Scientific Research Publishing

Journal of Information Security, 2025, 16(4), 500-516
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Cybersecurity Reporting: Preliminary Empirical Evidence on the Impact of Item 1C of 10-K Reports Filed with the SEC

Lawrence A. Gordon[1], Martin P. Loeb[1], Chih-Yang Tseng[2], Lei Zhou[1]

[1]Robert H. Smith School of Business, University of Maryland, College Park, MD, USA
[2]College of Management, Taiwan University, Taipei City
Email: lagordon@umd.edu, mploeb@umd.edu, chihyangtseng@ntu.edu.tw, lzhou@umd.edu

How to cite this paper: Gordon, L.A., Loeb, M.P., Tseng, C.-Y. and Zhou, L. (2025) Cybersecurity Reporting: Preliminary Empirical Evidence on the Impact of Item 1C of 10-K Reports Filed with the SEC. *Journal of Information Security*, **16**, 500-516.
https://doi.org/10.4236/jis.2025.164025

Received: August 21, 2025
Accepted: October 13, 2025
Published: October 16, 2025

Abstract

This paper provides evidence of the impact of the 2023 U.S. Security and Exchange Commission (SEC) disclosure rules requiring registrants to disclose their approach toward Cybersecurity Risk Management (CRM) in Item 1C (Cybersecurity) of Form 10-K. Specifically, the paper investigates how Material Weaknesses in Internal Control (MWIC) influence a firm's decision to disclose the integration of its CRM system into its Enterprise Risk Management (ERM) framework in Item 1C. The empirical analysis indicates that firms reporting MWIC are significantly less likely to disclose in Item 1C the fact that they integrated their CRM system into their ERM framework compared to companies that do not report any MWIC. However, companies reporting both IT MWIC and non-IT MWIC are significantly more likely to disclose in Item 1C the fact that they integrated their cyber risk management systems into their overall enterprise risk management framework compared to companies only reporting non-IT MWIC.

Keywords

Cybersecurity Economics, Information Security, Cybersecurity Regulations, 10-K Cybersecurity Disclosures, Internal Control, Material Weaknesses

1. Introduction

Organizations face a variety of risks, including financial, operational, investment, financial reporting, compliance, and cybersecurity risks. Viewed from a holistic or overall perspective, managing these risks is referred to as Enterprise Risk Management (ERM). COSO ([1]: p. 2) defines Enterprise Risk Management as "…a

process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives". In a complementary publication, COSO ([2]: p. 6) "…clarifies the importance of enterprise risk management in strategic planning and embedding it throughout an organization—because risk influences and aligns strategy and performance across all departments and functions".

Internal Control plays a critical role in managing a company's ERM system, especially when it comes to managing financial reporting risk. Indeed, the reliability of financial reports filed with the U.S. Securities and Exchange Commission (SEC) is monitored via the Internal Control requirements specified by the Sarbanes-Oxley Act of 2002 (SOX). Furthermore, material weaknesses in Internal Control (IC) need to be identified and reported in a firm's 10-K report filed with the SEC.

A necessary, although not sufficient, condition of reliable financial reporting for contemporary organizations operating in a computer-based digital environment is cybersecurity. Thus, cybersecurity is a critical component of an organization's Internal Control system. In 2023, the SEC issued mandatory cybersecurity disclosure rules [3] requiring its registrants to disclose their approach toward Cybersecurity Risk Management (CRM) in Item 1C (Cybersecurity) of Form 10-K. These rules went into effect beginning with annual reports filed with the SEC for fiscal years ending on or after December 15, 2023. In discussing this requirement, the SEC explicitly notes that it would be beneficial for registrants to take a holistic approach to CRM. In essence, the SEC recommends that companies integrate their CRM systems into their ERM framework.

The objective of the study is to assess the association between companies that have reported MWIC in their 10-K reports and companies that have discussed in Item 1C the fact that their CRM systems are integrated into their ERM framework. To pursue this objective, we began by developing a database consisting of the information disclosed in Item 1C for companies filing a 10-K on or after December 15, 2023. Our database also contains information on reported MWIC in the year corresponding to the 1C data. To our knowledge, this is the first study to look at the association between companies reporting MWIC and the cybersecurity disclosures contained in Item 1C of 10-K filings.

The main findings from the current study are as follows. First, we found that companies that report MWIC are less likely to disclose in Item 1C the fact that they integrated their CRM system into their ERM framework compared to companies that do not report any MWIC. Second, we found that companies reporting both IT MWIC and non-IT MWIC are significantly more likely to disclose in Item 1C the fact that they integrated their cyber risk management systems into their overall Enterprise Risk Management (ERM) framework when compared to companies only reporting non-IT MWIC.

The remainder of this paper proceeds as follows. In the second section of the

paper, we briefly review the relevant literature leading up to the 2023 SEC rules concerning cybersecurity disclosures. We also provide a description of the requirements of Item 1C of Form 10-K in the second section of the paper. In the third section of the paper, we develop specific hypotheses underlying our empirical study. Section four outlines the methodology for compiling and analyzing Item 1C disclosures and corresponding MWIC data from 10-K filings submitted on or after December 15, 2023. The fifth section of the paper discusses our study's empirical findings, as well as the statistical tests used to derive such findings. The implications of our findings are discussed in the sixth section of the paper. Concluding comments are provided in the seventh section of the paper.

