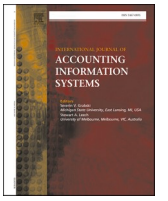
International Journal of Accounting Information Systems 57 (2026) 100775

Contents lists available at ScienceDirect

International Journal of Accounting Information Systems

journal homepage: www.elsevier.com/locate/accinf



Mandatory cybersecurity disclosure: Early evidence from 10-K reports

Elina Haapamäki [a,*], Jukka Sihvonen [b]

[a] University of Vaasa, School of Accounting and Finance, P.O. Box 700, 65200 Vaasa, Finland
[b] Aalto University, Department of Accounting, P.O. Box 11000 (Otakaari 1B), 00076 AALTO, Finland

ARTICLE INFO

JEL classifications:
D8
G14
K22
K24
M41
M48

Keywords:
Cybersecurity
Risk disclosure
Mandatory
Regulation
Textual analysis
Event study

ABSTRACT

This study provides early evidence on U.S. public companies' responses to the SEC's 2023 rule requiring detailed annual disclosures on cybersecurity risk management and governance. Using textual analysis of 3,440 Item 1C disclosures in 10-K filings from 2024, we investigate the determinants of these newly required disclosure characteristics and assess market reactions. Results show variation in disclosure quality—proxied by length, redundancy, and specificity—primarily driven by firm size, financial performance, auditor quality, cybersecurity and litigation risk exposures, and peer practices, though these factors collectively explain only moderate variance. Past cyber incidents, firm digitalization, material IT weaknesses, and tech-firm status show no influence, suggesting strategic discretion persists even under a mandate. Additional analyses show that Item 1C represents new disclosure content rather than a relocation of existing risk disclosures. To assess market reactions, we utilize event studies, analyze cybersecurity-related discussions in earnings call transcripts, and examine investor attention through filing download activity. The results indicate a minimal response from both investors and analysts to these newly mandated disclosures. These insights hold important implications for policymakers regarding the balance between regulatory burden and informational value, as jurisdictions globally adopt similar cybersecurity disclosure policies.

1. Introduction

> *"Today, cybersecurity is an emerging risk with which public issuers increasingly must contend. Investors want to know more about how issuers are managing those growing risks… I think companies and investors alike would benefit if this information were required in a consistent, comparable, and decision-useful manner."*— SEC Chair Gary Gensler, March 2022

Cybersecurity risks pose a significant threat to organizations, the global economy, and national security, receiving increasing attention from stakeholders and regulators worldwide (WEF, 2024). In response, the regulators are implementing increasingly stringent requirements to ensure organizations establish appropriate governance and transparency regarding their cybersecurity management. This paper examines a significant regulatory development in the United States: The Securities and Exchange Commission's recent cybersecurity reporting mandate (SEC, 2023). This mandate introduced comprehensive rules requiring public companies to disclose detailed information on their cybersecurity risk management, strategy, and governance practices in their 10-K

* Corresponding author.
E-mail addresses: elihaa@uwasa.fi (E. Haapamäki), jukka.sihvonen@aalto.fi (J. Sihvonen).

https://doi.org/10.1016/j.accinf.2026.100775
Received 20 October 2025; Received in revised form 28 March 2026; Accepted 1 April 2026
Available online 9 April 2026

annual reports (Regulation S-K Item 106), as well as mandating timely disclosure of material cybersecurity incidents via Form 8-K. This study specifically investigates the initial wave of annual cybersecurity disclosures, providing important insights into how firms adapt from voluntary disclosure regime to new, standardized transparency requirements and whether these mandatory annual disclosures achieve their intended policy objective of enhancing market transparency. By providing empirical evidence on both firm disclosure practices and market outcomes from one of the first major economies to mandate public cybersecurity disclosures, we respond to Leuz's (2018) call for evidence-based policymaking with insights that can inform and enhance cybersecurity regulations worldwide.

The 2023 SEC cybersecurity mandate (Regulation S-K Item 106) received 150 public comment letters[1] from different stakeholder groups. Investor advocates and the SEC suggested that mandatory disclosure would reduce information asymmetry and mispricing by providing consistent, comparable and useful information for decision-making purposes. Proponents such as the California Public Employees' Retirement System (CalPERS), Better Markets, and the Principles for Responsible Investment (PRI) characterized pre-regulation disclosures as scattered and unpredictable, which diminished their utility for investment decisions (SEC comment letters, File No. S7-09–22, 2022).

The following arguments were presented by industry opponents. The Chamber of Commerce raised concern about high compliance costs. The Business Roundtable and the Securities Industry and Financial Markets Association (SIFMA) warned that detailed disclosures could expose security architectures to malicious actors, creating a transparency-security tradeoff. The U.S. Small Business Administration (SBA) Office of Advocacy emphasized that smaller and emerging growth companies would bear a disproportionate burden, given their limited revenue and lack of specialized compliance expertise (SEC comment letters, File No. S7-09–22, 2022). These contrasting positions reflect a broader empirical question in the disclosure literature: whether mandatory regimes enhance the informational value of risk disclosures or impose compliance costs that exceed their benefits.

Prior literature provides a foundation for understanding corporate disclosure practices related to risk. Studies on annual reports document a trend toward increased length and complexity, often driven by regulatory changes such as the mandatory inclusion of risk factors (Item 1A) since 2005 (Dyer et al., 2017). Research indicates that while risk factor disclosures can provide meaningful information about risk exposures and assessments (Campbell et al., 2014; Kravet & Muslu, 2013), their informativeness varies, with more specific disclosures linked to stronger market responses and implicitly to lower information asymmetry (Hope et al., 2016). The shift to a *mandatory* and *standardized* regime for cybersecurity governance disclosures under Item 1C, however, presents a distinct empirical setting. Previous research on voluntary cybersecurity disclosures found that such disclosures increased following earlier SEC guidance (Gao et al., 2020; SEC, 2011), were influenced by factors such as industry characteristics and company size (Gao et al., 2020), and were sometimes predictive of future breaches (Wang et al., 2013). These voluntary disclosures, however, are subject to managerial discretion regarding whether and what to disclose. Studies on event-driven disclosures demonstrate that markets typically react negatively to cyber breach announcements (Spanos & Angelis, 2016), especially those disclosed via Form 8-K (Gordon et al., 2024), reflecting investor sensitivity to the timeliness and materiality of the incidents.

Despite this body of research, notable gaps remain, which this study aims to address by focusing on newly mandated Item 1C 'Cybersecurity' disclosures in annual 10-K reports. First, while research on general risk factors (Item 1A) highlights firm discretion in disclosure specificity (Campbell et al., 2014; Hope et al., 2016), the SEC's 2023 rule sharply constrains managerial discretion. Analyzing this new regulatory environment allows us to reassess classic disclosure determinants, such as firm size, profitability, and auditor quality, under compulsory conditions and to test whether factors that previously encouraged voluntary disclosure (e.g., breach history, technology focus) remain influential once reporting is obligatory. We also examine whether Item 1C represents new disclosure content or a relocation of existing cybersecurity information from other sections of the 10-K. We aim to extend disclosure theory to cybersecurity governance, where detailed, technical information must now be reported irrespective of firms' strategic preferences. Disclosure theory posits that credible disclosures reduce information asymmetry between managers and investors (Verrecchia, 1983; Diamond & Verrecchia, 1991), though mandatory regimes may encourage firms to produce standardized content that satisfies legal requirements without revealing sensitive information (Dye, 2001; Beyer et al., 2010). Applying this framework to the 2023 SEC mandate yields two competing predictions. The transparency channel predicts that newly required disclosures reduce information asymmetry and improve investor assessments of firm resilience. The compliance channel predicts that mandatory regimes produce standardized, minimally informative content with limited incremental value to investors. These two channels frame this study's central policy question and motivate the empirical tests that follow.

In this study, cybersecurity governance refers to the firm-level processes, board oversight structures, and management roles through which companies assess and manage cybersecurity risks. Applying disclosure theory to this context yields a prediction that was not present in previous mandatory disclosure scenarios: proprietary costs do not arise from market competitors, but rather from adversaries who could exploit disclosed security architectures. This implies that less specific disclosure may be a sign of rational risk management rather than poor governance. Firms may strategically limit disclosure to protect security. This distinguishes cybersecurity disclosure from other risk disclosures: in most contexts, comprehensive disclosure signals good governance, but in cybersecurity contexts, limited disclosure may reflect a deliberate security decision. We suggest that cybersecurity disclosure is distinctive because firms face a direct tradeoff between transparency and security. While market reactions to discrete breach announcements are well documented (Spanos & Angelis, 2016; Gordon et al., 2024), how investors process and react to *routine, annual, and comprehensive* mandated cybersecurity disclosures about ongoing risk management and governance remains largely unexplored. Addressing this gap

[1] SEC Website – Public Comments Portal:https://www.sec.gov/comments/s7-09–22/s70922.htm. This contains all public comments submitted in response to the SEC's proposed cybersecurity rules (File Number S7-09–22, titled "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure").

contributes to assessing whether the new cybersecurity disclosure regulations effectively inform investors or merely generate perfunctory compliance with limited informational utility beyond what is conveyed by event-driven 8-K filings.

The transition from voluntary to mandatory cybersecurity disclosure alters managerial discretion and information-sharing dynamics. Mandatory regimes may encourage firms to disclose cybersecurity risks regardless of actual risk levels (Li et al., 2018). The objective of the 2023 SEC mandate (Regulation S-K Item 106) is to eliminate reporting discretion, allowing examination of whether factors that influenced voluntary disclosure continue to affect disclosure quality under mandatory requirements. Cybersecurity disclosure differs from other mandatory risk disclosures because of its technical complexity and proprietary information sensitivities. There is concern that disclosing too much information could provide potential hackers with a roadmap for successful attacks (Berkman et al., 2018). Firms may therefore use boilerplate language to limit legal exposure despite regulatory demands for specificity. Item 1C is distinctive in requiring firms to report on internal governance and management processes, not merely general risk factors.

The central question motivating this study is whether the newly mandated Item 1C disclosures achieve their intended policy objective of enhancing market transparency. We address this question through two empirical tests. First, we examine what factors determine the characteristics and quality of these newly mandated cybersecurity disclosures (RQ1). Second, we investigate how market participants respond to these routine annual cybersecurity disclosures, distinct from incident-specific 8-K reports (RQ2). We incorporate early industry perspectives because quantitative data can show what changed after the 2023 SEC mandate, but expert perspectives explain why firms may exercise strategic discretion in reporting. Industry experts view the mandate's primary value as formalizing internal documentation rather than signaling information to markets.

Our findings indicate that while firms largely complied with the mandate, disclosure characteristics vary significantly, driven primarily by firm size as well as financial performance, auditor quality, cybersecurity and litigation risk exposures, and peer practices. Notably, factors such as past cyber incidents, IT weaknesses, firm digitalization, or tech status show no significant influence on the characteristics of these annual governance disclosures, suggesting strategic discretion in how firms frame their ongoing cybersecurity posture even under a mandate. Firm-specific factors collectively account for only a moderate proportion of the total variance observed in disclosure quality across the sample. Despite these new, detailed annual disclosures, we find minimal evidence of market response or increased analyst attention. The confirmatory channel provides a theoretical explanation for the minimal market response. Gigler and Hemmer (1998) argue that in a well-functioning disclosure regime, markets discount mandatory annual reports because material information has already been conveyed through timely signals. The minimal market response is consistent with this framework, though we cannot rule out that investors regard these disclosures as uninformative. Taken together, our results contribute to the understanding of mandatory cybersecurity reporting practices, challenging whether they effectively enhance market transparency for emerging risks like cyber threats.

The remainder of the article proceeds as follows: Section 2 provides a detailed literature review and formulates the research questions. Section 3 outlines the research methodology, including data collection, textual analysis techniques, and statistical models employed. Section 4 presents empirical findings concerning the determinants of disclosure characteristics. Section 5 discusses market reactions through an event study and supplementary analyses of investor and analyst attention. Section 6 summarizes the key conclusions, implications for regulatory policy, and suggestions for future research.

2. Literature review and research questions

2.1. SEC and cybersecurity disclosure

Cybersecurity disclosure requirements in the United States have evolved through three significant regulatory interventions. In

Table 1
Examples of SEC cybersecurity disclosure channels (AT&T Inc.).

Disclosure: Form 8-K (Item 1.05)
Focus: Material incident (event-driven, timely)
Excerpt:"*On April 19, 2024, AT&T Inc. learned that a threat actor claimed to have unlawfully accessed and copied AT&T call logs. AT&T immediately activated its incident response process to investigate and retained external cybersecurity experts to assist. Based on its investigation, AT&T believes that threat actors unlawfully accessed an AT&T workspace on a third-party cloud platform and, between April 14 and April 25, 2024, exfiltrated files containing AT&T records of customer call and text interactions.*"

Disclosure: 10-K Item 1A (Risk Factors)
Focus: General risk factor (annual, broad, forward-looking)
Excerpt: "*Cyberattacks impacting our networks or systems may have a material adverse effect on our operations. Cyberattacks including through the use of malware, computer viruses, distributed denial of services attacks, ransomware attacks, credential harvesting, social engineering and other means for obtaining unauthorized access to or disrupting the operation of our networks and systems and those of our suppliers, vendors and other service providers could have a material adverse effect on our operations.*"

Disclosure: 10-K Item 1C (Cybersecurity)
Focus: Governance processes (annual, structured)
Excerpt: "*Board and Audit Committee Oversight. Our Board of Directors has delegated to the Audit Committee the oversight responsibility to review and discuss with management the Company's privacy and data security, including cybersecurity, risk exposures, policies and practices, and the steps management has taken to detect, monitor and control such risks. […] We maintain a Chief Security Office, which is charged with management-level responsibility for all aspects of network and information security within the Company. Led by our CISO and comprised of a large team of highly trained security professionals across multiple countries.*"

Note: Excerpts are from AT&T Inc. SEC filings (CIK 0000732717). Item 1A and Item 1C, filed February 2024, are from the 10-K for fiscal year ending December 31, 2023. The 8-K report, filed July 12, 2024, is a subsequent incident disclosed under the new Item 1.05 requirement.

