, which is not recoverable under existing insurance coverage." However, the statement on investments is not that informative: "We have invested and continue to invest in the security of our systems and our technology infrastructure on an enterprise-wide basis." and "We have made, and continue to make, investments to improve our security and infrastructure." While these statements are not very descriptive, the fact that they refer to the incidents as the reasoning behind such investments, implying that CNA has internalized the threat to their business.

CNA's disclosure also captures the story of the event. After the initial compromise, due to a third party, CNA started making reactive risk statements regarding the incident in 2021 - the year of the incident: "The risk of a breach can exist whether software services are in our data centers or are cloud-based software services." This increased text disclosure follows previous research suggesting that firms react to a compromise (H. Li, No, and Wang, 2018). CNA also follows up on the dangers related to their vendor's systems and how such may affect them in 2023:

> The risks relating to future incidents in our, or our vendors', data security infrastructure, including in connection with cyber incidents, could have a material adverse effect on our business, results of operations or financial condition or may result in operational impairments and financial losses, as well as significant harm to our reputation.

This statement is additionally valuable as it only occurred from 2023 onwards, showing growth within their disclosure. However, this statement is repeated twice in the 2023 disclosure. Finally, CNA was one of the companies already implementing Item 1C within this disclosure, showing attention to the upcoming regulatory requirements.

It is usual for companies to repeat statements year after year, referred to as boilerplate disclosure. However, CNA has a few examples of repeating the same statements multiple times within the same 10-K. This repetition can be seen as unnecessary bloat, undermines the previously mentioned increase of text disclosure, and supports our notion to move away from purely frequency-based quantitative methods. CNA also mentions that such a incident was immaterial:

> Based on the information currently known, we do not believe that the March 2021 cybersecurity attack will have a material impact on our business, results of operations or financial condition, but no assurances can be given as we continue to assess the full impact from the incident, including costs, expenses and insurance coverage.

This statement is interesting because, while they do not expect the incident to be immaterial, they also do not expect it to fully covered by their cybersecurity insurance. This suggests a disconnect either between cyber insurance coverage and actual monetary damages, or between the perception of prospective risks and assessments of materiality. However, it's also possible that the presence of cyber insurance help limit the materiality of the incident itself.

While CNA's disclosure is not perfect, none are. CNA displays transparency regarding the fact that they have suffered a ransomware incident and when they suffered such. CNA explained why this occurred and reflected it in their following disclosures. All of this will aid investors and regulators when analyzing their 10-Ks and promote helpful information. Unfortunately, not all companies disclose incidents similarly.

## 5.2 Disconnected disclosures

We begin by analyzing CIK 0000912752 SINCLAIR BROADCAST GROUP INC, which highlights disconnectedness between prospective risks and realized cybersecurity damages. Sinclair has some noticeably good disclosure statements, giving both the date of the incident and a monetary amount of damages suffered as reported in 2021:

> The cybersecurity incident identified on October 17, 2021, resulted in the loss in the fourth quarter of 2021 of approximately $63 million in advertising revenue, primarily related to our broadcast segment, as well as approximately $11 million through the date of filing this Form 10-K in costs and expenses related to mitigation efforts, our ongoing investigation, and the security improvements resulting therefrom.

These two elements are both informative and show a care about transparency. Additionally, they also continue to discuss the impact of the incident informatively:

> The cybersecurity incident identified on October 17, 2021, resulted in the loss in the fourth quarter of 2021 of approximately $63 million of advertising revenue, primarily related to our broadcast segment, as well as approximately $7 million through the date of filing of this Form 10-K in costs and expenses related to mitigation efforts, our investigation, and the security improvements resulting therefrom.

This statement was disclosed in 2022, showing that they continue to modify their disclosure using up-to-date numbers. Additionally, Sinclair mentions the presence of a ransomware attack and how the company aims to combat such:

> Since the ransomware incident, our Board of Directors formed a cybersecurity subcommittee to provide greater oversight of the Company's cybersecurity measures and preparedness.

This is an excellent example of adjusting the disclosure to reflect the incident. However, Sinclair fails to maintain a qualitative connection.