2. Literature Review

COSO ([4]: p. 3) defines *Internal Control* as "…a process, affected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives related to operations, reporting, and compliance". There are three main objectives of Internal Control. These objectives are: "*Operations Objectives*—These pertain to effectiveness and efficiency of an entity's operations… *Reporting Objectives*—These pertain to internal and external financial and non-financial reporting and may encompass reliability, timeliness, transparency… *Compliance Objectives*—These pertain to adherence to laws and regulations…" ([4]: p. 3). Sections 302 and 404 of SOX specifically address Internal Control requirements that need to be reported in a firm's 10-K report filed with the SEC. As is clear from these sections, SOX defines Internal Control in terms of the reporting objectives noted above. Although not explicitly stated in SOX, a firm cannot have reliable financial reports without cybersecurity in a computer-based digital environment.[1] Thus, cybersecurity must be an integral part of a firm's Internal Control system in today's interconnected digital environment [6].

Cybersecurity risks, and resulting cyber incidents, are major concerns for organizations in both the private and public sectors of economies around the world. In fact, recent studies show that cybersecurity risks are among the top, if not the top, risk concerns for businesses. For example, the 2024 study by Allianz found cyber incidents to be the top global business risk for companies of all sizes ([7]: p. 7). Although the focus of the current study is on large U.S. publicly traded companies, cybersecurity risks and cyber incidents are of major concern to small companies, governmental municipalities and agencies, and macroeconomies throughout the world.

Issues related to cybersecurity risk, and resulting cyber incidents, have also been a fundamental national and economic security concern among U.S. politicians for

[1]By 2002, when SOX was passed, all major companies were dependent on computer-based information systems. In his 2007 Congressional Testimony before the Subcommittee on Homeland Security, Gordon [5] argued that, in a computer-based digital environment, cybersecurity is a necessary, although not sufficient, condition for a firm to have reliable financial reports. Today, this view is well accepted by those interested in reliable financial reports.

some time. This concern transcends political party affiliation [8] [9]. For example, President Bush initiated the U.S. National Strategy to Secure Cyberspace in 2003 [10]. This document began with the following: "The way business is transacted, government operates, and national defense is conducted have [sic] changed. These activities now rely on an interdependent network of information technology infrastructures called cyberspace. The *National Strategy to Secure Cyberspace* provides a framework for protecting this infrastructure that is essential to our economy, security, and way of life." [10]

In 2013, President Obama issued Executive Order (EO) 13636, noting that: "The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure in the face of such threats." [11] EO 13636 assigned NIST (National Institute of Standards and Technology) the task of developing a cybersecurity risk management framework within one year. In 2017, President Trump issued EO 13800, which required all federal government agencies to use the NIST cybersecurity framework for managing cybersecurity risk [12]. As stated in EO 13800, "Effective immediately, each agency head shall use *The Framework for Improving Critical Infrastructure Cybersecurity* (the Framework) developed by the National Institute of Standards and Technology, or any successor document, to manage the agency's cybersecurity risk" [12].

In 2021, President Biden issued the "Statement by President Joe Biden on Cybersecurity Awareness Month" that began with the following: "Cyber threats can affect every American, every business regardless of size, and every community. That's why my administration is marshalling a whole-of-nation effort to confront cyber threats." [13]

The growing concern with cybersecurity risks and cyber incidents during the early years of the 21st century also resulted in the SEC issuing "CF Disclosure Guidance: Topic No. 2" in 2011 (hereafter, 2011 Disclosure Guidance [14]). This was the first official statement by the SEC concerning the need for publicly traded companies to voluntarily disclose information on their cybersecurity risks and cyber incidents. The overriding theme of the 2011 Disclosure Guidance was that investors have a right to know about a registrant's cybersecurity risks and cyber incidents, when such information would potentially impact investment decisions concerning the company. Although this document resulted in a significant increase in the number of SEC registrants that voluntarily disclosed information concerning their cybersecurity risks and cyber incidents [15], cyber incidents were generally not disclosed in a timely manner [16].

Furthermore, despite the SEC's 2011 Disclosure Guidance, the frequency and magnitude of cyber incidents continued to increase at an alarming rate. In addition, the cyber incident at Equifax, Inc. in 2017 raised the issue of insider trading on cybersecurity-related information. Consequently, in 2018, the SEC's Commissioners revisited the issues associated with disclosures of cybersecurity risks and cyber incidents and issued the "Commission Statement and Guidance on Public Company Cybersecurity Disclosures" (hereafter, 2018 Commission Statement [17]). The 2018 Commission Statement expanded on points raised in the 2011

Disclosure Guidance and addressed "...two topics not developed in the staff's 2011 guidance, namely the importance of cybersecurity policies and procedures and the application of insider trading prohibitions in the cybersecurity context" ([17]: p. 6). More generally, the 2018 Commission Statement increased the importance and visibility of the cybersecurity disclosures in reports filed with the SEC. However, as with the 2011 Disclosure Guidance, the recommendations of the 2018 Commission Statement concerning disclosures of cybersecurity-related information were also of a voluntary nature.[2]