2011, the SEC issued CF Disclosure Guidance: Topic No. 2-Cybersecurity, guiding public companies on how to disclose potential cybersecurity risks and cyber incidents (Gao et al., 2020). The SEC subsequently approved an interpretive guidance in 2018, emphasizing sufficient disclosure controls and procedures while prohibiting insider trading based on non-public information about cyber incidents. Although unanimously approved by SEC commissioners, several commissioners considered the 2018 guidance insufficient (Gao et al., 2020). Consequently, in July 2023, the SEC fundamentally strengthened and formalized these requirements by adopting rules that represent a shift from guidance to a binding mandate. These rules require (1) rapid and detailed public disclosure of material cybersecurity incidents via Form 8-K and (2) extensive annual reporting on cybersecurity risk management, strategy, and governance in Form 10-K (SEC, 2023). These rules extend to foreign private issuers, who must provide comparable disclosures.

The 2023 rules introduce Regulation S-K Item 106, which forms the basis for the annual disclosures that are the focus of this study. Item 106 requires companies to describe their processes for assessing, identifying, and managing material cybersecurity risks, as well as the material impact or reasonably likely material impact of cybersecurity threats and past incidents. Item 106 further mandates that registrants detail the board of directors' oversight of cybersecurity risks and management's role and expertise in assessing and managing material cybersecurity threats (SEC, 2023). These standardized cybersecurity disclosure requirements, found under Item 1C of Form 10-K, add to the expanding mandatory content in annual filings and are effective for annual reports covering fiscal years ending on or after December 15, 2023. This transition to a compulsory regime is anticipated to reduce managerial discretion in *whether* and *how* to disclose foundational aspects of their cybersecurity risk management and governance, offering a new lens through which to examine disclosure practices.

Table 1 illustrates the distinct focus of these three cybersecurity disclosure channels using excerpts from AT&T Inc.'s SEC filings. Form 8-K (Item 1.05) provides an event-driven account of a specific incident, the unauthorized access to customer call records discovered in April 2024. Item 1A in the annual 10-K (filed February 2024 for fiscal year 2023) discusses cybersecurity as a general risk factor, describing the firm's exposure to cyberattacks in broad, forward-looking terms. Item 1C in the same 10-K describes the governance structures and management processes through which the firm oversees cybersecurity risk, including board committee responsibilities, the CISO's role, and organizational security functions. The contrast between these three channels motivates our research questions: while markets have been shown to react to incident-driven 8-K disclosures (Gordon et al., 2024), the informational value of routine governance disclosures in Item 1C remains unexplored.

2.1.1. Stakeholder perspectives on the mandate

The comment letters received by the SEC addressed the potential costs and benefits of mandatory cybersecurity disclosure. Analysis of comment letters[2] and the Final Rule document (Release No. 33–11216) brought up two perspectives that frame this study's research questions. Supporters, primarily investor advocates, emphasized transparency benefits. The SEC's Investor Advisory Committee characterized cybersecurity risk governance as material to investment decision-making. The Principles for Responsible Investment (PRI) contended that existing disclosures do not provide investors with the information necessary to evaluate whether companies have adequate governance structures. The SEC stated that mandatory disclosure would reduce information asymmetry and securities mispricing while lowering investor search and information processing costs (SEC, 2023, Section IV.C.1). Major accounting firms (PwC, Ernst & Young, and BDO) supported the mandate but advocated for clearer definitional standards for required disclosures (SEC, 2023, Sections II.C.1.b, II.C.2.b). This position likely reflects both the expanded advisory opportunities that new reporting requirements create and the practical need for auditable criteria.

Opponents, primarily industry associations and corporate issuers, raised concerns about compliance burden and unintended consequences. The American Bar Association, Business Roundtable, and Chamber of Commerce warned that detailed disclosure could increase a company's vulnerability to cyberattacks by revealing security architectures to threat actors. Others argued the requirements would force companies to model their cybersecurity policies on the rule's disclosure elements rather than practices suited to their context (Bank Policy Institute; New York Stock Exchange (NYSE); SIFMA). The SBA Office of Advocacy expressed concern that smaller firms face disproportionate burden given limited resources and expertise.

2.1.2. Industry expert views on the mandate

To gain practitioner insights into this new regulatory environment, we conducted preliminary interviews with four industry experts[3] who possess deep knowledge of both cybersecurity risk management and corporate disclosure practices. We conducted semi-structured interviews to understand how practitioners navigate this new regulatory environment and to inform our empirical research design. Each expert reviewed representative Item 1C disclosures and consistently observed that disclosure contents are predominantly compliance-oriented rather than operationally informative. They attributed this genericity to two primary factors: litigation concerns that could encourage vague language, and differences in data sensitivity across firms, where specific disclosures could compromise competitive positioning or security posture. Experts expressed particular concern about resource disparities, noting

[2] We analyzed SEC press releases (2022–39, 2023–139) and the Final Rule document (Release No. 33–11216), focusing on sections that synthesize public comments (II.C.1.b, II.C.2.b, II.G.2, IV.C.1–2, VI.B). This analysis encompassed positions from commenters, including investor advocates (CalPERS, Better Markets, PRI), industry associations (Chamber of Commerce, Business Roundtable), accounting firms (PwC, Ernst & Young, BDO), professional bodies (AICPA, ABA), and exchanges (NYSE, Nasdaq).

[3] The four industry experts who were interviewed are: i) a Chief Research Officer of a publicly listed cybersecurity provider, ii) a board member of another public cybersecurity provider, iii) a CEO of a cybersecurity industry association, and iv) a CFO of a publicly listed firm who serves on an audit committee.

that smaller companies face identical disclosure requirements despite limited resources, while larger firms' detailed reports establish unrealistic standards. One industry expert noted:

> *"The new disclosure rules may be unreasonable for smaller companies with limited resources. Reports prepared by large companies can provide an unrealistic view of the average company's actual cybersecurity level."*

While experts acknowledged the SEC mandate provides value by formalizing cybersecurity governance documentation, they emphasized these benefits are primarily organizational rather than market-facing, serving internal accountability and board oversight rather than investor decision-making. Indeed, experts consistently observed that firms approach these disclosures as regulatory obligations to be satisfied rather than opportunities to communicate meaningful information about their cybersecurity posture to investors.

2.2. Theoretical assumptions

As introduced in Section 1, disclosure theory yields competing predictions for the 2023 SEC mandate through the transparency channel (Verrecchia, 1983; Diamond & Verrecchia, 1991) and the compliance channel (Dye, 2001; Beyer et al., 2010). A third theoretical perspective, the confirmatory channel (Gigler & Hemmer, 1998), suggests that in a well-functioning regime, the market may discount annual reports because material information has already been preempted by timely, event-driven signals. We develop these predictions in the context of existing disclosure research.

Annual reports, particularly through the SEC-mandated Form 10-K, have grown significantly longer and more complex over recent decades, driven by evolving regulatory demands and managerial discretion. Research utilizing textual analysis shows marked trends of increasing disclosure length, reduced readability, and heightened use of standardized language (Dyer et al., 2017; Lang & Stice-Lawrence, 2015). Quantifying this expansion using topic modeling, Dyer et al. (2017) documented a 150% increase in 10-K length between 1996–2013, attributing this growth primarily to expanded discussions of risk factors, internal controls, and fair value accounting. This dramatic increase followed regulatory interventions, for example the SEC's 2005 mandate requiring firms to include risk factor disclosures (Item 1A).

Investigating why some firms' 10-Ks are longer than others, Cazier and Pfeiffer (2016) decomposed variations in 10-K length into three factors: operating complexity, disclosure redundancy, and managerial discretion. Their analysis showed that while firm complexity and mandated disclosure redundancy explain significant portions of length variation, the largest component remains discretionary. This finding highlights the tension in corporate disclosure practices: even under identical regulatory requirements, managers differ substantially in disclosure detail and approach. Such variation raises important questions about the determinants of disclosure practices when regulations mandate specific types of information, yet leave considerable room for managerial judgment regarding implementation (Cazier & Pfeiffer, 2016).

2.3. Risk factor disclosures in 10-K filings

Given the significant contribution of risk factors to the growth in 10-K length, a body of research has examined the informational content and market impact of these disclosures. The introduction of mandatory risk factor disclosures aimed to enhance investor understanding of significant firm-specific risks, and empirical evidence confirms these disclosures provide meaningful incremental information. Kravet & Muslu (2013) demonstrate that increases in risk-related language in 10-Ks are associated with higher stock return volatility and trading volume around filing dates, indicating that investors update their risk assessments based on narrative disclosures. Similarly, Campbell et al. (2014) document that firms facing greater inherent risks provide more extensive risk factor discussions, and these disclosures are associated with market metrics including systematic risk, idiosyncratic risk, and firm value.

The specificity and informativeness of risk disclosures appear particularly consequential for investors. Hope et al. (2016) develop a measure of disclosure specificity using Named Entity Recognition and find that, controlling for other factors, more specific risk disclosures are associated with stronger market reactions to 10-K filings and improve analysts' ability to assess risk—both of which suggest potential reductions in information asymmetry. These findings align with research by Bao and Datta (2014), who show that not all risk disclosures equally influence investor risk perceptions. These studies suggest that qualitative aspects of disclosure significantly impact how markets process risk information.

Despite the potential value of detailed risk disclosures, concerns persist about boilerplate language diminishing their usefulness. Beatty et al. (2019) report that market reactions to risk factor disclosures weakened following the 2008 financial crisis, implying that investors may discount lengthy, generic risk lists. Examining the legal consequences of disclosure quality, Cazier et al. (2021) find that courts and regulators are actually less likely to deem lengthy and standardized disclosures inadequate when assessing corporate liability. These studies underscore the tension between specificity and materiality in risk reporting, which become particularly relevant when examining specialized risks like cybersecurity where technical complexity and proprietary concerns may incentivize vague or standardized language.

The 2023 SEC mandate (Regulation S-K, Item 106) provides an opportunity to examine traditional disclosure theories in a new context. The transparency channel, proposed by Verrecchia (1983) and Diamond and Verrecchia (1991), predicts that newly required, credible disclosures should reduce information asymmetry and improve investor assessments of firm resilience. The compliance channel, drawing on Beyer et al. (2010) and Dye (2001), predicts that mandatory regimes may instead produce standardized, minimally informative content that offers little incremental value to investors. This study applies these two theoretical channels to cybersecurity disclosure and examines how firms navigate the transparency-security tradeoff under a mandatory regime.

The transparency and compliance channels introduced in Section 1 take on a distinct form in cybersecurity disclosure. Unlike other risk reporting contexts, proprietary costs arise not from market competitors but from adversaries who could exploit disclosed security architectures. This study examines how firms navigate this transparency-security tradeoff under the mandatory regime.

2.4. Voluntary cybersecurity disclosure practices

Prior to explicit regulatory mandates, cybersecurity disclosures within 10-K reports evolved through several distinct phases. Initially, these disclosures were guided indirectly by broader regulatory frameworks. Gordon et al. (2006) provide early evidence that the Sarbanes-Oxley Act indirectly encouraged firms to enhance voluntary disclosures of information security activities, even without explicit cybersecurity disclosure mandates.

The SEC (2011) guidance marked a significant inflection point in cybersecurity disclosure practices. Berkman et al. (2018) examined increased cybersecurity disclosure following this guidance and found that the market positively values cybersecurity awareness in corporate disclosures. Their analysis showed that disclosure tone matters; a more negative tone in cyber disclosures is associated with lower market values. These findings persisted after controlling for IT governance quality and firms' overall disclosure characteristics, suggesting that investors independently value the nature and quality of cybersecurity disclosures, not merely their presence.

The evolution of cybersecurity disclosures before and after regulatory guidance provides valuable insights into the information content of these disclosures. Li et al. (2018) examine 10-K filings and find that prior to the SEC (2011) guidance, relatively few firms disclosed cybersecurity risks, but when they did, it was usually because they faced genuine threats—these disclosures were predictive of future cyber incidents (Wang et al., 2013). This suggests that, absent explicit mandates, only firms with significant cyber risk tended to voluntarily report it, making such disclosures a valuable risk signal. After the 2011 guidance, however, cybersecurity risk factor disclosures became far more common across all firms. The association between having disclosed cyber risk and subsequently experiencing a breach weakened in the post-guidance period, indicating that the guidance successfully spurred broader disclosure but potentially diluted its informational content.

Investigating the determinants of voluntary cybersecurity disclosures, Gao et al. (2020) conduct a comprehensive study of public companies' cybersecurity risk disclosures from 2007 to 2018 and document several key trends. The prevalence and length of cyber risk disclosures rose significantly over that period, with a noticeable uptick following the 2011 SEC guidance. They identify several factors driving these voluntary disclosures: industry characteristics (firms in high-tech and data-intensive industries tended to report more cyber risk), firm size (larger firms provided more extensive cyber disclosures), and firms' own experience with cybersecurity incidents (prior breaches led to increased disclosure).