Sinclair reported prospective risks prior to the incident related to subcategories: Business Disruption, Reputation, Third Party, Information, and Financial Loss; and had CD statements addressing: Legal Costs, Business Disruption, Information and Financial Loss. Additionally, their prospective risks post-incident increase for: Legal Costs, Business Disruption, Third Party, Unauthorized User, and Financial Loss, with Information even decreasing. Quantitatively, this mismatch between prospective risks and materialized CD statements shows a disconnect in awareness of an incident as, for example, any investors who had read their disclosure pre-incident have any information to assume that Legal Costs issues may arise from a cybersecurity incident. Another example of the disconnect is Third Party, where prospective risks were present before the incident and increased post-incident, but no CD statements were associated. The increase in the risks section suggests that it is not based on realized risk but on regulatory pressures or the need to bloat their filings instead of providing relevant information related to risks and the impact of the incident.

## 5.3 Unaware disclosure

Our next disclosure case is CIK 0001050825 STEELCASE INC. Steelcase's filings exemplify companies whose disclosures indicate a lack of awareness of any cybersecurity threat. Steelcase was the only company not to disclose any statements relevant to cybersecurity within their entire 10-K in the years prior the incident. This changed post-incident when they added vague statements such as: "We may be adversely affected by security breaches, errors or disruptions relating to our software and software- as-a-service offerings." There is also a discrepancy within their disclosure. According to the CIRA dataset, they suffered a ransomware incident in 2020; however, according to their disclosure, they first detected the cyber attack in 2021: "In Q3 2021, we detected a cyber-attack that resulted in unauthorized access to our information technology systems." Post-incident Steelcase reported primarily PCR statements of cybersecurity and slightly on the CD statements of said incident. Intriguingly, Steelcase reports on the monetary damages of the incident as follows:

> To protect our systems during that cyber-attack, we temporarily shut down our global operations, which resulted in a delay of approximately $60 [Million] in revenue from Q3 2021 to Q4 2021; however, we do not believe this incident had or will have a materially adverse impact on our business, operating results or financial condition or the effectiveness of our internal controls.

This statement has valuable information, as they do not expect this incident to be immaterial. Steelcase's filings reveal a company that learned from its mistake; that mistake is not believing that cybersecurity risks were worth disclosing prior to an incident. As previously mentioned, any informative content should be pursued to benefit regulators and stakeholders.

## 5.4 Overlooking impact disclosure

The final disclosures belongs to CIK 0000028823 DIEBOLD NIXDORF, INC. Diebold fails to address the impact of the incident in their disclosure, with the closest approximate CD statement being:

> We have experienced cybersecurity incidents in the past, but none of these incidents, individually or in the aggregate, has had a material adverse effect on our business, reputation, operations or products.

While the statement does not mention any impact of the incident, it alludes to the fact that they have suffered them in the past and that their impact was immaterial. This aligns with the central issue of Diebold, where,

post-incident, they vastly increased their disclosure on prospective risks. However, any impact suffered are not present in the disclosure. This suggests that their primary way of informing investors and regulators is in the form of prospective risks, hypothetical issues that could arise, such as this statement introduced post-incident:

> Although we have implemented cybersecurity measures designed to detect and limit the risk of unauthorized access to our systems and acquisition of, loss, modification of, use, access to, or disclosure of our data, threat actors are using evolving, sophisticated, and ever-changing techniques to obtain unauthorized access to systems and data.

Statements like this suggest that regardless of what the company does,incidents are still inevitable, a pattern found within all disclosures. These statements are less informative than statements that address actionable plans or materialized damages as they do not offer transparent information.

## 5.5 Lackluster disclosure

When looking for an example of a lackluster disclosure, our mentality focused on a company whose disclosure an investor would read before and after a compromise and would struggle to see any relevant change in information presented. Both the quantity of prospective risks and risk mitigation do not substantially increase post-incident, and there is a lack of recognition of any impact of the incident or any statements describing their incident response plan. The best example is CIK 0000912463 GUESS INC. Guess Inc. does not reflect much change within its disclosures. They fail to mention any statements that relate to their incident response plan. However, noteworthy, this brings them in line with 45% of all the companies who also fail to do so. Their statements disclosing risk mitigation strategies do remain constant, with the following statement appearing in 2018, 2019, and 2020:

> We believe that high levels of automation and technology are essential to maintain our competitive position and support our strategic objectives and we continue to invest in and update computer hardware, network infrastructure, system applications and cyber security.