The 2011 Disclosure Guidance and the 2018 Commission Statement were important steps taken by the SEC to improve the disclosure of registrants' cybersecurity risks and cyber incidents. However, the increasing number and magnitude of cyber breaches since 2018 have culminated in the SEC once again revisiting the issues associated with disclosure of cybersecurity risks and cyber incidents. More specifically, in 2023, the SEC issued mandatory cybersecurity disclosure rules under the title of "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure". The 2023 SEC cybersecurity disclosure rules are intended "...to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incidents by public companies that are subject to the reporting requirements of the Securities Exchange Act of 1934" ([3]: p. 1). The 2023 SEC cybersecurity disclosure rules also require "…periodic disclosures about a registrant's processes to assess, identify, and manage material cybersecurity risks, management's role in assessing and managing material cybersecurity risks, and the board of directors' oversight of cybersecurity risks" ([3]: p. 1).

The 2023 SEC rules specify that disclosures concerning cybersecurity risk management, strategy and governance be in Item 1C, a new subsection of Form 10-K. More to the point, beginning with annual reports filed with the SEC for fiscal years ending on or after December 15, 2023, a 10-K report filed with the SEC by a registrant should contain Item 1C entitled "Cybersecurity". The addition of 1C to a company's 10-K report put in place new mandatory cybersecurity disclosure requirements. As discussed in the next section of this paper, the 2023 SEC cybersecurity disclosure rules also emphasize that it is important for companies to take a holistic approach toward risk by integrating their CRM systems within an ERM framework.

As discussed above, the 2023 SEC disclosure rules include many specific types of cybersecurity-related information that firms should disclose in Item 1C. In addition, the 2023 SEC disclosure rules require registrants to report material cybersecurity incidents in Item 1.05 of Form 8-K.[3] The study reported in this paper is,

[2]The increasing concern with cybersecurity risks and the resulting cybersecurity incidents resulted in a large stream of research studies that have looked at the impact of cyber incidents on investors (e.g., [8] [16] [18]-[24]). The results of these studies are mixed but generally find some evidence of a negative short-term impact on the stock market returns of firms that are victims of successful cyber-attacks.

[3]Although beyond the scope of the current research study, the 2023 SEC rule requiring registrants to report material cybersecurity incidents in Item 1.05 of Form 8-K also represents a recognition by the SEC of the growing importance of cybersecurity to the economic security of a nation. For a further discussion related to material cybersecurity incidents and the SEC 2023 cybersecurity disclosure rules, see [8].

however, focused on assessing whether firms with MWIC disclose in Item 1C the fact that their CRM systems are integrated into their Enterprise Risk Management (ERM) systems. This focus will be the basis for the hypotheses discussed in the next section of the paper.

3. Hypotheses

The 2023 SEC's regulation concerning cybersecurity disclosures explicitly notes that registrants should describe their Cybersecurity Risk Management (CRM) processes in sufficient detail to address, when applicable, "Whether and how any such processes have been integrated into the registrant's overall risk management system or processes"; (Regulation S-K, Item 106 [b]). In other words, SEC recognized the fact that it is beneficial for companies to take a holistic approach to risk management by integrating their CRM systems into their ERM framework.

Although not all registrants disclose the fact that they integrate CRM into ERM, there are several potential benefits to making such a disclosure. Five benefits are as follows. First, cybersecurity risk has a direct impact on other risk categories confronting a company, including financial risk, operational risk, investment risk, and compliance risk. Indeed, in today's interconnected digital environment, cyber risk is a core concern to all other risk factors that rely on information being transmitted and stored via the Internet or any other computer-based information system. Second, by integrating CRM systems into ERM systems, registrants are in a better position to prioritize different risk concerns and to better manage a company's comprehensive risk posture. Third, by integrating CRM systems into ERM systems, registrants can achieve technology-related cost efficiencies in terms of risk identification, assessment, monitoring, and recovery. Fourth, registrants that disclose the fact that their CRM systems are integrated into their ERM systems provide an additional level of transparency concerning their basic approach toward risk management for investors, regulatory agencies, and customers. Fifth, since ERM is, or at least should be, aligned with a company's strategic objectives, embedding CRM within the ERM framework explicitly integrates cyber risk concerns within an organization's strategic planning process.

The above potential benefits provide a compelling argument for a company to disclose the fact that it has integrated its CRM system into its ERM framework in Item 1C. This point is especially true for registrants that do not have any IC reported on their 10-K reports. The lack of any Internal Control weaknesses provides a prima facie case that a company has reliable financial reports, which implies robust cybersecurity practices.

Despite the potential benefits concerning a registrant's decision to disclose the integration of its CRM system into its ERM framework in Item 1C, there may be a strong incentive for a registrant to avoid such disclosure. This incentive arises particularly when a registrant has only non-IT MWIC reported in its 10-K report. In such cases, a conservative approach may be to refrain from mentioning the CRM-ERM integration in Item 1C to avoid inadvertently signaling concerns about the

reliability of financial reporting to stakeholders (e.g., investors, regulators, supply-chain partners, and customers). In other words, when a company reports MWIC in its 10-K, some investors (both current and prospective) could interpret a discussion of CRM-ERM integration in Item 1C as a potential indicator of cybersecurity risk regardless of whether IT MWIC are present. Therefore, even if the CRM system is integrated within the ERM framework, choosing not to disclose this information in the specifically designated IC cybersecurity section of the 10-K report may be deemed the best strategy by many SEC registrants.