The SEC's role in shaping disclosure practices extended beyond formal guidance to include enforcement actions through comment letters. Examining regulatory enforcement mechanisms, Calderon and Gao (2022) analyze how SEC comment letters addressing disclosure deficiencies influenced cybersecurity reporting from 2004 to 2019. They documented a significant increase in SEC comment letters concerning cybersecurity in 2011, coinciding with the issuance of new guidance, but surprisingly found no similar surge following SEC (2018) updated guidance. Their findings reveal that firms took an average of 26 days to respond to SEC comment letters, with only about 10 percent meeting the SEC's recommended 10-day timeframe. Calderon and Gao (2022) highlight the SEC's evolving enforcement and its influence on disclosure practices even before formal mandates were established.

Collectively, these studies on voluntary and guidance-influenced disclosures offer valuable insights into firms' cybersecurity reporting incentives when discretion is high. However, the 2023 SEC *mandatory* rule creates a new landscape where compliance with standardized annual reporting on risk management and governance is compulsory, potentially altering observed disclosure patterns and the influence of their determinants. This transition to a mandatory regime for cybersecurity governance disclosures, therefore, leads to our first research question:

RQ1: What factors determine the characteristics of mandatory cybersecurity disclosures?

2.5. Market reactions to event-driven cybersecurity disclosures

While the studies above examine routine cybersecurity disclosures in annual reports, a parallel stream of research investigates market responses to cybersecurity breach disclosures—typically conveyed through discrete events such as media announcements or SEC Form 8-K filings. This literature provides important insights into how investors process and value cybersecurity information. Spanos & Angelis (2016) conduct a systematic review of 45 event studies and conclude that in about three-quarters of cases, a reported cyber breach leads to a significantly negative abnormal stock return for the affected firm. This finding aligns with the intuition that breaches impose real costs (remediation expenses, legal liabilities, reputational harm, lost business) that investors price into firm valuations.

Despite this general pattern, the literature documents considerable heterogeneity in market outcomes following breach disclosures. Several studies report only modest or non-significant stock price effects for certain types of breaches. For example, Campbell et al. (2003) report that breaches involving unauthorized access to sensitive customer or proprietary data trigger significant negative returns, whereas events like website defacements or denial-of-service attacks typically do not. Cavusoglu et al. (2004) further identify firm-specific and contextual factors that influence market reactions. These findings suggest that investors differentiate between cybersecurity incidents based on their perceived severity and long-term implications.

The manner and timing of disclosure appears to significantly influence market reactions to cybersecurity incidents. Gordon et al. (2024) provide direct evidence by comparing breaches disclosed in a Form 8-K versus breaches disclosed through other means (such as

later inclusion in a 10-K or through media sources). They find that breaches disclosed via Form 8-K trigger significantly stronger immediate negative stock price reactions, but are followed by a more pronounced post-event recovery, compared to breaches disclosed through other channels. This pattern suggests that 8-K filings signal the materiality and seriousness of a breach, prompting a sharper initial re-pricing of the stock and a quicker investor adjustment thereafter.

Beyond the immediate reaction to breach announcements, markets also appear to monitor firms' subsequent disclosures regarding cybersecurity. Chen et al. (2023) provide evidence that investors assess how firms adjust risk disclosures post-breach. They show that when a breached firm's subsequent 10-K fails to increase its cybersecurity risk disclosures (or actually reduces the discussion), investors respond with significantly negative abnormal returns. In contrast, firms that expand their disclosures as expected experience neutral market reactions to the 10-K filing. This behavior implies that market participants use disclosure changes as signals about management's approach to cybersecurity: a firm that downplays cybersecurity risks after suffering a breach may be interpreted as either not fully addressing the issue or withholding information, thereby eroding investor confidence (Chen et al., 2023).

Jiang et al. (2022) complement this perspective by analyzing how firms decide whether and how much to disclose about cybersecurity risks after a breach. Their study shows that disclosure behavior is shaped by a combination of prior breach experience, industry risk, and market reactions. Firms with multiple breaches or those facing negative investor reactions are more likely to increase their disclosures, whereas firms in high-tech or highly regulated industries often provide more extensive disclosures regardless of breach severity. The authors interpret this behavior as strategic, that is, balancing the benefits of transparency against concerns about competitive harm or legal liability.

In addition, using a sample of cybersecurity breaches from 2005 to 2018, Chen et al. (2025) find that analysts' earnings forecasts become less accurate and more dispersed following breaches. Cross-sectional analyses reveal these adverse effects are stronger for firms in volatile business environments, high-growth industries, and those with poor internal information environments. However, the effects are mitigated when management provides more earnings guidance. These findings suggest that cybersecurity breaches create economic and reporting complexities that impair analysts' forecasting ability.

The established market sensitivity to material incident disclosures, which are now formally channeled through timely 8-K filings under the 2023 SEC rule, emphasizes the importance of cybersecurity events. However, these event-driven disclosures differ in their nature, timing, and scope from the newly mandated, routine, and comprehensive annual disclosures regarding ongoing cybersecurity risk management, strategy, and governance practices required under Item 1C of Form 10-K. While markets clearly react to announcements of specific, material cybersecurity incidents (often via 8-K filings), this leads to our second research question:

RQ2: How do market participants respond to routine cybersecurity disclosures in annual filings?

2.6. Research gap

The 2023 SEC mandate departs from prior guidance-based approaches (SEC 2011; 2018) by requiring detailed, standardized annual cybersecurity disclosures under Regulation S-K Item 106, aiming to address known shortcomings in voluntary reporting (Gao et al., 2020; Li et al., 2018). Although there is extensive research on general risk factor disclosures (Item 1A)—highlighting managerial discretion and boilerplate concerns (Beatty et al., 2019; Cazier & Pfeiffer, 2016; Dyer et al., 2017)—the relevance of these findings to the specific domain of cybersecurity under this new, comprehensive annual mandate remains uncertain, given cybersecurity's technical complexity, proprietary information sensitivities, and evolving litigation risks. Our study addresses this gap, responding directly to calls for research on regulatory impacts in this domain (Haapamäki & Sihvonen, 2019; Walton et al., 2021), and evidence-based policy-making in general (Leuz, 2018). Specifically, we investigate how firms balance between Item 106 requirements and strategic disclosure by examining the determinants and variations in these newly required disclosures (RQ1). Furthermore, current literature predominantly focuses on market reactions to reactive, event-driven breach announcements (Spanos & Angelis, 2016; Gordon et al., 2024), many of which would now fall under the new 8-K incident reporting rules. This creates a distinct gap concerning the market interpretation of proactive, routine, standardized annual disclosures about cybersecurity risk management and governance. In RQ2, we address this gap by evaluating whether investors can discern meaningful signals about cybersecurity governance quality and risk management effectiveness from these annual disclosures, or regard them as low-information compliance statements, particularly in light of the more immediate 8-K incident reports.

3. Research design

3.1. Empirical model

We first examine the firm-level determinants of cybersecurity disclosure characteristics by estimating cross-sectional regressions for textual characteristics of Item 1C disclosures. Our analysis models three key disclosure characteristics (*Words*, *Bloat*, and *Specificity*, defined below) as functions of lagged firm attributes. Specifically, we estimate the following regression model:

$$DisclosureMetric_t = \alpha + \beta(Financials)_{t\text{-}1} + \gamma(AnnualReport)_{t\text{-}1} + \delta(Technology)_{t\text{-}1} + \lambda(Prior\ Disclosure)_{t\text{-}1} + \theta PeerAvg_t + SizeFE + IndustryFE + \epsilon_t \quad (1)$$

where $DisclosureMetric_t$ represents a textual characteristic of Item 1C disclosure filed in year t (2024); firm subscripts are omitted for brevity. Each dependent variable is analyzed in a separate regression with the same set of explanatory variables. The inclusion of $PriorDisclosure_{t\text{-}1}$ is important for isolating the incremental impact of the SEC mandate, as it controls for cybersecurity information

already available to market participants through voluntary disclosures made under prior SEC guidance (SEC 2011; 2018). All explanatory variables, except peer-average disclosure metrics, are measured as of the prior year (*t-1*) to mitigate simultaneity and reverse causality concerns. For instance, we use 2023 profitability to explain 2024 disclosures, thereby avoiding the use of current-year performance that could be influenced by the same cyber events prompting more extensive disclosure. We incorporate industry fixed effects using the Fama-French 12-industry classification to control for unobserved industry-specific disclosure norms. Additionally, we include firm-size fixed effects by grouping firms into distinct size buckets based on their rounded log-10 market capitalization, accounting for non-parametric size-related influences on disclosure practices (Gopalan et al., 2023). Standard errors are heteroskedasticity-robust, and our results are consistent when clustering by industry. This empirical framework enables us to identify firm characteristics cross-sectionally associated with more extensive or higher-quality cybersecurity disclosures.

3.2. Sample selection

Our sample is drawn from U.S. public companies' Form 10-K annual reports filed in 2024 – the first year of mandatory cybersecurity Item 1C disclosures mandated by Regulation S-K 106. Initially, we identify all 10-K filings from 2024 containing an Item 1C section and retrieve their full texts from Calcbench, a provider of parsed financial filings. We exclude disclosures provided solely by reference and those indicating omitted disclosure. Subsequently, we merge the resulting filings with Compustat to obtain financial statement data and Audit Analytics to incorporate firm-level details on firm type, prior cybersecurity incidents, and internal control deficiencies. Filings unmatched with these databases are excluded, resulting in an initial sample of 5,248. We further eliminate 1,497 observations not meeting minimum financial data requirements (total assets and sales of at least one million dollars, or missing data for net income, common equity, or stock price). Additionally, we remove 311 observations representing blank shells, funds, trusts, asset-backed securities, REITs, and subsidiaries without tickers. After filtering, our final sample comprises 3,440 firm-year observations. Table 2 reports the sample composition.

3.3. Dependent variables

We use three textual constructs to quantify each firm's Item 1C disclosure. These measures capture the length, verbosity, and specificity of the disclosure.

Words. We define the total amount of disclosure dedicated to cybersecurity by the word count of the Item 1C section. As word counts are count data, we model this measure using Poisson regression. This measure serves as a basic indicator of disclosure extensiveness (Campbell et al., 2014; Kravet & Muslu, 2013).

Bloat. We adopt the concept of disclosure "bloat" to assess the degree of boilerplate or redundant content in the cybersecurity disclosure. Following Kim et al. (2024), we operationalize *Bloat* as the relative difference between the length of the disclosure and that of its summary, summarized by a large language model (gpt-4o-mini). Higher bloat values indicate that the original disclosure contains a greater proportion of uninformative, redundant, or irrelevant content. We apply the model instructions and parameters detailed in Kim et al. (2024).

Specificity. We measure the specificity of the cybersecurity disclosure by quantifying the presence of firm-specific details versus

Table 2
Sample composition ($N = 3{,}440$).

	Frequency	Percent
Panel A: Industry		
(1) NoDur	159	5
(10) Hlth	568	17
(11) Money	624	18
(12) Other	471	14
(2) Durbl	96	3
(3) Manuf	292	8
(4) Enrgy	112	3
(5) Chems	81	2
(6) BusEq	584	17
(7) Telcm	65	2
(8) Utils	92	3
(9) Shops	296	9
Total	3,440	100
Panel B: Market cap		
<10 M	160	5
10 M–100 M	574	17
100 M–1B	1,057	31
1B-10B	1,156	34
>10B	493	14
Total	3,440	100

Note: Panel A: Fama-French 12 industry classification. Panel B: market capitalization in 2023 year-end.

generic text. Following the approach of Hope et al. (2016) for risk-factor disclosures, we use Named Entity Recognition through the SpaCy natural language processing library in Python to count the number of concrete details in the Item 1C text. These include proper names, abbreviations, quantitative values, dates, product or system names, and other specific identifiers of the firm's circumstances. We then scale this count by the total words in the section to obtain a specificity ratio. A higher specificity score means the disclosure is more detailed (e.g., referencing specific units), whereas a low score suggests more general language with few firm-specific details.

These three measures capture disclosure quality from both the firm's and the investor's perspective, aligning with RQ1 and RQ2. *Words* proxies for the firm's disclosure effort under the mandate; for investors, longer disclosures provide more comprehensive coverage that reduces information asymmetry (Campbell et al., 2014). *Bloat* captures the firm's reliance on generic language—firms may produce redundant content to satisfy formal requirements while limiting operationally sensitive detail, consistent with proprietary cost models where managers balance transparency against competitive and litigation risks (Verrecchia, 1983; Hope et al., 2016). From the investor's perspective, it quantifies how much content a reader must filter to extract substance (Kim et al., 2024). Bloat thus reflects both the firm's strategic boilerplate choice and the resulting information density available to investors. *Specificity* reflects the firm's willingness to disclose concrete details such as named systems, governance structures, and quantitative thresholds; lower specificity indicates a deliberate protective choice under proprietary costs (Hope et al., 2016). For investors, these specific references provide decision-useful signals, eliciting stronger market reactions and improving analyst risk assessment (Hope et al., 2016).

3.4. Independent variables

Our independent variables are motivated by prior research on risk disclosure determinants (Kravet & Muslu, 2013, Campbell et al., 2014; Hope et al., 2016; Beatty et al., 2019) and cybersecurity disclosure practices (Berkman et al., 2018; Gao et al., 2020; Jiang et al., 2022), and fall into several categories reflecting firm attributes likely influencing cybersecurity disclosures.