It changed a small amount in 2021, "We continue to invest in and update computer hardware, network infrastructure, system applications and cyber security." In 2022, it changed to: "We continue to invest in new technologies and update computer hardware, network infrastructure, system applications and cyber security." In 2023, it changed to: "We continue to invest in new technologies and update computer hardware, network infrastructure, system applications, and cyber-security." All these changes are minor, and while they are not intentional, this may interfere with research focusing on unique statements and textual changes in 10-Ks.

Additionally, when Guess does speak about the impact of the incident, their statements are vague and give little to no information on what happened - though they do manage to state that the impact was immaterial: "While we do experience damage or interruption to our systems, such events have not in the past had a material adverse impact on our business, financial condition, or results of operations." Guess Inc.'s disclosure changes the least when comparing their quantitative and qualitative statements before and after the incident. While that does not necessarily mean they have a poor cybersecurity posture, it suggests such to any investors and regulators interested in their disclosure. While they were our highlighted firm, many other firms make these mistakes in their disclosures. As already mentioned, 45% of companies fail to report on any form of incident response, while almost all companies (with Steelcase Inc. being the only exception pre-incident) report on their prospective risks. Not all statements disclosed are equally valuable to investors and regulators.

# 6 Concluding remarks

Transparent and informative cybersecurity disclosure benefits investors and regulators. We have examined up to six years of 10-K annual filings for 61 publicly-traded firms that experienced ransomware incidents. We manually labeled 7,681 cybersecurity-related statements extracted from the filings using a categorization developed through an iterative process inspired by grounded theory. Using the categorized data, we presented a method to analyze how firms' disclosure changes following a ransomware incident.

Our results indicate disclosure trends toward prospective risks, an increasing proportion of firms disclosing mitigation strategies, with 55% indicating incident response strategies, statements found to be significantly associated to variables that are directly linked to suffered impact – suggesting a lack of transparent information. Likewise, our research shows that firms struggle to connect types of prospective risks with materialized damages, let alone fail to preemptively realize the risks of ransomware – suggesting a lack of awareness of ongoing threats. These results have demonstrated the significant promise of analyzing such data deeper in future. Even now, the manually crafted dataset can help investors, regulators, and academics guide future analysis of cybersecurity risk in 10-K disclosures.

There are a few limitations to this research at its current point. There may be inconsistencies in the raw text examples extracted from the 10-Ks, as well as potential bias introduced by the coding methodology used. The broad nature of 10-K disclosures makes it challenging to determine whether a give statement is relevant to the topic of interest. An example of such is the intentional scoping out of privacy related statements (such as to do with GDPR and CCPA). While these statements can be relevant to cybersecurity disclosure, many of them were excluded due to a lack of focus on cybersecurity. However, we have mitigated this bias to a significant extend through the natural validation process embedded in our methodology, which was specifically designed to be inspired by grounded theory.

Another limitation of this project is the current view that each statement can only relate to one of the four primary categories. Previous cybersecurity incidents have become a secondary category, as is evident by Previous Cybersecurity Incident. However, depending on the interpretation, many statements can easily be divided into more than one primary category. This issue has been lessened due to altering the original category definitions, making each category more unique. However, specific statements are easily still applicable to more than one category.

We analyzed the presence of subcategories in both the PCR and CD statements. In future, we will expand the analysis to include subcategories for other categories. Deeper analysis required a sophisticated analysis method. Imploring methods such as Natural Language Processing (NLP), VSM, or utilizing a large language model (LLM) could improve this analysis. This improvement could come in various spaces, such as improving the ability to find subcategories that we may have missed or incorrectly grouped. Additionally, it could enhance the manual categorization of future 10-K disclosures.

# 7 Acknowledgments

We gratefully acknowledge support from the US National Science Foundation Award No. 2147505.

# References

Anderson, R. (2001). Why information security is hard – an economic perspective. *Seventeenth Annual Computer Security Applications Conference*, 0358. https://doi.org/10.1109/ACSAC.2001.991552

Anderson, R., & Moore, T. (2006). The economics of information security. *Science*, *314*(5799), 610–613. https://doi.org/10.1126/science.1130992

Aunshul Rege. (2025). *Critical infrastructure ransomware attacks (CIRA) dataset* (tech. rep. No. Version 12.13) (https://sites.temple.edu/care/cira/). Temple University.

