Across the Pond:
How U.S. Firms' Boards of Directors Adapted to the Passage of the GDPR*

April Klein†
Stern School of Business, New York University
Warwick Business School, University of Warwick
ECGI

Raffaele Manini
UPF Barcelona School of Management
Universitat Pompeu Fabra

Yanting (Crystal) Shi
Stern School of Business, New York University

*Accepted by Partha Mohanram. We are grateful to and thank Partha Mohanram (deputy editor-in-chief), two anonymous referees, Aleksander Aleszczyk, Jennifer Arlen, Massimiliano Bonacchi, Disen Huang, Baljit Sindhu, and the seminar participants at the Free University of Bolzano-Bozen, Corporate Governance Center at the Stern School of Business NYU, NYU Law School and the University of Sydney. We also thank the NYU Sustainability Center for providing us with the TruValue Labs Insight360™ database.
†Corresponding author. Stern School of Business, New York University, 44 West 4th Street, New York, NY 10012, Email: ak5@stern.nyu.edu, Ph: (212) 998-0014

Data availability statement: All data are publicly available from sources cited in the text.

Across the Pond:
How U.S. Firms' Boards of Directors Adapted to the Passage of the GDPR

Abstract

One of the prime responsibilities of the board of directors is to understand and oversee its firm's risk profile. We exploit a recent European Union (EU) regulation, the General Data Protection Regulation (GDPR), as a quasi-exogenous shock to the cyber risk landscape to assess whether boards of U.S. firms changed their focus and governance structures to deal with this new challenge. Although an EU regulation, the GDPR applies to all American public firms with at least one EU user. Adopting a difference-in-differences methodology, we use firms previously regulated by the HIPAA as a control group, and find that boards of treated U.S. firms, on average, increase their focus on cyber risk, add more directors with cyber/IT expertise, and more frequently assign cyber risk oversight to the board or to a board committee. In cross-sectional tests, we show that these changes are positively associated with a firm's *ex ante* cyber risk, but are unrelated to whether a firm had a large EU presence, suggesting a more global reaction to the GDPR. In addition, we examine some of the consequences of these board changes. We find boards that promptly responded by changing their board focus, expertise, and monitoring assignment of cyber risk around the passage of GDPR had fewer future cyber-attacks/data breaches and less related media attention. Our findings suggest that, on average, American corporate boards promptly responded to changes in the cyber risk environment.

Keywords: corporate governance, board of directors, cyber-risk, GDPR

“Data will eclipse both land and machinery as the most important asset in the 21st Century”
-Yuval Noah Harari in “21 Lessons for the 21st Century”

1. Introduction

One of the prime responsibilities of the board of directors is to understand and oversee its firm’s risk profile (SEC 2009a). However, firm risk is an everchanging construct, a landscape subject to “increasing volatility, complexity, and ambiguity of the world” (COSO 2017). In this paper, we examine whether boards of directors of U.S. firms increase their monitoring of cyber risk in response to a tangible change in the firm’s cyber risk environment.[1] We then examine the consequences of these responses, for example, correlating changes in the boards’ focus and expertise on cyber risk to subsequent changes in cyber-attacks and data breaches. To our knowledge, this is the first paper to conduct this type of inquiry, thus, providing an important first step in understanding how boards respond to changes in cyber risk.

We use a recent European Union (EU) regulation, the 2016 General Data Protection Regulation (GDPR), as an indicator for a quasi-exogenous change in the cyber risk environment that firms face. The GDPR encompasses a wide-sweeping set of regulations aimed at protecting EU citizens from unwanted uses of their personal internet data. It provides data privacy security for all EU citizens, despite where the internet site or the company is domiciled. Therefore, any U.S. company with a website used by any EU resident(s) is subject to the GDPR. For example, Proctor and Gamble’s (P&G) website includes a link allowing users to choose their location. If a user selects an EU country, e.g., Italy, then in adherence to the GDPR, a privacy link opens up with information about how P&G uses its customers’ private information, and provides the user with various options on how to change privacy preferences.