Financial characteristics include firm *size* (log market capitalization), which is among the most consistent predictors of disclosure quantity and quality in prior research (Campbell et al., 2014; Gao et al., 2020); profitability (return on assets, *roa*) and capital structure (leverage, *lvg*), which proxy for resource capacity and creditor monitoring incentives that may affect disclosure effort (Campbell et al., 2014; Jiang et al., 2022); liquidity (cash-to-assets ratio, *cash*), as firms with higher liquid asset holdings are better positioned to invest in compliance and reporting infrastructure (Rosati et al., 2022; Cazier & Pfeiffer, 2016); growth opportunities (market-to-book ratio, *mtb*), as high-growth firms face stronger proprietary costs of disclosure and greater incentives to manage market expectations (Campbell et al., 2014; Hope et al., 2016; Dyer et al., 2017); and audit quality (Big-4 auditor indicator, *big4*), as Big-4 auditors are associated with enhanced cybersecurity risk awareness and procedural rigor (Rosati et al., 2022). We also include institutional ownership *inst_own*, as institutional investors may demand higher-quality disclosures through monitoring and engagement (Beatty et al., 2019; Campbell et al., 2014; Abramova et al., 2020), and analyst coverage (number of analysts, *num_est*), which proxies for the richness of the firm's information environment (Campbell et al., 2014; Beatty et al., 2019).

Annual report characteristics capture the firm's overall disclosure style and linguistic environment, ensuring that Item 1C variation reflects cybersecurity-specific choices rather than firm-wide drafting tendencies. These include 10-K length (total word count), sentiment (proportion of negative and positive words), uncertainty and litigation risk (proportion of uncertain and litigious words), and organizational complexity (Loughran & McDonald, 2024). We also include an indicator for whether the firm received an SEC comment letter on its prior filing, as comment letters prompt firms to change their disclosures (Calderon & Gao, 2022; Wang et al., 2022). We look at comment letters to 10-K and 10-Q two years prior to the Item 1C filings.

Technological attributes encompass indicators for IT-related material weaknesses in internal controls (Lawrence et al., 2018; Berkman et al., 2018); firm digitalization, which captures the firm's strategic digital orientation and, by extension, its cyber attack surface (Kindermann et al., 2021; Sihvonen, 2024); cybersecurity risk exposure derived from earnings call language (Jamilov et al., 2021), which proxies for the salience of cyber risk in the firm's operations (Berkman et al., 2018); technology or risk-focused board committees, which signal governance-level engagement with cybersecurity oversight (Berkman et al., 2018); and technology industry classification based on four-digit SIC codes (Lawrence et al., 2018).

Prior disclosures include *prior_attack*, an indicator variable controlling for the firm's history of cyber incident disclosures, including prior 8-K filings (Gao et al., 2020; Gordon et al., 2024; Li et al., 2018; Jiang et al., 2022), and *prior_cyber*, the proportion of cybersecurity-related words in the Item 1A (Risk Factors) section of the firm's 10-K filed in the year preceding the mandatory Item 1C disclosure (Chen et al., 2023; Jiang et al., 2022). These variables control for cybersecurity information already available to investors before the mandated Item 1C disclosures, allowing us to isolate the incremental disclosure decisions firms make under the new regulatory regime. Peer averages capture industry norms and potential peer influences on cybersecurity disclosure (Cazier et al., 2021). Using the Text-Based Network Industry Classification (TNIC) developed by Hoberg and Phillips (2016), we identify each firm's close peers based on similarities in business descriptions. For each firm, we calculate the TNIC similarity-weighted average of peers' Item 1C disclosure characteristics. By incorporating peer behavior, we mitigate omitted variable concerns, particularly those arising from factors beyond the FF-12 industry level (e.g., common shocks or regulatory scrutiny) that could similarly influence firms' disclosures. Detailed variable definitions and data sources are provided in the Appendix.

3.5. Summary statistics

Table 3 reports the summary statistics for our sample. The Item 1C disclosures in our sample contain an average (median) of 739 (710) words, with substantial variation in length. The middle 50% of disclosures range from 516 to 925 words, corresponding roughly

from one-half to three pages of text. The bloat ratio – measuring the proportion of generic or boilerplate language – averages 0.59 (IQR = 0.52–0.68), indicating moderate information density but significantly lower than 0.79 of MD&A sections reported in Kim et al. (2024). Specificity, evaluating precise and concrete disclosure content, averages at a relatively low level of 0.05, in line with Hope et al. (2016).

Fig. 1 illustrates systematic variations in cybersecurity disclosures across industries (Panel A) and firm sizes (Panel B). Analysis using Fama-French 12 industry classifications shows that money and finance sectors, along with utilities, provide the most extensive disclosures (approximately 850 words), reflecting heightened cybersecurity threats and regulatory scrutiny in these industries. These sectors also demonstrate highest specificity ratios. In contrast, consumer durables and chemicals sectors produce shorter, more generalized disclosures. Notably, the healthcare sector occupies a low-to-intermediate position despite its handling of sensitive patient data, exhibiting moderate disclosure length and quality metrics. The explanatory power of industry classifications, measured by fixed-effects R^2 values, is relatively modest (ranging from 0.013 to 0.062), with specificity ratio showing the strongest industry-based variation.

In Panel B of Fig. 1, firm size analysis illustrates a clearer gradient. Larger firms (>$10B in market capitalization) produce substantially longer (approximately 900 words) and more specific cybersecurity disclosures than smaller firms (<$10 M in market capitalization, approximately 500 words). However, larger organizations also show higher rates of language redundancy, as indicated by their elevated bloat ratios. The explanatory power of firm size, measured by fixed-effects R^2 values (ranging from 0.076 to 0.130), significantly exceeds that of industry classification. Overall, these findings indicate that firm size systematically influences disclosure characteristics more than its industry, although a significant portion of disclosure variation remains unexplained by these factors.

4. Results of disclosure determinants

Table 4 presents regression results examining the determinants of Item 1C cybersecurity disclosure characteristics, measured across three dimensions: disclosure length (*Words*), redundant language (*Bloat*), and firm-specific detail (*Specificity*). The *Words* model is estimated using Poisson regression on raw word counts, which is appropriate for count data; the *Bloat* and *Specificity* models use OLS. Models incorporating industry and size fixed effects explain 16–18% of the variation in disclosures ($p < 0.01$), indicating statistically significant yet moderate explanatory power. The modest R-squared values align with prior studies (Campbell et al., 2014; Hope et al., 2016), suggesting firm characteristics provide partial but incomplete explanations of disclosure behaviors in emerging regulatory contexts. This finding is consistent with Cazier and Pfeiffer (2016), who demonstrate that managerial discretion accounts for significant variation in regulated disclosure practices beyond what firm characteristics alone explain. Columns 1–3 report the level regressions discussed in this section; Columns 4 and 5 report the change analysis regressions discussed in Section 4.1.

Financial performance metrics consistently predict disclosure quality. Firm size, measured as log market capitalization, positively predicts all three disclosure dimensions (0.032, $p < 0.01$ for *Words*; 0.009, $p < 0.01$ for *Bloat*; 0.129, $p < 0.01$ for *Specificity*). This finding is consistent with the well-documented positive association between firm size and disclosure extensiveness (Campbell et al., 2014; Gao et al., 2020). Return on assets (*roa*) and leverage (*lvg*) positively correlate with all disclosure dimensions (mostly $p < 0.01$), exhibiting notable coefficients particularly for *Specificity* (0.240 and 0.269, respectively). Institutional ownership is positively associated with disclosure length and bloat (0.089 and 0.025, respectively; both $p < 0.01$), consistent with institutional investors demanding more extensive disclosures through monitoring and engagement (Abramova et al., 2020). The association does not extend to *Specificity*, suggesting that institutional pressure influences disclosure volume rather than content precision. Auditor quality, operationalized through Big Four audit engagements, is positively associated with *Bloat* and *Specificity* ($p < 0.10$), though the association is weaker than for other financial determinants. This finding aligns with Rosati et al. (2022), who document increased auditor risk awareness and procedural enhancements related to cybersecurity incidents. Analyst coverage and SEC letters show no significant association with disclosure characteristics after controlling for firm size and institutional ownership.

Previous year's 10-K disclosure (*length*) positively predicts current disclosure length (0.135; $p < 0.01$), but simultaneously increases boilerplate language usage (coefficient of 0.041, $p < 0.01$). This reflects literature highlighting the "stickiness" of corporate disclosure practices (Cazier & Pfeiffer, 2016; Dyer et al., 2017). Litigation risk exposure (*litigation*) exhibits a statistically significant negative relationship with all three disclosure dimensions (Words: −0.039; Bloat: −0.013; Specificity: −0.180, all $p < 0.05$). Firms facing greater litigation risks appear to strategically limit disclosure details to reduce legal vulnerabilities. This pattern is consistent across all dimensions: firms exposed to litigation risk produce shorter, less redundant, and less specific disclosures, consistent with content reduction as a defensive strategy rather than selective editing of particular content types. In cybersecurity contexts, this behavior reflects the unique tension between transparency and vulnerability: detailed disclosure can expose security architectures to adversaries and trigger litigation (Amir et al., 2018; Ettredge et al., 2018), a concern the SEC itself acknowledged by permitting firms to withhold technical details that could impede their cybersecurity response (SEC, 2023, Instruction 4). Our finding partially contradicts the voluntary-regime finding of Gao et al. (2020), who documented an increase in litigious language following regulatory guidance. Instead, our mandatory-regime results suggest firms employ content reduction as a deliberate defensive legal strategy.

Firm *complexity* significantly predicts more specific disclosures (0.729; $p < 0.01$), reflecting the need for detailed risk communication among complex organizations, though it does not significantly predict disclosure length or bloat. Cybersecurity risk score (*cyber_score*; Jamilov et al., 2021) positively correlates with disclosure length and *Bloat* (0.074 and 0.020, respectively; both $p < 0.01$), indicating that firms exposed to cyber threats tend toward more extensive but also more redundant disclosures. Additionally, the existence of a dedicated risk committee (*risk_comm*) positively influences disclosure length and *Specificity* (0.055, $p < 0.05$; and 0.337, $p < 0.01$), suggesting risk oversight enhances both the volume and precision of cybersecurity disclosures. Technology firms produce longer disclosures (0.106; $p < 0.05$), though not more specific ones.

Table 3
Descriptive statistics (N = 3,440).

Variable	Mean	SD	P1	P25	P50	P75	P99
Item 1C (time t)							
Words	739	329	68	516	710	925	1697
Bloat	0.59	0.12	0.29	0.52	0.60	0.68	0.82
Specificity	0.05	0.02	0.01	0.03	0.05	0.06	0.10
Financials (t–1)							
size	20.46	2.43	14.51	18.83	20.60	22.15	25.82
roa	−0.10	0.35	−2.00	−0.11	0.01	0.06	0.32
lvg	0.82	0.39	0.08	0.55	0.84	1.02	2.25
cash	0.15	0.17	0.00	0.03	0.08	0.19	0.81
mtb	1.87	18.29	−94.30	−0.23	1.47	3.87	91.18
big4	0.54	0.50	0	0	1	1	1
inst_own	0.64	0.33	0.00	0.37	0.73	0.91	1.00
num_est	7.85	8.23	0	2	5	11	35
10-K Stats (t–1)							
length	10.94	0.49	9.74	10.62	10.90	11.21	12.23
senti_nega	2.05	0.39	1.13	1.77	2.04	2.30	3.07
senti_posi	0.60	0.17	0.29	0.47	0.58	0.70	1.13
uncertainty	1.58	0.34	0.80	1.36	1.59	1.83	2.32
litigation	1.49	0.60	0.60	1.05	1.36	1.78	3.32
complexity	0.41	0.14	0.16	0.30	0.38	0.48	0.84
sec_letter	0.04	0.19	0.00	0.00	0.00	0.00	1.00
Technology (t–1)							
itmw	0.06	0.24	0	0	0	0	1
digi_score	4.00	0.64	2.71	3.50	3.94	4.52	5.30
cyber_score	3.39	0.52	2.00	3.08	3.43	3.75	4.46
tech_comm	0.07	0.25	0	0	0	0	1
risk_comm	0.13	0.34	0	0	0	0	1
tech_firm	0.15	0.36	0	0	0	0	1
Prior disclosure (t–1)							
prior_attack	0.16	0.36	0	0	0	0	1
prior_cyber	3.51	1.02	0	3.34	3.77	4.08	4.69

Note: Variables measured at time *t* (2024 fiscal year) or *t–1* (2023). Variable definitions are in the Appendix.