Berkman, H., Jona, J., Lee, G., & Soderstrom, N. (2018). Cybersecurity awareness and market valuations. *Journal of Accounting and Public Policy*, *37*, 508–526. https://doi.org/10.1016/j.jaccpubpol.2018.10.003

Brown, S. V., & Tucker, J. W. (2011). Large-sample evidence on firms' year-over-year MD&A modifications. *Journal of Accounting Research*, *49*, 309–346. https://doi.org/10.1111/j.1475-679X.2010.00396.x

Campbell, J. L., Chen, H., Dhaliwal, D. S., min Lu, H., & Steele, L. B. (2014). The information content of mandatory risk factor disclosures in corporate filings. *Review of Accounting Studies*, *19*, 396–455. https://doi.org/10.1007/s11142-013-9258-3

Celeny, D., & Marćhal, L. (2023, October). Cyber risk and the cross-section of stock returns. https://doi.org/http://dx.doi.org/10.2139/ssrn.4587993

Cheong, A., Yoon, K., Cho, S., & No, W. G. (2021). Classifying the contents of cybersecurity risk disclosure through textual analysis and factor analysis. *Journal of Information Systems*, *35*, 179–194. https://doi.org/10.2308/ISYS-2020-031

Connolly, L., Wall, D., Lang, M., & Oddson, B. (2020). An empirical study of ransomware attacks on organizations: An assessment of severity and salient factors affecting vulnerability. *Journal of Cybersecurity*.

Eling, M., Ibragimov, R., & Ning, D. (2023). Time dynamics of cyber risk. *SSRN*. https://doi.org/10.2139/ssrn.4497621

Florackis, C., Weber, M., Michaely, R., & Louca, C. (2023). Cybersecurity risk. *The Review of Financial Studies*, *36*, 351–407. https://doi.org/https://doi.org/10.1093/rfs/hhac024

Gandal, N., Moore, T., Riordan, M., & Barnir, N. (2023). Empirically evaluating the effect of security precautions on cyber incidents. *Computers and Security*, *133*. https://doi.org/10.1016/j.cose.2023.103380

Gao, L., Calderon, T. G., & Tang, F. (2020). Public companies' cybersecurity risk disclosures. *International Journal of Accounting Information Systems*, *38*, 100468. https://doi.org/10.1016/j.accinf.2020.100468

Grier, C., Thomas, K., & Nicol, D. M. (2010). Barriers to security and privacy research in the web era. *Proceedings of the Workshop on Ethics in Computer Security Research*.

Hajizada, A., & Moore, T. (2023). On gaps in enterprise cyber attack reporting. *Proceedings - 8th IEEE European Symposium on Security and Privacy Workshops, Euro S and PW 2023*, 227–231. https://doi.org/10.1109/EuroSPW59978.2023.00030

Harry, C., & Gallagher, N. (2018). Classifying cyber events: A proposed taxonomy. *Journal of Information Warfare*, *17*(3), 17–31.

Jamilov, R., Rey, H., & Tahoun, A. (2021). The anatomy of cyber risk. http://www.nber.org/papers/w28906

Katz, D., & McIntosh, L. (2025). Corporate Governance Update: "Materiality" in America and Abroad. Retrieved July 23, 2025, from https://corpgov.law.harvard.edu/2021/05/01/corporate-governance-update-materiality-in-america-and-abroad/

King, A., & Gallagher, M. (2020, March). United States Cyberspace Solarium Commission Final Report [https://cybersolarium.org/wp-content/uploads/2022/05/CSC-Final-Report.pdf].

Kwon, J., & Johnson, M. E. (2014). Proactive versus reactive security investments in the healthcare sector. *Paper Knowledge . Toward a Media History of Documents*, *38*, 451–472.

Landis, R. J., & Koch, G. G. (1977). The measurement of observer agreement for categorical data. *Biometrics*, *33*, 159–174. https://doi.org/https://doi.org/10.2307/2529310

Li, F. (2008). Do stock market investors understand the risk sentiment of corporate annual reports? https://doi.org/10.2139/ssrn.898181

Li, H., No, W. G., & Boritz, J. E. (2020). Are external auditors concerned about cyber incidents? evidence from audit fees. *Auditing*, *39*, 151–171. https://doi.org/10.2308/ajpt-52593

Li, H., No, W. G., & Wang, T. (2018). SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. *International Journal of Accounting Information Systems*, *30*, 40–55. https://doi.org/10.1016/j.accinf.2018.06.003