Of course, a company's MWIC may include IT-related MWIC. When a registrant's MWIC includes IT MWIC, it seems prudent for the company to signal to investors that it is addressing the IT MWIC concern in Item 1C. One way to provide such a signal is to disclose in Item 1C that the company has integrated its CRM system within its ERM framework. More specifically, companies that report IT MWIC in their 10-K reports would likely see value in highlighting the fact that they are addressing their cybersecurity-related MWIC via the integration of their CRM system within their ERM framework. Thus, these companies are more likely to discuss the integration of their CRM systems within their ERM framework than firms that only have non-IT MWIC.

The above discussion leads us to test two hypotheses, which are stated in the alternative form below.

$H1_1$: Companies that report MWIC in their 10-K reports are less likely to disclose in Item 1C of their 10-K reports that they integrated their CRM system into their ERM framework compared to companies that do not report any MWIC.

$H2_1$: Companies reporting both IT MWIC and non-IT MWIC are more likely to disclose in Item 1C the fact that they integrated their cyber risk management systems into their overall Enterprise Risk Management (ERM) framework when compared to companies that only report non-IT MWIC.

4. Methodology

The approach for testing the above hypotheses required developing a database consisting of the information disclosed in Item 1C of 10-K filings submitted to the SEC for the fiscal year ending 2023. The development of such a database began by downloading 10-K reports filed with the SEC between December 15, 2023, and August 30, 2024. This process yielded 10-K reports for 6176 companies. Analysis of Item 1C was conducted by reviewing this section of the 10-K reports to determine whether each firm's CRM system was integrated within the firm's ERM framework. More specifically, we search for the key term "Enterprise Risk Management" in Section 1C. Surrounding texts were read to ensure the integration of CRM into ERM. Examples of the discussions on such integration are presented in **Appendix**.

We also collected information on the MWIC of companies, as reported in the 10-K filings of companies for the same fiscal year as the Item 1C data, from Audit Analytics (*i.e.*, Audit Analytics collects and categorizes MWIC for publicly traded

companies).[4] Audit Analytics identifies two specific categories of MWIC that are particularly relevant to our study: DC and IC in *information technology*, *software*, *access/security issues*. According to Audit Analytics, category "DC—information technology, software, access/security issues" is defined as "this category of disclosure control issues identifies registrants that have indicated that their material weaknesses or disclosure issues are associated with or derive from deficiencies in their internal information reporting systems, software processing, access controls and/or security systems. This category is also used to identify circumstances when a company has indicated that they are implementing a new ERP or financial reporting system within its organization. "Category IC—information technology, software, security & access issues" is defined as "deficiencies in this category include deficient program controls, software programs/implementation, segregation of duties associated with personnel having access to computer accounting or financial reporting records and related problems with oversight/access to electronic data/programs". These two categories directly capture issues related to cybersecurity and we refer to them collectively as IT MWIC.

To formally test our first hypothesis (**H1$_1$**), we run the following logit regression model Equation (1) using our whole sample.[5]

$$\begin{aligned}\text{Prob}(\text{ERM}=1) = {} & \beta_0 + \beta_1 \text{MWIC} + \beta_2 \text{Size} + \beta_3 \text{MB} + \beta_4 \text{ROA} + \beta_5 \text{Leverage} \\ & + \beta_6 \text{FreeCashFlow} + \text{INdustrty FE} + \varepsilon\end{aligned}. \quad (1)$$

To formally test our second hypothesis (**H2$_1$**), we run the following logit regression model Equation (2) using the subsample of firms reporting MWIC.

$$\begin{aligned}\text{Prob}(\text{ERM}=1) = {} & \beta_0 + \beta_1 \text{IT MWIC} + \beta_2 \text{Size} + \beta_3 \text{MB} + \beta_4 \text{ROA} \\ & + \beta_5 \text{Leverage} + \beta_6 \text{FreeCashFlow} + \text{INdustrty FE} + \varepsilon\end{aligned}. \quad (2)$$

where,

ERM is an indicator variable for the company's integration of CRM with its ERM. ERM is set to 1 if the firm's Section 1C cybersecurity risk disclosure mentions the term "enterprise risk management", and 0 otherwise.

MWIC is an indicator-variable for each of the 21 material weaknesses in Internal Control categorized by Audit Analytics as required by Section 404 of SOX. MWIC is set to 1 if a firm discloses a material weakness in its 10-K report and 0 otherwise.

IT MWIC is an indicator-variable for material weaknesses in Internal Control related to information technology, software, security & access issues (IT) as categorized by Audit Analytics. IT MWIC is set to 1 if a firm discloses an IT material weakness in its 10-K report and 0 otherwise.

Size is the firm's size, measured by the firm's sales revenue.

MB is the market-to-book ratio. The market value is year-end closing share price

[4]Audit Analytics, which was founded in 2003, is a widely used database by both academicians and practitioners (see: https://auditanalytics.com/doc/AuditAnalytics_for_Academia.pdf).