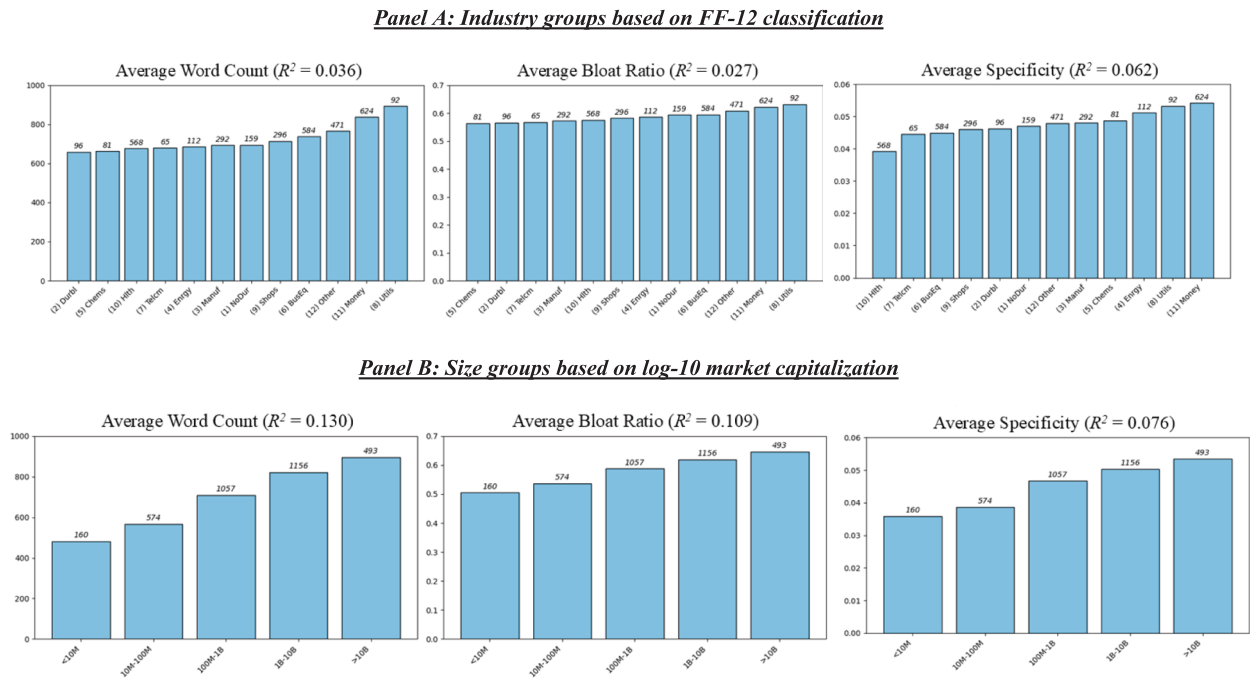


Fig. 1. Item 1C characteristics across industry and size groups. Subplot titles report the adjusted R^2 of the group fixed effects.

Table 4
The determinants of cybersecurity disclosure characteristics and disclosure change.

	Item 1C Disclosure Characteristics			Cyber Disclosure Change	
	(1)	(2)	(3)	(4)	(5)
	Words	Bloat	Specificity	ΔTopics	ΔVolume
size	0.032***	0.009***	0.129***	0.060***	0.015*
	(3.07)	(3.23)	(2.77)	(3.19)	(1.75)
roa	0.083***	0.026***	0.240**	0.010	0.059**
	(2.91)	(3.54)	(2.10)	(0.16)	(2.47)
lvg	0.077***	0.017***	0.269***	−0.103**	−0.015
	(3.52)	(2.93)	(3.05)	(−2.38)	(−0.86)
cash	−0.046	−0.002	−0.191	−0.142	−0.042
	(−0.90)	(−0.15)	(−0.93)	(−1.47)	(−0.98)
mtb	−0.000	−0.000	0.000	−0.001	0.000
	(−1.14)	(−0.00)	(0.13)	(−1.34)	(0.28)
big4	0.028	0.010*	0.165*	0.006	0.002
	(1.34)	(1.81)	(1.83)	(0.15)	(0.14)
inst_own	0.089***	0.025***	0.231	0.337***	0.129***
	(2.77)	(2.73)	(1.57)	(5.18)	(4.80)
num_est	0.000	0.003	−0.067	−0.032	−0.013
	(0.03)	(0.75)	(−1.11)	(−1.17)	(−1.19)
sec_letter	−0.058	−0.007	−0.003	−0.071	−0.028
	(−1.56)	(−0.79)	(−0.02)	(−0.79)	(−0.97)
length	0.135***	0.041***	−0.050	−0.330***	−0.203***
	(6.14)	(7.21)	(−0.53)	(−7.58)	(−10.85)
senti_nega	0.045*	0.007	0.155	−0.134***	−0.085***
	(1.70)	(0.94)	(1.29)	(−2.64)	(−3.79)
senti_posi	0.047	0.011	0.017	0.008	−0.056
	(0.87)	(0.72)	(0.07)	(0.08)	(−1.25)
uncertainty	0.002	0.008	−0.556***	−0.234***	−0.119***
	(0.06)	(0.82)	(−3.59)	(−3.16)	(−3.86)
litigation	−0.039**	−0.013**	−0.180**	0.043	0.032**
	(−2.06)	(−2.48)	(−2.25)	(1.18)	(2.13)
complexity	0.082	0.017	0.729***	0.098	0.025
	(1.59)	(1.12)	(3.03)	(0.98)	(0.54)
digi_score	0.019	0.009**	−0.056	−0.224***	−0.098***
	(1.14)	(2.08)	(−0.77)	(−7.03)	(−6.49)
cyber_score	0.074***	0.020***	0.046	−0.193***	−0.232***
	(3.97)	(4.08)	(0.54)	(−5.22)	(−12.07)
tech_firm	0.106**	0.009	−0.218	−0.007	0.042
	(2.52)	(0.76)	(−1.23)	(−0.08)	(1.33)
itmw	0.000	0.003	−0.121	0.036	−0.017
	(0.01)	(0.41)	(−0.98)	(0.63)	(−0.71)
tech_comm	−0.003	0.006	0.144	0.053	0.021
	(−0.11)	(0.90)	(1.14)	(1.13)	(0.99)
risk_comm	0.055**	0.009	0.337***	−0.044	−0.002
	(2.55)	(1.46)	(3.19)	(−1.10)	(−0.13)
prior_cyber	−0.001	0.001	0.046	−0.057***	−0.022
	(−0.13)	(0.35)	(1.13)	(−2.61)	(−1.62)
prior_attack	0.014	0.001	0.074	−0.014	−0.024
	(0.72)	(0.15)	(0.86)	(−0.41)	(−1.54)
peer_avg	0.165***	0.062	0.164***	0.700***	0.427***
	(4.70)	(1.46)	(4.02)	(4.42)	(4.98)
Industry FE	Yes	Yes	Yes	Yes	Yes
Size FE	Yes	Yes	Yes	Yes	Yes
Adj. (Pseudo) R^2	0.158	0.185	0.159	0.210	0.371

Note: t-statistics based on robust S.E. in parentheses. * $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$. Columns (1)–(3) examine determinants of Item 1C disclosure characteristics: *Words* is estimated via Poisson regression on raw word counts; *Bloat* (redundancy ratio) and *Specificity* (named entity ratio) are estimated via OLS. Columns (4)–(5) examine the magnitude of disclosure change from 2023 to 2024: *ΔTopics* is the log Kullback–Leibler divergence between the firm's 2023 Item 1A and 2024 combined Item 1A + 1C topic distributions; *ΔVolume* is the log ratio of cybersecurity sentences in 2024 to 2023. All independent variables are lagged one year except *peer_avg*. Industry fixed effects use the Fama-French 12 classification; size fixed effects are based on rounded log-10 market capitalization. Variable definitions are in the Appendix. $N = 3{,}440$.

Our findings indicate that a firm's disclosure practices are significantly associated with those of its industry peers. Peer average disclosure (*peer_avg*) positively correlates with disclosure length and specificity (0.165, $p < 0.01$; and 0.164, $p < 0.01$), indicating substantial mimetic behavior within industries. This finding is consistent with prior research demonstrating firms' tendency to align disclosures with industry peers (Cazier et al., 2021).

In Table 4, Bloat and Specificity tend to move in the same direction across firm characteristics: variables associated with more redundancy are also associated with more specificity. Although these constructs may appear conceptually opposed, they capture

distinct dimensions of disclosure quality. Bloat measures the proportion of content that is redundant relative to a compressed summary, while Specificity measures the density of named entities such as organizational roles, system names, and quantitative thresholds. Firms with greater disclosure investment (larger firms, those with Big Four auditors, risk committees, and higher cyber risk exposure) produce text that contains both more concrete detail and more surrounding filler material. The co-movement reflects disclosure effort: comprehensive disclosures embed specific governance details within a broader narrative that includes contextual and procedural language. This pattern is stable across subsample splits by prior incidents, industry, and digitalization (Online Appendix Tables OA.1–OA.3).

In contrast to e.g. Gao et al. (2020), recent cybersecurity breaches, technology sector affiliation, IT-related internal control weaknesses, and firm digitalization levels do not significantly influence cybersecurity disclosure attributes. Under voluntary disclosure regimes, breaches are among the strongest predictors of cybersecurity disclosure changes (Chen et al., 2023; Jiang et al., 2022; Gao et al., 2020). The absence of this effect under the Item 1C mandate suggests that mandatory disclosure establishes a compliance floor that neutralizes the incremental disclosure incentives created by breach experience. Our findings also differ from Lawrence et al. (2018), who identify a relationship between IT control weaknesses and increased cybersecurity disclosures. The insignificance of digitalization contrasts with Sihvonen (2024), and could reflect either strategic underreporting or prior incorporation of cybersecurity content into existing disclosures; we disentangle these explanations in Section 4.1.

The null findings for prior cybersecurity disclosure intensity (*prior_cyber*) and prior attacks (*prior_attack*) are particularly noteworthy, as they contrast with the voluntary disclosure literature where these variables are among the most consistent predictors of cybersecurity disclosure behavior (Chen et al., 2023; Jiang et al., 2022; Gao et al., 2020). Two explanations account for this divergence. First, a structural explanation: as the change analysis in Section 4.1 demonstrates, Item 1C addresses governance and process topics that are largely absent from prior Item 1A disclosures.

This structural disconnect between the content of prior voluntary disclosures and the governance focus of §106 limits the predictive power of pre-existing voluntary cybersecurity content. Second, a compliance floor explanation: under voluntary regimes, breach experience creates differential disclosure incentives because affected firms face pressure to signal remediation (Chen et al., 2023; Jiang et al., 2022). The Item 1C mandate requires all firms, regardless of incident history, to disclose governance processes and risk management frameworks, establishing a uniform baseline that neutralizes the incremental incentive that breach experience previously provided. The null effect in the level regressions (Columns 1–3) thus reflects the structural disconnect between Item 1A risk language and Item 1C governance content, rather than an absence of any prior-disclosure effect on the transition to the new regime.

4.1. Change analysis

The preceding analysis establishes cross-sectional variation in Item 1C disclosure characteristics. A related question is whether the mandate induced substantively new information, or whether firms simply relocated existing cybersecurity content from other sections of the 10-K. To address this, we conduct two analyses: a topic-level comparison of disclosure content before and after the mandate, and cross-sectional regressions examining which firm characteristics predict the magnitude of disclosure change.

Following Lowry et al. (2020), we compare the topic composition of cybersecurity-related sentences in Item 1A (Risk Factors) across 2022–2024 with the new Item 1C disclosures in 2024. We train a supervised classifier (TF-IDF with logistic regression) on Item 1C sentences, using each filing's subsection headings as natural topic labels across eight cybersecurity disclosure topics aligned with Regulation S-K §106, supplemented with non-cyber sentences sampled from Item 1A filings with low cybersecurity keyword intensity as a negative class. When applied to Item 1A, the classifier assigns each sentence a probability vector over topics; sentences classified as non-cyber are excluded, yielding a firm-level cybersecurity topic distribution for each year. To measure the difference between topic distributions, we use Kullback–Leibler (KL) divergence, a standard information-theoretic measure of how one topic distribution differs from another. We compute KL divergence sequentially—each year's distribution against the preceding year's—so that the year-over-year stability of Item 1A serves as an internal benchmark against which the Item 1A-to-Item 1C content shift can be evaluated.

Table 5 reports the topic distributions. First, cybersecurity disclosures within Item 1A remained stable from 2022 to 2024 (KL divergence ≈ 0.01), with Material Risk consistently accounting for 76% of cybersecurity-related sentences.[4] Second, Item 1C represents fundamentally different content. The KL divergence between Item 1A and Item 1C in 2024 is 5.92, orders of magnitude larger than the year-over-year Item 1A variation, indicating fundamentally distinct topic distributions. Item 1C shifts emphasis toward Risk Processes (43%), Board Oversight (20%), and Management Role (13%), directly reflecting the governance and process requirements of §106 that have no counterpart in Item 1A. Third, firms added rather than relocated content: the median firm maintained its Item 1A cybersecurity disclosure volume (26 sentences in 2024 vs. 25 in 2023) while producing 29 additional sentences in Item 1C, more than doubling total cybersecurity disclosure.

Columns 4 and 5 of Table 4 examine which firm characteristics predict the magnitude of disclosure change. The dependent variables capture two distinct dimensions: Δ*Topics* (column 4) is the log of KL divergence between the firm's 2023 Item 1A topic distribution and its 2024 Item 1A and 1C combined distribution, where higher values indicate greater content transformation; Δ*Volume* (column 5) is the log ratio of cybersecurity sentences in 2024 to 2023, where positive values indicate increased volume. These models explain 21% and 37% of variation, respectively, consistent with the mandate creating a measurable structural shift.

The results show that firms with more pre-existing cybersecurity content made smaller adjustments. Cybersecurity risk score, 10-K

[4] This category comprises mostly generic language describing potential threats, e.g., "*Security breaches can create system disruptions and shutdowns that could result in disruptions to our operations.*".

Table 5
Topic distribution by disclosure section.