Li, W., Leung, A., & Yue, W. (2023). Where is it in information security? The interrelationship among it investment, security awareness, and data breaches. *MIS Quarterly*, *47*, 317–342. https://doi.org/10.25300/misq/2022/15713

Liu, T., Sun, Y., Liu, Y., Gui, Y., Zhao, Y., Wang, D., & Shen, C. (2015). Abnormal traffic-indexed state estimation : A cyber – physical fusion approach for smart grid attack detection. *Future Generation Computer Systems*, *49*, 94–103. https://doi.org/10.1016/j.future.2014.10.002

Moore, T., Kenneally, E. E., Collett, M., & Thapa, P. (2019). Valuing cybersecurity research datasets.

Nagle, F., Ransbotham, S., & Westerman, G. (2017). The effects of security management on security events. *Workshop on the Economics of Information Security (WEIS)*, 1–18.

Nelson, K. K., & Pritchard, A. C. (2016). Carrot or stick? The shift from voluntary to mandatory disclosure of risk factors. *Journal of Empirical Legal Studies*, *13*, 266–297. https://doi.org/10.1111/jels.12115

Peng, J., & Li, C.-W. (2022). Security breaches and modifications on cybersecurity disclosures. *Journal of Accounting and Management Information Systems*, *21*. https://doi.org/10.24818/jamis.2022.03007

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity*, *2*, 121–135. https://doi.org/10.1093/cybsec/tyw001

Sarabi, A., Naghizadeh, P., Liu, Y., & Liu, M. (2016). Risky business : Fine-grained data breach prediction using business profiles. *Journal of Cybersecurity*, *2*, 15–28. https://doi.org/10.1093/cybsec/tyw004

Schlackl, F., Link, N., & Hoehle, H. (2022). Antecedents and consequences of data breaches: A systematic review. *Information and Management*, *59*, 103638. https://doi.org/10.1016/j.im.2022.103638

Tan, J., Jin, H., Zhang, H., Zhang, Y., Chang, D., Liu, X., & Zhang, H. (2023). A survey: When moving target defense meets game theory. *Computer Science Review*. https://doi.org/10.1016/j.cosrev.2023.100544

Telang, R. (2021). Could ransomware attacks ultimately benefit consumers? [https://hbr.org/2021/08/could-ransomware-attacks-ultimately-benefit-consumers]. *Harvard Business Review*.

U.S. Securities and Exchange Commission. (1999). Sec staff accounting bulletin: No. 99 – materiality [https://www.sec.gov/interps/account/sab99.htm].

U.S. Securities and Exchange Commission. (2011). Cf disclosure guidance: Topic no. 2 [https://www.sec.gov/rules/other/2018/34-83723.pdf].

U.S. Securities and Exchange Commission. (2018). Commission statement and guidance on public company cybersecurity disclosures [https://www.sec.gov/rules/interp/2018/33-10459.pdf].

U.S. Securities and Exchange Commission. (2023, July). Cybersecurity risk management, strategy, governance, and incident disclosure final rule [https://www.sec.gov/files/rules/final/2023/33-11216.pdf].

Wong, R. Y., Chong, A., & Aspegren, R. C. (2023). Privacy legislation as business risks: How GDPR and CCPA are represented in technology companies' investment risk disclosures. *Proceedings of the ACM on Human-Computer Interaction*, *7*. https://doi.org/10.1145/3579515

Woods, D. W., & Böhme, R. (2021). Systematization of knowledge: Quantifying cyber risk. *IEEE Symposium on Security and Privacy (S&P)*.

Woods, D. W., Böhme, R., Wolff, J., & Schwarcz, D. (2023). Lessons lost: Incident response in the age of cyber insurance and breach attorneys. *32nd USENIX Security Symposium (USENIX Security 23)*, 2259–2273. https://www.usenix.org/conference/usenixsecurity23/presentation/woods

Woods, D. W., & Seymour, S. (2023). Evidence-based cybersecurity policy? a meta-review of security control effectivness. *Journal of Cyber Policy*, *8*(3), 365–383. https://doi.org/10.1080/23738871.2024.2335461

Zhang, Y., & Smith, T. (2023). The impact of customer firm data breaches on the audit fees of their suppliers. *International Journal of Accounting Information Systems*, *50*, 100628. https://doi.org/10.1016/j.accinf.2023.100628