There are several advantages to our setting. Almost all U.S. firms face cyber risk, with the

[1] We use cyber risk to encompass risks related to cybersecurity, cyber-attacks, and data privacy.

amount of exposure varying across firms. Yet, the demand for cybersecurity and cyber privacy is unobservable to outsiders, making it difficult to correlate them with firm actions. Previous papers overcome this challenge by using data breaches (Liu 2020; Haislip et al. 2019) or cyber-attacks (Amir et al. 2018; Kamiya et al. 2018) as firm-specific shocks. However, data breaches and cyber-attacks are relatively rare events, and firm responses to them may not be representative of the entire economy.

In contrast, the GDPR is a plausible exogenous shock to the cyber risk landscape affecting almost all U.S. firms, but in varying degrees. These risks include compliance and regulatory risks involved in adopting and adhering to the mandates within the new regulation. For example, the GDPR requires firms to manage their customers' data, to provide clear and wide latitudes to customers to opt in or out of data collection, to provide timely notices of data breaches, and to maintain privacy by design protocols for the inclusion of data protection from the onset designing new systems. Regulatory risks include possible fines by any of the 28 EU countries for non-compliance, which can be up to four percent of the firm's global annual revenues. In addition, future regulatory changes could result from European Court decisions on cases involving the GDPR[2] or jurisdictions outside of the EU subsequently passing GDPR-like regulations.

The GDPR also changed the business environment for firms as they relate to data collection. Prior to the GDPR, the risks associated with firms collecting and using their customers' data were negligible, in that website users had little control over their data and, most likely, were unaware of how their data were being used by firms (for example sold to third-party vendors). With the

[2] For example, on July 16, 2020, the Court of Justice of the European Union ruled that the EU-US Data Protection Shield was invalidated due to concerns around surveillance by U.S. state and law enforcement agencies. Known as "Schrems II," this ruling significantly alters the way companies can transfer personal data from EU countries to the United States.

institution of the GDPR, users are given unprecedented control over how their data could be used, thus altering a firm's business model of how it can attract and maintain web users with different priorities. Aridor et al. (2021), using a proprietary dataset from an online travel intermediary, find that the opt-in/opt-out requirement of GDPR resulted in a 12.5% drop in intermediary-observed consumers. This drop in users resulted in a short-term dip in advertising revenues for the affected firms. However, they also find that the remaining consumers use the websites more frequently and for longer periods of time, thus mitigating the initial drop in advertising revenues.

By using the GDPR as our exogenous shock, we are able to conduct our analyses on a broad sample of over 2,000 companies. Using Form DEF14A proxy statement disclosures as our main source of information, we examine three board attributes: (1) whether the board pays more attention to cyber risk, cybersecurity and cyber privacy [focus], (2) whether the board significantly adds directors with cyber risk or information technology (IT) expertise [composition], and (3) whether the board increasingly assigns its cyber risk oversight to the board itself and/or one of its committees [monitoring assignment]**.** Our empirical results are consistent with boards significantly enhancing their oversight of cyber risk in the period around the passage of the GDPR. The percentage of boards discussing cyber risk in their proxy statements rises from 10.70% to 23.12% between the pre- and post-GDPR periods. The percentage of boards explicitly assigning cyber risk oversight to themselves and/or one of their committees increases from 8.93% to 17.30%, with audit committees seeing an almost three-fold jump in cyber risk monitoring. Boards significantly increase their inclusion of a director with cyber/IT knowledge; in the post-GDPR period, almost one quarter of all boards have at least one director with this expertise. Thus, we present evidence consistent with boards of directors, on average, enhancing their cyber risk monitoring in response to the new demands created by the GDPR.[3]

[3] We acknowledge that the GDPR is not solely responsible for all changes in the cyber risk environment over our

However, these new demands are not monolithic across firms. Accordingly, we examine cross-sectional variations to how boards reacted to the GDPR. Since the GDPR regulates EU residents only, we see if firms with higher business exposures to EU customers are more likely to make significant changes in their board oversight of cyber risk. Using three different measures of EU exposure, we find no evidence that a firm's relative dependence on EU residents influenced its board's immediate response to the GDPR. This non-containment is consistent with the GDPR's effect on cyber risk "leaping across the pond," impacting a broader group of U.S. firms. We also present evidence that differences in board responses across firms vary with their ex ante cyber risk exposure. Finally, using a difference-in-differences methodology, we show that boards of firms in an already cybersecurity regulated industry, healthcare, made fewer changes in response to the passage of the GDPR, when compared to firms in other industries.