SEC §106 Topic	Item1A(2022)	Item1A(2023)	Item1A(2024)	Item1C(2024)
Material Risk	75.8%	75.7%	76.1%	13.3%
Risk Processes	16.4%	16.3%	16.2%	42.6%
Integration	0.1%	0.1%	0.1%	1.4%
Board Oversight	1.1%	1.1%	1.0%	20.4%
Management Role	1.1%	1.0%	0.9%	12.9%
3rd Party Engagement	0.2%	0.2%	0.2%	2.1%
3rd Party Oversight	5.2%	5.3%	5.3%	5.0%
Escalation	0.2%	0.3%	0.3%	2.2%
Cyber sentences	22	25	26	29
KL divergence	—	0.01	0.01	5.92

Notes: Topic percentages based on sentence-level classification using a supervised classifier (TF-IDF with logistic regression) trained on Item 1C subsections across an 8-topic taxonomy aligned with SEC §106 categories. *Cyber sentences* is the median number of cybersecurity-related sentences per firm. KL divergence is the firm-level median Kullback–Leibler divergence between preceding and current column's topic distributions. Sample: Item 1A (2022–2024) and Item 1C (2024) sections for the 3,440 sample firms.

length, and prior Item 1A cybersecurity intensity all negatively predict disclosure change, consistent with these firms having already addressed cybersecurity topics in their prior filings. Firm digitalization also negatively predicts both outcomes; combined with its null effect in the level regressions (columns 1–3), this suggests that more digitalized firms had already incorporated cybersecurity into their reporting rather than strategically underreporting. Institutional ownership strongly predicts greater change in both dimensions ($p < 0.01$), consistent with institutional pressure encouraging more substantive responses to the mandate. Peer disclosure change is also significant in both models, indicating isomorphic adjustment within industry-size groups. Prior cyber attacks, board committees, and technology firm status show no significant association with disclosure change, paralleling their null effects in the level regressions.

Together, the topic analysis and change regressions support three conclusions. First, Item 1C represents genuinely new disclosure content focused on governance processes, not a relocation of existing risk factor language. Second, the mandate had its largest impact on firms with limited prior cybersecurity disclosure. Third, the null effects of prior disclosure intensity in the level regressions reflect a structural explanation: Item 1C addresses governance and process topics largely absent from Item 1A, limiting the predictive power of pre-existing voluntary cybersecurity content.

4.2. Robustness analysis

We assess the sensitivity of our findings through several robustness tests, summarized here; detailed results are available upon request.

Alternative industry classifications. Our main specification uses the Fama-French 12-industry classification. To assess whether finer industry groupings alter the conclusion that firm size explains more disclosure variation than industry, we compare the explanatory power of five classification schemes (FF-12, FF-17, FF-30, FF-48, and two-digit SIC) against size quintiles. For disclosure length and bloat, five size quintiles alone explain approximately 10% of variance, whereas all industry schemes explain only 2–3%. For specificity, the gap narrows: both FF-48 and SIC-2 match size quintiles (adjusted $R^2 = 0.075$). Replacing FF-12 with SIC-2 in the full specification changes adjusted R^2 insignificantly. We conclude that the finding that firm size drives disclosure characteristics more than industry is robust to alternative industry classifications.

Excluding HIPAA/GLBA-regulated industries. Healthcare and financial services firms face sector-specific cybersecurity regulations (HIPAA and the Gramm-Leach-Bliley Act) that may independently shape their disclosure practices. We split the sample into non-regulated ($N = 2{,}248$) and regulated firms ($N = 1{,}192$) and run the full specification separately on each subsample. Joint equality tests show no structural differences for disclosure length ($\chi^2(24) = 26.5$, $p = 0.329$) or bloat ($\chi^2(24) = 25.1$, $p = 0.403$). For specificity, the joint test rejects equality ($\chi^2(24) = 55.0$, $p < 0.001$), with differences concentrated in 10-K sentiment variables. The main determinants of disclosure characteristics are not driven by sector-specific cybersecurity regulations.

To examine whether the determinants of disclosure characteristics differ across firm types, we conduct subsample analyses partitioned by prior cyber incidents, high cyber-risk industry classification (Technology, Telecom, Healthcare, and Finance), and firm digitalization (Online Appendix Tables OA.1–OA.3). Joint equality tests fail to reject the null of equal coefficients in eight of nine comparisons (all $p > 0.10$), indicating that the determinant structure is stable across firm types. The one exception is disclosure specificity in the industry split ($\chi^2(23) = 44.33$, $p = 0.005$), consistent with the regulated-industry finding reported above. At the coefficient level, prior cyber incidents remain insignificant across all subsamples, reinforcing the compliance-floor interpretation. Cybersecurity risk exposure and risk committee presence load significantly only in high cyber-risk industries and high-digitalization firms, suggesting these variables operate where cybersecurity is operationally salient rather than uniformly across the sample.

5. Market event study

To investigate market implications of these disclosures, we conduct an event study analyzing market reactions to 10-K filings containing the newly mandated Item 1C cybersecurity disclosures. Prior research on mandatory risk factor disclosures (Item 1A)

suggests that markets react to new risk information in annual filings, with more specific disclosures generating stronger investor responses (Hope et al., 2016; Kravet & Muslu, 2013). While material cybersecurity incidents are typically disclosed through Form 8-K filings (Gordon et al., 2024), the comprehensive Item 1C disclosures in 10-K reports serve a distinct informational role. These annual disclosures provide detailed descriptions of cybersecurity risk management processes, governance structures, and strategic approaches that may not be fully captured in event-driven incident reports.

Specifically, we examine whether specific characteristics of the Item 1C cybersecurity disclosure are associated with stronger or weaker market responses. The event date is the 10-K filing (day 0), and the analysis concentrates on a three-day event window (days –1, 0, and + 1). This narrow window captures immediate market reactions while accommodating minor information leakage or delayed investor responses around the filing (Campbell et al., 2014; Hope et al., 2016; Kravet & Muslu., 2013).

We begin with the sample of eligible firm-year observations used in Section 4 ($N = 3{,}440$). To ensure data integrity for an event study, we apply several filtering criteria: stock prices must exceed $1.00 at filing to exclude penny stocks and prevent extreme percentage return distortions; and we eliminate observations where the measurement window (three days surrounding the filing) overlaps with annual earnings announcements. This controlled isolation of the event window ensures that measured market reactions can be reliably attributed to the filings content rather than earnings surprise. The final sample (N = 1,204) is used to examine whether markets respond to firms' cybersecurity-related disclosures through statistically significant abnormal returns or trading volume.

Following prior research, we measure the magnitude of stock price movements regardless of direction by calculating the absolute cumulative abnormal return (|CAR|) for each three-day window centered on the 10-K filing date. We employ a market-adjusted model, defining abnormal stock returns as the difference between the firm's total return and the CRSP value-weighted market return. This approach is standard for short event windows and widely used in disclosure studies examining similar research questions (Campbell et al., 2014; Hope et al., 2016). As a complementary measure of investor reaction, we examine abnormal trading volume (AVOL), which captures unusual trading activity associated with the filing event. We calculate AVOL as the percentage increase in average daily volume during the three-day event window (days –1 to + 1) compared to the firm's average daily volume over the 60 trading days ending 10 days before the filing date. This benchmark period avoids contamination from earnings announcement-driven trading that might inflate the volume baseline.

To address the broader information environment surrounding cybersecurity disclosures, we incorporate control variables that account for prior information dissemination and factors that might influence market reaction magnitude. We estimate the following model:

$$\text{MktReaction} = \alpha + \beta(\text{DisclosureMetric}) + \gamma(\text{Controls}) + \text{IndustryFE} + \epsilon \quad (2)$$

where *MktReaction* is either |CAR| or AVOL and *DisclosureMetric* refers to our previously defined disclosure measures. Firm and time

Table 6
Market reaction to 10-K cybersecurity disclosures.

	(1) Full	(2) Att = Yes	(3) Att=No	(4) HiCyb = Y	(5) HiCyb=N	(6) 8 K = Yes	(7) 8 K=No
Panel A: |CAR|							
Words	–0.007	–0.002	–0.009	–0.013	–0.001	0.018	–0.006
	(–1.20)	(–0.47)	(–1.21)	(–1.52)	(–0.28)	(1.00)	(–1.13)
Specificity	–0.021	0.092	–0.060	0.033	–0.131	0.350	–0.019
	(–0.28)	(0.66)	(–0.70)	(0.35)	(–1.15)	(0.80)	(–0.26)
Bloat	0.002	–0.024	0.009	0.037	–0.031	–0.040	0.001
	(0.11)	(–1.01)	(0.40)	(1.31)	(–1.51)	(–0.50)	(0.07)
N	1,204	266	938	720	484	32	1,172
Adj. R^2	0.023	0.011	0.045	0.052	0.054	–0.053	0.028
Panel B: AVOL							
Words	–0.008	0.034	–0.027	–0.025	0.004	–0.004	–0.002
	(–0.18)	(0.43)	(–0.50)	(–0.37)	(0.07)	(–0.02)	(–0.04)
Specificity	0.284	0.809	0.403	1.150	–1.018	3.140	0.435
	(0.36)	(0.51)	(0.44)	(1.12)	(–0.85)	(0.45)	(0.55)
Bloat	–0.069	0.173	–0.103	–0.039	–0.053	–0.259	–0.090
	(–0.37)	(0.51)	(–0.47)	(–0.14)	(–0.24)	(–0.18)	(–0.47)
N	1,204	266	938	720	484	32	1,172
Adj. R^2	0.118	0.114	0.129	0.148	0.053	0.162	0.128
Controls	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Industry FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Note: t-statistics based on robust S.E. in parentheses. * $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$. Panel A: |CAR| is the absolute cumulative abnormal return over a three-day window centered on the 10-K filing date, using a market-adjusted model. Panel B: AVOL is abnormal trading volume, measured as the ratio of average daily volume during the event window to average daily volume over the baseline period (days –70 to –10). Each panel reports OLS regressions of the market reaction measure on three Item 1C disclosure characteristics (*Words*, *Bloat*, *Specificity*). Column (1) reports the full-sample model. Columns (2)–(3) split by prior cyber incident history from breach databases. Columns (4)–(5) split by high vs. low cyber-risk industry (Technology, Telecom, Healthcare, Finance per FF-12). Columns (6)–(7) split by whether the firm filed a cybersecurity-related 8-K (Item 1.05) in the 12 months preceding the 10-K filing date. Controls: log market capitalization, ROA, log market-to-book, leverage, log stock price, 60-day momentum, absolute earnings announcement CAR, prior 8-K indicator, prior Item 1A cybersecurity intensity, and FF-12 industry fixed effects. Controls that define the sample split are excluded from the corresponding subsample regressions.

subscripts are omitted for brevity. Our control variables include: *mcap*, the logarithm of the firm's market capitalization; *roa*, operating income to total assets; *mtb*, the logarithm of the market-to-book; *lvg*, total long term debt divided by total assets; *prc*, the log of the stock's price per share; *mom*, the stock's 60-day performance leading up to earnings announcement. All control variables are measured at fiscal year end. We also include *ear*, the absolute three-day CAR to the firm's most recent earnings announcement prior to the 10-K filing, to control for earnings-driven stock volatility. Importantly, we include *prior_8k*, an indicator for cybersecurity incident 8-K disclosures during the 365 days prior to the 10-K filing (Gordon et al., 2024), and *prior_cyber*, the proportion of cybersecurity-related words in the prior year's Item 1A Risk Factors section (Chen et al., 2023). These variables help control for information already available to the market through other disclosure channels. We estimate this model using OLS with heteroskedasticity-robust standard errors and include Fama-French 12 industry fixed effects in all specifications.

Table 6 reports the results of the event study analysis. The primary finding is that disclosure characteristics of the newly mandated Item 1C cybersecurity risk factors in 10-K filings do not elicit measurable market price or volume reactions. Disclosure length, bloat, and specificity measures all show economically small and statistically insignificant relationships with both |CAR| and AVOL (Column 1). Following Campbell et al. (2014), we also examine "unexpected disclosure" measures, defined as the difference between actual disclosure attributes and their predicted values based on Equation (1). These residuals capture the component of disclosure characteristics unexplained by firm-specific and industry factors, representing deviations from expected disclosure patterns. However, these alternative specifications yield no significant associations with |CAR| or AVOL. In untabulated analyses, we also adjust the actual disclosure attributes with peer averages, but all coefficients for peer-adjusted and abnormal disclosure measures remain statistically insignificant. Thus, regardless of how cybersecurity disclosure attributes are measured, we find no evidence of a systematic market reaction to the new Item 1C disclosures.

Prior literature suggests that investors respond more strongly to cybersecurity disclosures from firms with recent incident experience (Gordon et al., 2024; Chen et al., 2023). To test whether the null finding is driven by pooling heterogeneous subgroups, we conduct three cross-sectional splits: by whether the firm had a prior publicly known cybersecurity incident from breach databases (Columns 2–3), by high cyber-risk industry classification (Technology, Telecom, Healthcare, and Finance per FF-12; Columns 4–5), and by whether the firm filed a cybersecurity-related 8-K (Item 1.05) in the 12 months preceding the 10-K filing date (Columns 6–7). In all three splits, disclosure characteristics remain statistically insignificant for both |CAR| and AVOL, and joint equality tests fail to reject the null that coefficients are equal across subsamples (all $p > 0.10$). In untabulated analyses, we obtain consistent results when replacing the industry-based split with firm-level median split based on cybersecurity risk exposure (Jamilov et al., 2021) and when measuring prior incident experience using Reuters cybersecurity incident news coverage in the preceding 12 months. The null market reaction is not attributable to the aggregation of firms with different cybersecurity risk profiles or incident histories.

The absence of systematic market reactions to Item 1C disclosures is consistent with prior findings of muted investor responses to routine cybersecurity disclosures (Richardson et al., 2019; Benaroch, 2021) and can be attributed to several factors. First, investors may perceive these annual disclosures as primarily compliance-focused, containing substantial boilerplate language rather than substantive new information (Beatty et al., 2019; Kim et al., 2024). Second, markets may not yet have developed frameworks for interpreting cybersecurity governance disclosures in ways that affect firm valuation (Campbell et al., 2014). Third, investor attention to cybersecurity may concentrate on the concurrent 8-K incident reporting requirement, which conveys material events with immediate pricing implications (Gordon et al., 2024), potentially reducing the salience of routine annual disclosures. These considerations motivate our subsequent analyses of analyst and investor attention through alternative channels.