[5]Since only one year of data was available at the time of our study, we did not include a year fixed effect in our regression equations.

multiplied by outstanding shares.

ROA is the return on assets, calculated as the firm's operating income divided by the firm's total assets.

Leverage is the firm's leverage, calculated as the firm's total liabilities divided by its total assets.

FreeCashFlow measures the firm's resources available for integrating cybersecurity risk management with ERM. It is calculated as the cash flow from operating activities minus common and preferred dividends.

5. Empirical Results

5.1. Main Results

Although not stated as a specific hypothesis, we began by assessing whether SEC registrants are adhering to the new rules. As anticipated, most registrants are complying with the new rules and disclosing information concerning their cybersecurity risk management, strategy and governance in Item 1C of Forum 10-K.[6] Of the 6176 10-K reports that were initially downloaded, 5039 companies included disclosures under Item 1C in their 10-K reports for the fiscal year ending 2023 (*i.e.*, over 82%). The main reasons why 1137 (6176-5039) 10-K reports did not contain Item 1C are: (1) smaller reporting companies (*i.e.*, non-accelerated filers) were given until June 15, 2024 to comply with the 1C requirement, and (2) most special entities that are required to file a 10-K report are not required to include Item 1C in their 10-K filings.

Table 1. Sample construction and descriptive statistics.

Panel A: Sample Construction	
Sample Observations	Total Sample
10-K reports downloaded	6176
10-K reports containing no 1C	(1137)
Less: Missing data in Compustat and/or Audit Analytics	(835)
Final sample of firms	4204

Panel B: Descriptive Statistics

	All		**IT MWIC = 1**		**IT MWIC = 0**		**MWIC = 0**	
Variable	**Mean**	**StDev**	**Mean**	**StDev**	**Mean**	**StDev**	**Mean**	**StDev**
ERM	0.43	0.50	0.38	0.49	0.27	0.45	0.46	0.50
Sale	5105.82	25094.48	1021.79	4024.45	1120.28	9520.79	5934.40	27251.03
MB	20.62	395.83	44.72	642.28	102.66	1009.61	8.25	160.20
ROA	0.15	2.20	0.02	2.86	0.02	5.94	0.18	0.84
Leverage	1.51	20.59	0.98	2.18	8.16	62.34	0.71	2.86
FreeCashFlow	717.39	4361.58	63.49	341.90	62.78	730.94	852.16	4770.64
N	**4204**		**272**		**446**		**3486**	

[6]The 2023 SEC cybersecurity disclosure rules, as stated in Regulation S-K Item 106, are mandatory. Thus, we were not surprised by the fact that firms are complying with the rules.

The sample of 5039 companies was further reduced because the data necessary to test our hypotheses was not available for 835 companies. Thus, our final sample was 4204 (5039-835) companies. Table 1 Panel A shows how our final sample was constructed. Of the 4204 companies in our final sample, 718 firms had MWIC, while the remaining 3486 (4204-718) companies did not have any MWIC. Of the 718 companies with MWIC, 272 included IT MWIC and 446 did not.

Table 1 Panel B and Figure 1 provide descriptive statistics on our sample. As illustrated in Figure 1, 45.60% of the firms without any MWIC, 37.50% of the firms with both IT MWIC and non-IT MWIC, and 27.10% of the firms with only non-IT MWIC discussed the integration of their CRM system within the firm's ERM framework.

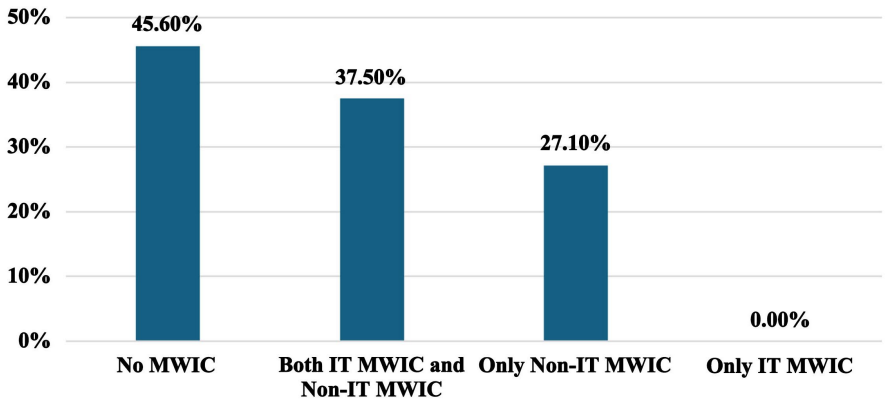

Figure 1. Proportion of firms disclosing the integration of CRM with ERM in Item 1C.

Table 2. Association between disclosing the integration of CRM with ERM and absence of MWIC.

Variable	Coefficient	Wald
Intercept	−0.536	0.506
MWIC	**−0.608**	**45.602*****
Size	0.000	1.361
MB	0.000	0.057
ROA	0.079	3.634*
Leverage	−0.008	1.255
FreeCashFlow	0.000	0.003
Industry FE	Included	
N	4204	
Chi-Square	110.45***	

a. Regression equation: $\text{Prob}(\text{ERM}=1)=\beta_0+\beta_1\text{MWIC}+\beta_2\text{Size}+\beta_3\text{MB}+\beta_4\text{ROA}+\beta_5\text{Leverage}+\beta_6\text{FreeCashFlow}+\text{INdustrty FE}+\varepsilon$. b. *indicates significance at the level of 0.1, **indicates significance at the level of 0.05, ***indicates significance at the level of 0.01.