We then examine some of the economic consequences associated with the changes in board monitoring and with the approval of the GDPR itself. If board responses are due to an enhanced cyber risk environment, then we would expect to see a subsequent reduction in cyber risk for firms whose boards make the largest adjustments. On the other hand, if these changes are merely cosmetic in nature, then we should see no tangible outcomes. Our paper presents evidence consistent with the first hypothesis. We document a reduction in the likelihood of a firm receiving a cyber-attack or data breach during the years 2017-2019 in accordance with the magnitude of the firm's board changes between 2014 and 2016. Cyber risk exposure, as measured by media coverage of the firm's data security falls in a similar fashion. We also document a sharp increase in a firm's discussion of GDPR within the 10-K Report over time, culminating with almost 25% of all firms in our sample including a discussion of it in the "Business" or "Risk Factors" sections

transition period. Other events, for example, prominent cyber-attacks and data breaches, most likely also changed this environment. We address some of these issues throughout the paper, including the influence that these attacks and breaches may have had on our findings.

in 2019.

Our findings support the view that boards responded quickly and effectively to an unexpected shift in the cyber risk landscape. Over the period surrounding the passage of the GDPR, boards substantively increased their focus, expertise and cyber risk assignment, with firms with higher ex ante cyber risk making the most changes. Further, firms with boards that responded more quickly experience fewer future cyber-attacks, data breaches and media attention to its data security.

Our study contributes to several lines of research. First, we delve into the relatively unexplored area of board adaptability and effectiveness as it relates to an exogenous change in a firm's risk environment. This inquiry complements previous studies examining how changes in board composition impact firm performance (e.g., Duchin et al. 2010; Adams et al. 2018; and Van Peteghem et al. 2018), accounting transparency (Armstrong et al. 2014), and financial reporting quality (e.g., Bryan, et al. 2013; Kim and Klein 2017). Our study differs from these papers in that we examine voluntary changes in board structure, instead of those mandated by a new law or regulation.

Second, our paper contributes to the overall literature on cyber risk. Previous papers examine how disclosures of cyber risk from the Form 10-K are priced by the stock market (Berkman et al. 2018; Gordon et al. 2010). Other studies examine firm or market responses to cyber-attacks and data breaches (Kamiya et al. 2018; Amir et al. 2018; Haislip et al. 2019; Liu 2020). We complement these studies by using the GDPR as a plausible exogenous shock to the firm's cyber risk environment. Thus, we are able to examine board responses to cyber risk shocks for a broad group of firms.

Third, we add to the literature on how a regulation promulgated in one jurisdiction can have consequences on other regions of the world. Many papers examine global effects of U.S. laws or regulations, for instance, PCAOB inspections (Oesch and Urban 2019) or the Sarbanes-Oxley Act of 2002 (Piotroski and Srinivasan 2008). Our paper looks at how a European regulation transfers to an American setting.

2. Institutional Background: The GDPR and Cyber Privacy Laws

On May 25, 2016, the EU adopted the GDPR. A two-year transition period was enacted, making the regulation effective from May 25, 2018 onwards.

The GDPR

The GDPR is structured towards ensuring EU citizens data privacy within the context of today's internet and big data environment. It replaces an earlier EU data protection rule, the 1995 EU Data Protection Directive 95/46/EC. Two criticisms of the 1995 Directive were that its scope of personal data was limited to identification, for example, a person's name, photo, email addresses, phone numbers and personal identification numbers (e.g., social security number, bank account number, credit card number) and, because it was a directive and not a regulation, EU member states could adopt their own rules, for example, different data breach notification laws.

Appendix 2 contains a detailed summary of some of the major provisions of the GDPR. The GDPR has extra-territorial jurisdiction, affecting all U.S. firms that have EU customers or users. Article 3 states that the collection of personal data or behavioral information from any EU resident falls under the purview of the GDPR. Thus, the GDPR has extra-territorial jurisdiction, affecting all U.S. firms that have EU customers or users.

The GDPR increases data privacy. It requires firms to draw up detailed "data-protection impact assessments," which explain how personal data are processed. Privacy-enhancing IT techniques discussed in the GDPR are pseudonymization (replacing personally identifiable information with artificial identifiers) and encryption (converting personal information into a secret code). Other provisions mandate companies to give clear and simple instructions to website users on how to provide and withdraw consent on allowing companies to use and share their private data; the ability to receive private data stored by the company; and the right to ask the company to erase their stored data.