Table 7
Investor attention to cybersecurity disclosures.

	(1) *Earnings Call Discussions*	(2) *SEC Edgar Downloads*
Cyber × *Post*	0.343	0.226
	(1.13)	(1.19)
Firm FE	Yes	Yes
Quarter FE	Yes	Yes
Adj. (pseudo) R^2	0.059	0.724
Observations	2,070	1,520

Notes: t-statistics in parentheses. * $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$. Column (1): *Discussions* is the BM25 score measuring prominence of cybersecurity discussion in earnings call Q&A sections (zero for firm-quarters without cybersecurity discussions). *Cyber* = 1 for US firms, subject to the cybersecurity disclosure mandate; control group is non-US firms. *Post* = 1 for Q1–Q3 2024 (S-K 106 in effect); *Post* = 0 for Q1–Q3 2023. Sample is a balanced panel of 345 firms discussing cybersecurity within either period. Standard errors clustered by firm. Column (2): *Downloads* is the number of SEC EDGAR human-readable file views over a 5-day trading window following the filing date. Sample is 760 Form 10-K/A amendments filed in 2024 for fiscal years ending in December 2023, each observed twice; downloads of the original 10-K and downloads of the subsequent amendment. *Cyber* = 1 if the amendment adds Item 1C omitted from the original filing; control group is other amendments. *Post* = 1 for the amendment filing; *Post* = 0 for the original 10-K filing.

5.1. Analyst attention to cybersecurity disclosures in earnings calls

To assess whether the mandate increased market participants' attention to cybersecurity, we examine cybersecurity discussions in earnings call Q&A sections. Earnings calls provide a direct measure of which topics analysts prioritize (Matsumoto et al., 2011), and prior work uses call transcripts to capture firm-level variation in cybersecurity risk salience (Jamilov et al., 2021).

We construct a balanced panel of 345 firms that discussed cybersecurity in at least one earnings call during Q1–Q3 of 2023 or 2024, yielding 2,070 firm-quarter observations. For each call, we measure cybersecurity discussion prominence using BM25 relevance scores. BM25 is an information retrieval scoring function that weights term frequency while controlling for document length, so that longer earnings calls do not mechanically score higher. Firm-quarters without cybersecurity mentions receive a score of zero. We estimate the following difference-in-differences specification:

$$Discussions_{i,t} = \alpha_i + \gamma_t + \beta \cdot Cyber_i \times Post_t + \varepsilon_{i,t} \quad (3)$$

where α_i and γ_t are firm and year-quarter fixed effects, $Cyber_i$ equals one for U.S. firms that are subject to S-K 106, and $Post_t$ equals one for Q1–Q3 2024. The control group is non-U.S. firms not subject to the mandate, and pre-mandate period Q1–Q3 2023.

Table 7 Column (1) reports the results. The interaction coefficient is positive but not statistically significant ($\beta = 0.343$, $t = 1.13$), indicating no measurable increase in analyst attention to cybersecurity following the mandate. These findings complement the event study results and suggest that analysts were already familiar with the cybersecurity practices of their covered firms or did not perceive the standardized Item 1C disclosures as providing material new information. The null result is broadly consistent with Richardson et al. (2019), who find limited analyst response to cybersecurity breach disclosures, and may reflect the monitoring dynamics documented by Amir et al. (2018), where firms with active analyst following have already conveyed their cybersecurity posture through existing channels.

5.2. Measuring investor attention to standalone cybersecurity disclosures

The event study examines market reactions to 10-K filings where Item 1C appears alongside earnings announcements and other material information. The absence of significant market response could result from information overflow rather than a lack of investor interest. To isolate attention to cybersecurity content specifically, we analyze SEC EDGAR download patterns for Form 10-K/A amendments, which correct or supplement the original 10-K without concurrent financial disclosures. Following prior research that uses SEC EDGAR server log data to measure investor attention to specific disclosure types (Loughran & McDonald, 2017), we examine filing download patterns to capture direct investor interest in cybersecurity disclosures.

Our sample comprises 760 Form 10-K/A amendments filed in 2024 for fiscal years ending on or after December 15, 2023, when companies became subject to the new cybersecurity disclosure requirements. We classify amendments into two categories: those adding Item 1C cybersecurity disclosures omitted from the original filing, and control amendments containing non-cybersecurity information. Each amendment is observed twice: downloads of the original 10-K filing and downloads of the subsequent amendment. We measure investor attention as the number of human-readable file views over a five-day trading window following each filing date. We estimate the specification in Equation (3) where $Cyber_i$ equals one if the 10-K/A amendment adds Item 1C content (zero for other amendments), $Post_t$ equals one for the amendment filing (zero for the original 10-K). The model is estimated using Poisson regression to accommodate count data. Given the few cybersecurity amendments ($N = 11$), we use bootstrapped standard errors (1,000 iterations).

Table 7, Column 2 reports the results. The interaction coefficient is positive but not statistically significant ($\beta = 0.226$, $t = 1.19$), indicating that cybersecurity amendments do not attract measurably different investor attention compared to other amendment types. This pattern may partly reflect the processing-cost dynamics identified by Blankespoor (2019): when mandatory disclosures do not materially reduce information processing costs, investors may not allocate incremental attention. Taken together with the event study and earnings call results, the evidence suggests that despite the SEC's regulatory emphasis on cybersecurity transparency, investors do not differentially prioritize cybersecurity information relative to other corporate disclosures. Our finding of a minimal market response to Item 1C aligns with recent research on specialized SEC mandates, such as the CEO-employee pay ratio rule examined by Jung et al. (2021), which demonstrates that mandatory disclosures often serve as a hybrid between regulation and strategic communication. Cybersecurity governance information may satisfy a stakeholder need for accountability and formal documentation without necessarily providing the type of news that triggers immediate market re-pricing.

6. Conclusions

In 2023, the SEC implemented Regulation S-K Item 106, mandating standardized cybersecurity disclosures for all publicly traded companies. This study examines the initial responses to this mandate by analyzing the resulting disclosures in 10-K annual reports and the associated market reactions. We also investigate whether the mandate generates new disclosure or merely relocates existing cybersecurity content from elsewhere in the 10-K.

As one of the first major economies to mandate public cybersecurity disclosures, unlike the forthcoming EU NIS2 Directive which requires non-public documentation, the U.S. regulation serves as a valuable reference point for evaluating transparency-oriented cybersecurity disclosure policies. Firm characteristics, especially firm size and industry, significantly influence cybersecurity disclosure practices under the new mandate, though they explain only moderate variance. Financial performance, Big-4 auditors, firm

complexity, cyber risk exposure, and risk committee presence consistently predict higher-quality disclosures with greater length, and specificity. Conversely, firms with elevated litigation risk tend to limit disclosure detail.

Past reporting patterns often affect current practices, increasing boilerplate language, while firms typically mirror their industry peers' disclosure approaches. Notably, prior cyber breaches, IT weaknesses, digitalization levels, or tech status showed no significant correlation with disclosure quality, suggesting possible strategic underreporting (Amir et al., 2018; Ettredge et al., 2018; Jiang et al., 2022). The additional analyses showed that Item 1C represents new disclosure content that is focused on governance processes, rather than existing risk factor language being relocated. The mandate had its greatest impact on firms with limited prior cybersecurity disclosure.

Interestingly, we find no evidence of a systematic market reaction to the new cybersecurity disclosures. Our additional analyses of investor attention through earnings calls and filing download activity suggest that despite the SEC's regulatory emphasis on cybersecurity transparency, investors do not differentially prioritize or allocate additional attention to cybersecurity information. As Beyer et al. (2010) state, more information is not always beneficial when strategic players interact. In cybersecurity disclosure, this strategic player is not a market competitor but a malicious adversary. This explains why firms may limit disclosure as a security decision — a behavior that distinguishes cybersecurity from other risk reporting contexts where comprehensive disclosure is rewarded.

Our findings are relevant to the stakeholder debate documented in the SEC's rulemaking process. The minimal market reaction we observe (RQ2) provides limited support for the SEC's prediction that mandatory disclosure would reduce information asymmetry and mispricing. At least in the first compliance year, it seems that investors are not extracting useful information from these disclosures that would lead to differential pricing. This finding lends some support to industry concerns that the mandate imposes compliance costs without equivalent benefits to investors, though such benefits may yet emerge as investors learn to interpret these disclosures. The size-driven variation in disclosure quality (RQ1) confirms industry warnings that smaller firms face disproportionate challenges in meeting disclosure requirements. Policymakers should evaluate whether compliance costs are proportionate to benefits, especially for smaller firms. These insights are relevant not only for potential revisions to S-K 106, but also for other jurisdictions planning to implement similar requirements, directly addressing Leuz's (2018) call for evidence-based policymaking informed by timely research.

Like most empirical research, our study has limitations. With only one year of data currently available, we caution against drawing definitive conclusions about the long-term impact of these new regulations. We also acknowledge that the benefits of the new disclosure regime may be primarily organizational rather than market-facing, as highlighted by our expert interviewees. Mandatory cybersecurity disclosures, although verifiable and potentially delayed, can perform a confirmatory role consistent with Gigler and Hemmer's (1998) framework, thereby enriching the informational environment concerning prior and future event-driven disclosures. The minimal market response is consistent with a well-functioning confirmatory regime as conceptualized by Gigler and Hemmer (1998), though we cannot rule out that investors regard these disclosures as uninformative. While the market relies on more timely information sources for valuation, the disclosure regime succeeds in establishing formal accountability and governance standards. Rather than being substitutes, we suggest that these two requirements (Form 8-K and 10-K Item 1C) are best understood as complements within a well-functioning disclosure system. The 8-K serves a price-discovery function by providing timely information on material shocks to the firm's cybersecurity posture. The 10-K Item 1C serves a confirmatory and accountability function. This interpretation has important policy implications. Our results suggest the disclosure is functioning as theory predicts; annual governance disclosures (Item 1C) serve confirmatory and accountability functions. The challenge for policymakers becomes not necessarily increasing the informational content of Item 1C disclosures but rather ensuring that the confirmatory role effectively supports governance objectives.

Nevertheless, it is important to conduct early analyses of these disclosures to understand their initial impact. As more years of cybersecurity disclosure data become available, future research will be able to explore the evolution of these practices, assess any longer-term market effects, and investigate which specific aspects of disclosure quality or content might eventually influence investor decisions or other outcomes, such as the likelihood of future cyber attacks (Wang et al., 2013), mitigative effects (Chen et al., 2023; Jiang et al., 2022), or changes in the firm's cost of capital (Heinle & Smith, 2017).

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Appendix A. Variable definitions

Variable	Source	Definition
Item 1C characteristics (time *t*)		
Words	10K	Total word count in the cybersecurity disclosure section (Campbell et al., 2014)
Bloat	10K	Proportion of cybersecurity disclosure considered redundant or less relevant. Calculated as the difference between the original disclosure length and an AI-generated summary, scaled by the original length (Kim et al., 2024).
Specificity	10K	Proportion of specific entities (e.g., people, organizations, abbreviations, numbers, monetary values) mentioned in the cybersecurity disclosure (Hope et al., 2016).
Financials (*t-1*)		

(*continued on next page*)

(*continued*)

size	CS	Natural logarithm of market value of equity at fiscal year end.
roa	CS	Return on assets, calculated as operating income divided by total assets.
lvg	CS	Financial leverage; total liabilities divided by total assets.
cash	CS	Cash holdings; cash and equivalents scaled by total assets.
mtb	CS	Market-to-book ratio; market value divided by book value of equity.
big4	CS	Equals 1 if auditor is a Big Four firm, 0 otherwise.
inst_own	TR	Proportion of shares outstanding held by institutional investors.
num_est	IBES	Number of analysts issuing earnings estimates.
10-K characteristics (*t-1*)		
length	LM	Natural logarithm of total length (words) of the entire 10-K report.
senti_nega	LM	Proportion of negative words in the 10-K report.
senti_posi	LM	Proportion of positive words in the 10-K report.
uncertainty	LM	Proportion of uncertainty-related words in the 10-K report.
litigation	LM	Proportion of litigation-related words in the 10-K report.
complex	LM	Proportion of complexity-related words in the 10-K report.
sec_letter	AA	Equals 1 if the firm received a prior SEC comment letter, 0 otherwise.
Technology (*t-1*)		
itmw	AA	Equals 1 if IT-related internal control weaknesses reported, 0 otherwise.
digi_score	10K	Firm-level digitalization score (Kindermann et al., 2021)
cyber_score	10K	Firm-level cyber-risk exposure (Jamilov et al., 2021)
tech_comm	BX	Equals 1 if firm has a technology committee, 0 otherwise.
risk_comm	BX	Equals 1 if firm has a risk committee, 0 otherwise.
tech_firm	CS	Equals 1 if firm operates in a technology-intensive industry, 0 otherwise.
Prior disclosure (*t-1*)		
prior_cyber	10K	Proportion of cybersecurity-related words in Item 1A of the 10-K.
prior_attack	AA	Equals 1 if firm previously disclosed a cyberattack, 0 otherwise.
Change analysis		
$\Delta Topics$	10K	Natural logarithm of KL divergence between the firm's 2023 Item 1A cybersecurity topic distribution and its 2024 combined Item 1A and Item 1C distribution.
$\Delta Volume$	10K	Natural logarithm of the ratio of cybersecurity-related sentences in 2024 (Item 1A and Item 1C combined) to 2023 (Item 1A only).
Peer and fixed effects		
peer_avg		Peer TNIC similarity-weighted average disclosure characteristic.
sizeFE	CS	Size fixed effects, based on rounded log-10 market capitalization.
industryFE	CS	Industry fixed effects, based on Fama-French 12-industry categorization.
Event study (event = 10-K filing date)		
$\lvert CAR \rvert$	CRSP	Absolute difference between firm's total return and CRSP value-weighted market return over three-day window (days –1 to + 1), centered on the 10-K filing date.
AVOL	CRSP	Ratio of trading volume over the three-day filing window (days –1 to + 1) to baseline volume in the pre-event period (days –70 to –10).
mcap	CRSP	The logarithm of the firm's market capitalization at fiscal year end.
prc	CRSP	The logarithm of the stock's price per share at fiscal year end.
mom	CRSP	The stock's 60-day cumulative return leading up to earnings announcement.
ear	CRSP	The absolute three-day cumulative abnormal return surrounding the firm's earnings announcement prior to the 10-K filing.
prior_8k	SEC	an indicator for cybersecurity incident 8-K disclosures during the 365 days prior to the 10-K filing.