We now turn our attention to the results of testing the two hypotheses discussed

in the third section of the paper. As shown in Table 2, companies with MWIC are less likely to disclose the integration of CRM within an ERM framework in Item 1C of their 10-K reports compared to companies that do not report any MWIC. The coefficient on this variable is −0.608, and the Wald statistic is significant at the 1% level. In other words, there is a statistically significant association between the absence of MWIC and the disclosure of CRM-ERM integration in Item 1C. These findings support our first alternative hypothesis.

As shown in Table 3, companies with both IT MWIC and non-IT MWIC are more likely to disclose the integration of CRM within an ERM framework in Item 1C of their 10-K reports compared to companies that report only non-IT MWIC. The coefficient on this variable is 0.404, and the Wald statistic is significant at the 5% level. In other words, our study results indicate that companies reporting both IT MWIC and non-IT MWIC are significantly more likely to disclose in Item 1C the fact that they integrated their cyber risk management systems into their overall Enterprise Risk Management (ERM) framework than those reporting only non-IT MWIC. These findings support our second alternative hypothesis.

Table 3. Association between disclosing the integration of CRM into ERM and presence of IT MWIC.

Variable	Coefficient	Wald
Intercept	−0.948	25.496***
IT MWIC	**0.404**	**5.608****
Size	0.000	0.301
MB	0.000	0.047
ROA	0.391	4.798**
Leverage	−0.013	3.364*
FreeCashFlow	0.000	0.019
Industry FE	Included	
N	718	
Chi-Square	25.79*	

a. Regression equation: $\text{Prob}(\text{ERM}=1)=\beta_0+\beta_1\text{IT MWIC}+\beta_2\text{Size}+\beta_3\text{MB}+\beta_4\text{ROA}+\beta_5\text{Leverage}+\beta_6\text{FreeCashFlow}+\text{INdustrty FE}+\varepsilon$. b. *indicates significance at the level of 0.1, **indicates significance at the level of 0.05, ***indicates significance at the level of 0.01.

5.2. Robustness Tests

Prior studies have shown that the companies audited by Big Four auditors may have higher audit quality and are therefore more likely to disclose the integration of CRM into ERM [25] [26]. Thus, in order to check for the robustness of our results, we reran Equations (1) and (2) by adding a control variable for Big Four auditors. After controlling for Big Four auditors, our results are essentially the same as those reported in Table 2 and Table 3, indicating that our findings are

robust.[7]

6. Implications

There are at least three important implications that can be gleaned from the current study. First, adding a new subsection to Form 10-K that explicitly addresses issues related to cybersecurity has resulted in a significant increase in the amount of cybersecurity-related information provided to the investors of SEC registrants. This additional information relates to a company's cybersecurity risk management, its strategy regarding cybersecurity, and its governance of cybersecurity. Of course, there is a fine line between informing investors and inadvertently providing a roadmap that could facilitate future cyber-attacks. Thus, companies need to pay particular attention to inferences that can be drawn from the information contained in Item 1C.

The second implication of the current study is that material weaknesses in a company's Internal Control, as defined by Sections 302 and 404 of SOX, play a significant role in shaping what is disclosed in Item 1C of Form 10-K regarding the integration of a company's CRM system with its ERM system. More specifically, companies that do not report any MWIC in their 10-K reports are apparently more likely to value the opportunity to disclose in Item 1C the integration of their CRM and ERM systems compared to firms reporting MWIC. Presumably, these companies view this disclosure as a way of signaling that they have reliable financial reports, including an appropriate level of cybersecurity. In contrast, companies that report only non-IT MWIC in their 10-K reports are less inclined to disclose in Item 1C that they have integrated their CRM and ERM systems compared to those without any MWIC.[8] It may be that these companies avoid disclosing the CRM-ERM integration to avoid inadvertently raising what they consider unnecessary concerns in Item 1C about the overall reliability of their financial reports. That said, and consistent with expectations, companies that report MWIC that include both IT MWIC and non-IT MWIC are more likely than companies with only non-IT MWIC to disclose in Item 1C the fact that they have integrated their CRM and ERM systems. These disclosures are likely intended to signal that the company is taking active steps to address its cybersecurity weaknesses.

The third implication of the study is that accountants and auditors, through their Internal Control duties, play a key role in corporate cybersecurity and its disclosure. Given the central importance of cybersecurity to nearly all organizational activities in today's interconnected digital world, it would be prudent for accounting educators to incorporate cybersecurity-related topics in their accounting curriculum. Additionally, given the importance of cybersecurity disclosures in

[7]These results are available upon requests from the authors.

[8]The fact that a company does not disclose the integration of its CRM system with its ERM system could be the result of the systems not being integrated or the fact that the company does not have an ERM system. Unfortunately, we can't determine from our database which of these two explanations account for our results.

the 10-K reports filed with the SEC by publicly traded companies, it would be prudent for cybersecurity educators to incorporate the SEC cybersecurity disclosure rules in their curriculum.