The GDPR enhances cybersecurity. Article 24 calls for the inclusion of data protection protocols when designing systems, thus placing a burden on firms to upgrade their data security. Articles 33 and 34 require firms to notify users of data breaches within 72 hours of becoming aware of the breach. Thus, the GDPR ties data privacy to how a firm handles cybersecurity.

Article 83 provides stiff penalties for violations of its regulations, with monetary fines reaching up to four percent of total global revenues or €20 million (whichever is greater). According to CoreView, 39 companies received "major" fines from May 2018 through May 2020 totaling almost €500 million for violations of the GDPR.[4] In January 2019, for example, Alphabet (Google) was fined €50 million by the French data regulator CNIL for a breach of GDPR rules on "transparency and lack of consent."

The GDPR is the first mandated cyber privacy regulation to encompass all U.S. firms (albeit those with at least one EU user).[5] It is in stark contrast to the existing U.S. regime, which is a self-regulator market-based system known as "Notice and Choice." (Davis and Marotta-Wurgler 2019). This system is overseen by the Federal Trade Commission (FTC), and it contains a series of recommendations about data privacy contained in the FTC Fair Information Practice Principles. These guidelines are not binding, and many studies show that U.S. firms' information practices comply poorly with these principles (see Davis and Marotta-Wurgler 2019).

Pre-and Post- Periods Around the Passage of the GDPR

Following most regulation papers, we define our pre- and post- periods as those immediately

[4] https://www.coreview.com/blog/alpin-gdpr-fines-list/

[5] The one exception is Section 312.8 of the *Children's Online Privacy Protection Rule,* which requires companies to "establish and maintain reasonable procedures to protect the confidentiality, security and integrity" of personal information collected on or off the internet for children under the age of 13."

preceding and following the approval timeline of the regulation. We believe that the www.eugdpr.org, an external website devoted to the "education of the public about the main elements of the General Data Protection Regulation," provides the most appropriate record of dates. As Appendix 3 shows, the passage of an EU regulation encompasses three phases: proposal, trilogue, and approval. Our first date, [D1], is the approval of the GDPR proposal by the Council of the European Union on June 15, 2015. The trilogue is a series of private negotiations culminating in a final draft of the proposed regulation. The timeline ends on May 25, 2016 [D18], when the GDPR is adopted. In all, our time period spans just 346 calendar days. We define the pre-period as the year prior to June 15, 2015 [D1] and the post-period as the year following May 25, 2016 [D18].

3. Literature Review and Hypotheses

The board of directors performs an oversight role within the firm by monitoring and advising top management on the firm's overall performance and risk profiles (Fama and Jensen 1983; Harris and Raviv 2008). In theory, firms and boards use cost/benefit analyses to structure their boards to meet their needs (Hermalin and Weisbach 1998). Empirical evidence generally supports this view with respect to board size and independence (Coles et al. 2008) and committee structures (Klein 1998; Ittner and Keusch 2015). Boards also strategically include directors with specialized professional skills, for example attorneys and politicians (Agrawal and Knoeber 2001), bankers (Guner et al. 2008), industry knowledge (Cohen et al. 2014; Wang et al. 2015; Faleye et. Al. 2018), and financial accounting knowledge (DeFond et al. 2005).

As these papers illustrate, board composition and structure are endogenously determined. We exploit this endogeneity to address our research questions, which are whether boards adapt quickly to a shift in their cyber risk environment, and whether these board changes reduce future cyber risk. There are several reasons to believe this may be true. First, in general, boards assume the responsibility of monitoring overall firm risk. This oversight is codified by the SEC (SEC 2009a), but also advocated by the Committee of the Sponsoring Organization of the Treadway Commission (COSO 2004, 2019), the National Association of Corporate Directors (NACD) (2014, updated in 2017 and 2020), Big-4 accounting (Deloitte 2018) and corporate law firms (Gregory 2015/2016).