Sources: 10-K filing (10K); Audit Analytics (AA), BoardEx (BX), Compustat (CS), Institutional Brokers' Estimate System (IBES), Securities Exchange Commission EDGAR (SEC), Loughran-McDonald (LM), Thomson-Reuters (TR).

Appendix B. Supplementary data

Supplementary data to this article can be found online at https://doi.org/10.1016/j.accinf.2026.100775.

Data availability

All data are from publicly available sources identified in the study.

References

Abramova, I., Core, J.E., Sutherland, A., 2020. Institutional investor attention and firm disclosure. Account. Rev. 95 (6), 1–21. https://doi.org/10.2308/tar-2018-0494.

Amir, E., Levi, S., Livne, T., 2018. Do firms underreport information on cyber-attacks? evidence from capital markets. Rev. Acc. Stud. 23 (3), 1177–1206. https://doi.org/10.1007/s11142-018-9452-4.

Bao, Y., Datta, A., 2014. Simultaneously discovering and quantifying risk types from textual risk disclosures. Manag. Sci. 60 (6), 1371–1391. https://doi.org/10.1287/mnsc.2014.1930.

Beatty, A., Cheng, L., Zhang, H., 2019. Are risk factor disclosures still relevant? evidence from market reactions to risk factor disclosures before and after the financial crisis. Contemp. Account. Res. 36 (2), 805–838. https://doi.org/10.1111/1911-3846.12444.

Benaroch, M., 2021. Third-party induced cyber incidents—much ado about nothing? Journal of Cybersecurity 7 (1), 1–18. https://doi.org/10.1093/cybsec/tyab020.

Berkman, H., Jona, J., Lee, G., Soderstrom, N., 2018. Cybersecurity awareness and market valuations. J. Account. Public Policy 37 (6), 508–526. https://doi.org/10.1016/j.jaccpubpol.2018.10.003.

Beyer, A., Cohen, D.A., Lys, T.Z., Walther, B.R., 2010. The financial reporting environment: Review of the recent literature. J. Account. Econ. 50 (2–3), 296–343. https://doi.org/10.1016/j.jacceco.2010.10.003.
Blankespoor, E., 2019. The impact of information processing costs on firm disclosure choice: evidence from the XBRL mandate. J. Account. Res. 57 (4), 919–967. https://doi.org/10.1111/1475-679X.12268.
Calderon, T.G., Gao, L., 2022. Changes in corporate cybersecurity risk disclosures after SEC comment letters. J. Account. Public Policy 41 (5), 106993. https://doi.org/10.1016/j.jaccpubpol.2022.106993.
Campbell, J.L., Chen, H., Dhaliwal, D.S., Lu, H., Steele, L.B., 2014. The information content of mandatory risk factor disclosures in corporate filings. Rev. Acc. Stud. 19 (1), 396–455. https://doi.org/10.1007/s11142-013-9258-3.
Campbell, K., Gordon, L., Loeb, M., Zhou, L., 2003. The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. J. Comput. Secur. 11 (3), 431–448. https://doi.org/10.3233/JCS-2003-11308.
Cavusoglu, H., Mishra, B., Raghunathan, S., 2004. The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. Int. J. Electron. Commer. 9 (1), 70–104. https://doi.org/10.1080/10864415.2004.11044320.
Cazier, R., McMullin, J., Treu, J., 2021. Are lengthy and boilerplate risk factor disclosures inadequate? an examination of judicial and regulatory assessments of risk factor language. Account. Rev. 96 (4), 131–155. https://doi.org/10.2308/TAR-2018-0657.
Cazier, R.A., Pfeiffer, R.J., 2016. Why are 10-K filings so long? Account. Horiz. 30 (1), 1–21. https://doi.org/10.2308/acch-51240.
Chen, C.Y., Goh, B.W., Lee, J., Li, N., 2025. The effect of cybersecurity breaches on analysts' earnings forecasts. European Accounting Review 1–27. https://doi.org/10.1080/09638180.2025.2476760.
Chen, J., Henry, E., Jiang, X., 2023. Is cybersecurity risk factor disclosure informative? evidence from disclosures following a data breach. J. Bus. Ethics 187, 199–224. https://doi.org/10.1007/s10551-022-05107-z.
Diamond, D.W., Verrecchia, R.E., 1991. Disclosure, liquidity, and the cost of capital. J. Financ. 46 (4), 1325–1359. https://doi.org/10.1111/j.1540-6261.1991.tb04620.x.
Dye, R.A., 2001. An evaluation of "essays on disclosure" and the disclosure literature in accounting. J. Account. Econ. 32 (1–3), 181–235. https://doi.org/10.1016/S0165-4101(01)00024-6.
Dyer, T., Lang, M., Stice-Lawrence, L., 2017. The evolution of 10-K textual disclosure: evidence from latent Dirichlet allocation. J. Account. Econ. 64 (2–3), 221–245. https://doi.org/10.1016/j.jacceco.2017.07.002.
Ettredge, M.L., Guo, F., Li, Y., 2018. Trade secrets and cyber security breaches. J. Account. Public Policy 37 (6), 564–585. https://doi.org/10.1016/j.jaccpubpol.2018.10.006.
Gao, L., Calderon, T.G., Tang, F., 2020. Public companies' cybersecurity risk disclosures. Int. J. Account. Inf. Syst. 38, 100468. https://doi.org/10.1016/j.accinf.2020.100468.
Gigler, F., Hemmer, T., 1998. On the frequency, quality, and informational role of mandatory financial reports. J. Account. Res. 36 (Supplement), 117–147. https://doi.org/10.2307/2491310.
Gopalan, R., Martin, X., Srinivasan, K., 2023. Regulatory protection and opportunistic bankruptcy. Contemp. Account. Res. 40 (1), 544–576. https://doi.org/10.1111/1911-3846.12828.
Gordon, L.A., Loeb, M.P., Lucyshyn, W., Sohail, T., 2006. The impact of the Sarbanes-Oxley Act on the corporate disclosures of information security activities. J. Account. Public Policy 25 (5), 503–530. https://doi.org/10.1016/j.jaccpubpol.2006.07.005.
Gordon, L.A., Loeb, M.P., Zhou, L., Wilford, A.L., 2024. Empirical evidence on disclosing cyber breaches in an 8-K report: initial exploratory evidence. J. Account. Public Policy 46, 107226. https://doi.org/10.1016/j.jaccpubpol.2024.107226.
Haapamäki, E., Sihvonen, J., 2019. Cybersecurity in accounting research. Manag. Audit. J. 34 (7), 808–834. https://doi.org/10.1108/maj-09-2018-2004.
Heinle, M.S., Smith, K.C., 2017. A theory of risk disclosure. Rev. Acc. Stud. 22 (4), 1459–1491. https://doi.org/10.1007/s11142-017-9414-2.
Hoberg, G., Phillips, G., 2016. Text-based network industries and endogenous product differentiation. J. Polit. Econ. 124 (5), 1423–1465. https://doi.org/10.1086/688176.
Hope, O.-K., Hu, D., Lu, H., 2016. The benefits of specific risk-factor disclosures. Rev. Acc. Stud. 21 (4), 1005–1045. https://doi.org/10.1007/s11142-016-9371-1.
Jamilov, R., Rey, H., & Tahoun, A. (2021). The anatomy of cyber risk (Working Paper No. w28906). National Bureau of Economic Research. DOI: 10.3386/w28906.
Jiang, W., Legoria, J., Reichelt, K.J., Walton, S., 2022. Firm use of cybersecurity risk disclosures. J. Inf. Syst. 36 (1), 151–180. https://doi.org/10.2308/ISYS-2020-067.
Jung, S.-M., Kim, N., Ryu, H.S., Shin, J.Y., 2021. Why do firms utilize the flexibility allowed in CEO employee pay ratio disclosure? evidence from Dodd-Frank Act Section 953 (b). Account. Horiz. 35 (2), 83–106. https://doi.org/10.2308/HORIZONS-19-053.
Kim, A. G., Muhn, M., & Nikolaev, V. V. (2024). Bloated disclosures: Can ChatGPT help investors process information? (Chicago Booth Research Paper). DOI: 10.2139/ssrn.4425527.
Kindermann, B., Beutel, S., de Lomana, G.G., Strese, S., Bendig, D., Brettel, M., 2021. Digital orientation: Conceptualization and operationalization of a new strategic orientation. Eur. Manag. J. 39 (5), 645–657. https://doi.org/10.1016/j.emj.2020.10.009.
Kravet, T., Muslu, V., 2013. Textual risk disclosures and investors' risk perceptions. Rev. Acc. Stud. 18, 1088–1122. https://doi.org/10.1007/s11142-013-9228-9.
Lang, M., Stice-Lawrence, L., 2015. Textual analysis and international financial reporting: Large sample evidence. J. Account. Econ. 60 (2–3), 110–135. https://doi.org/10.1016/j.jacceco.2015.09.002.
Lawrence, A., Minutti-Meza, M., Vyas, D., 2018. Is operational control risk informative of financial reporting deficiencies? Audit. J. Pract. Theory 37 (1), 139–165. https://doi.org/10.2308/ajpt-51784.
Leuz, C., 2018. Evidence-based policymaking: promise, challenges and opportunities for accounting and financial markets research. Account. Bus. Res. 48 (5), 582–608. https://doi.org/10.1080/00014788.2018.1470151.
Li, H., No, W., Wang, T., 2018. SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. Int. J. Account. Inf. Syst. 30, 40–55. https://doi.org/10.1016/j.accinf.2018.06.003.
Loughran, B., McDonald, T., 2017. The use of EDGAR Filings by investors. J. Behav. Financ. 18 (2), 231–248. https://doi.org/10.1080/15427560.2017.1308945.
Loughran, B., McDonald, T., 2024. Measuring firm complexity. J. Financ. Quant. Anal. 59 (6), 2487–2514. https://doi.org/10.1017/S0022109023000716.
Lowry, M., Michaely, R., Volkova, E., 2020. Information revealed through the regulatory process: Interactions between SEC and companies ahead of their IPO. Rev. Financ. Stud. 33 (12), 5510–5554. https://doi.org/10.1093/rfs/hhaa007.
Matsumoto, D., Pronk, M., Roelofsen, E., 2011. What makes conference calls useful? the information content of managers' presentations and analysts' discussion sessions. Account. Rev. 86 (4), 1383–1414. https://doi.org/10.2308/accr-10034.
Richardson, V.J., Smith, R.E., Watson, M.W., 2019. Much ado about nothing: the (lack of) economic impact of data privacy breaches. J. Inf. Syst. 33 (3), 227–265. https://doi.org/10.2308/isys-52379.
Rosati, P., Gogolin, F., Lynn, T., 2022. Cybersecurity incidents and audit quality. European Accounting Review 31 (3), 701–728. https://doi.org/10.1080/09638180.2020.1856162.
SEC (2011). CF disclosure guidance: Topic No. 2. https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.
SEC (2018). Commission statement and guidance on public company cybersecurity disclosures. https://www.sec.gov/rules/interp/2018/33-10459.pdf.
SEC (2023). Cybersecurity risk management, strategy, governance, and incident disclosure. https://www.federalregister.gov/documents/2023/08/04/2023-16194/cybersecurity-risk-management-strategy-governance-and-incident-disclosure.
Sihvonen, J. (2024). Digitalization and cybersecurity: Firm-level evidence. Unpublished manuscript.
Spanos, G., Angelis, L., 2016. The impact of information security events to the stock market: a systematic literature review. Comput. Secur. 58, 216–229. https://doi.org/10.1016/j.cose.2015.12.006.
Verrecchia, R.E., 1983. Discretionary disclosure. J. Account. Econ. 5, 179–194. https://doi.org/10.1016/0165-4101(83)90011-3.

Walton, S., Wheeler, P.R., Zhang, Y., Zhao, X., 2021. An integrative review and analysis of cybersecurity research: current state and future directions. J. Inf. Syst. 35 (1), 155–186. https://doi.org/10.2308/ISYS-19-033.

Wang, T., Kannan, K., Ulmer, J., 2013. The association between the disclosure and the realization of information security risk factors. Inf. Syst. Res. 24 (2), 201–218. https://doi.org/10.1287/isre.1120.0437.

Wang, W., Zhang, L., Wilson, M., Kala, T., 2022. SEC compensation-related comment letters and excess CEO compensation. European Accounting Review 31 (5), 1089–1118. https://doi.org/10.1080/09638180.2022.2046120.

WEF (2024, January). Widening disparities and growing threats cloud global cybersecurity outlook for 2024. https://www.weforum.org/press/2024/01/wef24-global-cybersecurity-outlook-2024/.