7. Concluding Comments

Technological advances over the past several decades have all been dependent on computer-based digital systems. This holds true for systems that utilize the Internet, social networks, artificial intelligence, data analytics, blockchain, financial and economic systems, manufacturing robotics, and virtually all other forms of computer-based information systems. A central concern across all these systems is cybersecurity. Indeed, cyber risk has become one of the, if not the, top risk concerns facing organizations in today's digital environment.

The importance of cyber risk and the impact of resulting cyber incidents have long been key concerns for the U.S. Securities and Exchange Commission (SEC). The SEC 2011 Disclosure Guidance and 2018 Commission Statement were significant steps by the SEC to encourage publicly traded firms to improve their disclosure of the companies' cybersecurity risks and cyber incidents. The resulting disclosures were, however, of a voluntary nature and lacked consistency across companies. As SEC Chair, Gary Gensler, noted in a press statement on July 26, 2023, "Currently, many public companies provide cybersecurity disclosure to investors. I think companies and investors alike, however, would benefit if this disclosure were made in a more consistent, comparable, and decision-useful way."[9] Consequently, the SEC issued mandatory cybersecurity disclosure rules in 2023 under the title of "Cybersecurity Risk Management, Strategy, Governance and Incident Disclosure" [3]. A major component of these rules is that annual 10-K reports filed with the SEC for fiscal years ending on or after December 15, 2023, should contain a new section, Item 1C, titled "Cybersecurity." These rules recommend that, where applicable, registrants address in 1C whether their CRM practices have been integrated within their Enterprise Risk Management (ERM) framework.

Based on an analysis of data gathered between December 15, 2023, and August 30, 2024, preliminary empirical evidence found an association between companies that disclose the integration of CRM within an ERM framework and the MWIC reported by those firms. Of course, the most important issue is whether such disclosures, and their relationship to MWIC, are decision-useful to investors, as emphasized by SEC Chair Gensler. As more data becomes available, it will be possible to address this issue, along with many other important issues related to the data provided in 1C of Form 10-K.

As with all empirical studies, the study reported in this paper has limitations. The limitations of this study include the following. First, our analysis is based on a limited data set, as the 2023 rules only applied to annual 10-K reports filed with the SEC for fiscal years ending on or after December 15, 2023. As more data becomes available, a clearer picture of the association between companies that dis-

[9]See: https://www.sec.gov/newsroom/press-releases/2023-139.

close the integration of CRM within an ERM framework and the MWIC reported by firms will likely emerge. For example, it would be possible to examine whether the integration of CRM into ERM has a reverse impact on MWIC. Second, although firms are now required to include Item 1C in their 10-K reports, nearly all SEC registrants are still discussing issues related to their cybersecurity risks and cyber incidents under Item 1A (Risk Factors) in their 10-K reports. Thus, further research concerning issues related to the information disclosed in Item 1C should also take into consideration the disclosure of information related to cybersecurity in Item 1A. Third, we cannot distinguish between firms that have not integrated CRM into ERM and firms that either do not have an ERM system or have chosen not to disclose such integration.

The above limitations notwithstanding, we believe that the findings from this study provide an important first look at the disclosures in Item 1C. Our next step is to address the three limitations discussed above.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2004) Enterprise Risk Management—Integrated Framework, Executive Summary.

[2] Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2017) Enterprise Risk Management: Integrating with Strategy and Performance, Executive Summary.

[3] Securities and Exchange Commission (2023) Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure. https://www.sec.gov/files/rules/final/2023/33-11216.pdf

[4] Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2013) Internal Control—Integrated Framework, Executive Summary.

[5] Gordon, L.A. (2007) Incentives for Improving Cybersecurity in the Private Sector: A Cost-Benefit Perspective, Congressional Testimony before Homeland Security Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology. Congressional Record. https://www.govinfo.gov/content/pkg/CHRG-110hhrg48977/html/CHRG-110hhrg48977.htm

[6] Gordon, L.A., Loeb, M.P., Lucyshyn, W. and Zhou, L. (2018) Empirical Evidence on the Determinants of Cybersecurity Investments in Private Sector Firms. *Journal of Information Security*, **9**, 133-153. https://doi.org/10.4236/jis.2018.92010

[7] Allianz Commercial (2024) Allianz Risk Barometer: Identifying the Major Business Risks for 2024. 1-51. https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/Allianz-Risk-Barometer-2024.pdf

[8] Gordon, L.A., Loeb, M.P., Zhou, L. and Wilford, A.L. (2024) Empirical Evidence on Disclosing Cyber Breaches in an 8-K Report: Initial Exploratory Evidence. *Journal of Accounting and Public Policy*, **46**, Article ID: 107226. https://doi.org/10.1016/j.jaccpubpol.2024.107226

[9] Gordon, L.A., Loeb, M.P. and Zhou, L. (2020) Integrating Cost-Benefit Analysis into the NIST Cybersecurity Framework via the Gordon-Loeb Model. *Journal of Cybersecurity*, **6**, 1-8. https://doi.org/10.1093/cybsec/tyaa005

[10] Bush, G. (2003) The White House. National Strategy to Secure Cyber-Space. https://www.cisa.gov/sites/default/files/publications/cyberspace_strategy.pdf

[11] Obama, B. (2013) Executive Order 13636—Improving Critical Infrastructure Cybersecurity. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

[12] Trump, D. (2017) Executive Order 13800—Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. https://www.federalregister.gov/documents/2017/05/16/2017-10004/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure

[13] Biden, J. (2021) Statement by President Joe Biden on Cybersecurity Awareness Month. https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2021/10/01/statement-by-president-joe-biden-on-cybersecurity-awareness-month/

[14] Securities and Exchange Commission (2011) CF Disclosure Guidance: Topic No. 2. https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

[15] Audit Analytics (2016) Cybersecurity Disclosure in Risk Factors. https://blog.auditanalytics.com/cybersecurity-disclosures-in-risk-factors/

[16] Amir, E., Levi, S. and Livne, T. (2018) Do Firms Underreport Information on Cyber-Attacks? Evidence from Capital Markets. *Review of Accounting Studies*, **23**, 1177-1206. https://doi.org/10.1007/s11142-018-9452-4

[17] Securities and Exchange Commission (2018) Commission Statement and Guidance on Public Company Cybersecurity Disclosures. https://www.sec.gov/files/rules/interp/2018/33-10459.pdf

[18] Campbell, K., Gordon, L.A., Loeb, M.P. and Zhou, L. (2003) The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market. *Journal of Computer Security*, **11**, 431-448. https://doi.org/10.3233/jcs-2003-11308

[19] Hovav, A. and D'Arcy, J. (2003) The Impact of Denial-of-Service Attack Announcements on the Market Value of Firms. *Risk Management and Insurance Review*, **6**, 97-121. https://doi.org/10.1046/j.1098-1616.2003.026.x

[20] Kannan, K., Rees, J. and Sridhar, S. (2007) Market Reactions to Information Security Breach Announcements: An Empirical Analysis. *International Journal of Electronic Commerce*, **12**, 69-91. https://doi.org/10.2753/jec1086-4415120103

[21] Gordon, L.A., Loeb, M.P. and Zhou, L. (2011) The Impact of Information Security Breaches: Has There Been a Downward Shift in Costs? *Journal of Computer Security*, **19**, 33-56. https://doi.org/10.3233/jcs-2009-0398

[22] Hilary, G., Segal, B. and Zhang, M.H. (2016) Cyber-Risk Disclosure: Who Cares? Georgetown McDonough School of Business Research Paper. https://doi.org/10.2139/ssrn.2852519

[23] Spanos, G. and Angelis, L. (2016) The Impact of Information Security Events to the Stock Market: A Systematic Literature Review. *Computers & Security*, **58**, 216-229. https://doi.org/10.1016/j.cose.2015.12.006

[24] Richardson, V.J., Smith, R.E. and Watson, M.W. (2019) Much Ado about Nothing:

The (Lack of) Economic Impact of Data Privacy Breaches. *Journal of Information Systems*, **33**, 227-265. https://doi.org/10.2308/isys-52379

[25] Cohen, J., Krishnamoorthy, G. and Wright, A. (2017) Enterprise Risk Management and the Financial Reporting Process: The Experiences of Audit Committee Members, CFOs, and External Auditors. *Contemporary Accounting Research*, **34**, 1178-1209. https://doi.org/10.1111/1911-3846.12294

[26] Rosati, P., Gogolin, F. and Lynn, T. (2020) Cyber-Security Incidents and Audit Quality. *European Accounting Review*, **31**, 701-728. https://doi.org/10.1080/09638180.2020.1856162

Appendix. Examples of Discussion on Integration of CRM into ERM in Item 1Cs

2024-01-30 Alphabet Inc.

"ITEM 1C. CYBERSECURITY

We maintain a comprehensive process for identifying, assessing, and managing material risks from cybersecurity threats as part of our broader risk management system and processes. We obtain input, as appropriate, for our cybersecurity risk management program on the security industry and threat trends from multiple external experts and internal threat intelligence teams. Teams of dedicated privacy, safety, and security professionals oversee cybersecurity risk management and mitigation, incident prevention, detection, and remediation. Leadership for these teams are professionals with deep cybersecurity expertise across multiple industries, including our Vice President of Privacy, Safety, and Security Engineering. **Our executive leadership team, along with input from the above teams, are responsible for our overall enterprise risk management system and processes and regularly consider cybersecurity risks in the context of other material risks to the company**.

…"

2024-03-12 Franklin Financial Services Corop

"Item 1C. Cybersecurity

The Corporation has developed an information security program to assess, identify, and monitor cybersecurity risks. The Corporation regularly assesses cybersecurity risks arising from the operating environment and attempts to identify the likelihood and severity of the risk and the possible impact of the risk on the Corporation, its customers, and employees...**The Corporation's information security program is led by the Chief Technology Officer in conjunction with the Chief Risk Office and the Executive Enterprise Risk Management Committee. The Board Enterprise Risk Management Committee is responsible for oversight of the Corporation's cybersecurity and information security program and regularly reviews and evaluates information security and cybersecurity risks provided by management.**

…"