Whereas many papers examine the association between firm performance (e.g., Tobin's Q) and board characteristics, a modest literature exists on the relation between board attributes and firm risk. Bernile et al. (2018) find that greater overall board diversity leads to lower stock return volatility, thus presenting a connection between board composition and managing firm risk. Ormazabal (2010) and Ittner and Keusch (2015) seek to understand the association between board structure and risk oversight. Ormazabal (2010) creates a five-dimensional "observable" risk oversight index, in which the inclusion of a risk oversight board committee is one of the factors. He finds a negative association between his index and credit risk and equity risk. Ittner and Keusch (2015) find no direct association between how the board assigns its risk oversight function, e.g., to the board as a whole and/or to one of its committees, and equity risk; although they do report a positive association between overall board oversight and the sophistication of the firm's overall risk management. Dionne and Triki (2005) and Dionne et al. (2019) examine director characteristics and specific corporate risk-mitigating actions, for example, hedging activities. They find that director financial literacy correlates positively to a more effective hedging policy.

Second, the scope of firm risk has evolved over time, with firms increasingly managing a more comprehensive "enterprise risk" (Ormazabal 2010). Enterprise risk encompasses uncertainties beyond the traditional financial and operating risks. Its concept was introduced by COSO in 2004, who wrote that:[6]

> "Enterprise risk management is a process, effected by an *entity's board of directors*, [our italics] 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

[6] COSO is a private sector initiative sponsored and funded by the American Accounting Association, the American Institute of Certified Public Accountants, the Financial Executives International, the Institute of Management Accountants, and the Institute of Internal Affairs.

> to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives" (COSO 2004).

In 2017 and 2019, COSO updated its original document by including ESG and cyber risk as two distinct risks to be monitored by the firm's board.

Third, several papers show that firms respond to an increase in idiosyncratic risk by changing their board structures. These risks include poor operating performance (Kaplan and Reischus 1990), bankruptcy (Gilson 1990), option backdating (Ertimur et al. 2011) and financial fraud (Srinivasan 2005; Fich and Shivdasani 2007). These papers suggest that boards may adapt to their new cyber risk environment by instituting changes in their focus, composition, and monitoring assignment of cyber risk.

However, an extensive literature is consistent with an opposite view — boards may not adapt effectively or quickly to the GDPR. In the management arena, Boivie et al. (2017) claim that boards inherently are ineffective monitors of top management. Many papers conclude that boards are entrenched, thus requiring new regulations to push them out of complacency (e.g., Duchin et al. 2010; Armstrong et al. 2014; Bryan et al. 2013). Further, firms often skirt new corporate governance regulations by not having the required number or percentage of (truly) independent directors after the transition date (e.g., Duchin et al. 2010; Kim and Klein 2017). Since the GDPR is silent on board composition or board structure, it is very possible that boards will not change their cyber risk oversight after its passage. Moreover, there is mixed evidence on whether adding expertise actually improves board monitoring. Kim and Starks (2016) present evidence that board heterogeneity in directors' underlying skillsets improves firm performance, but Adams et al. (2018) come to an opposite conclusion. Thus, firms may choose to not add a director with cyber/IT expertise to the board following the passage of the GDPR.

We therefore state our first hypothesis in the null form.

HYPOTHESIS 1. *Boards of directors, on average, do not change their monitoring of cyber risk after the approval of the GDPR.*

Our second hypothesis relates to the GDPR being an EU regulation that encompasses EU consumers only. Therefore, it is not clear whether U.S. firms without a significant EU presence will make changes to their boards in response to this regulation. Frankenreiter (2021) and Davis and Marotta-Wurgler (2019) examine the extent to which U.S. websites changed their U.S. privacy policies in response to the GDPR's new requirements. They report dissimilar results, with Frankenreiter (2021) reporting no major modifications, but Davis and Marotta-Wurgler (2019) finding more substantive changes. The difference in results can be attributed mainly to their sample selection criteria. Frankenreiter (2021) uses a broader sample of firms, whereas Davis and Marotta-Wurgler (2019) target a smaller sample of websites with obvious consumer privacy concerns, for example, dating apps.

We present our second hypothesis in the null form:

HYPOTHESIS 2. *Boards of directors of firms with large exposures to the EU, on average, are equally likely to change their oversight of cyber risk after the approval of the GDPR as firms without large EU exposures*.

Our third hypothesis relates to ex ante cyber risk. If the GDPR is a shock to a firm's cyber risk environment, then firms with higher ex ante cyber risk may be more affected by its risk implications. This would suggest they would be more likely to make changes in their boards' focus and composition to deal more effectively with the expected changes. However, firms with high ex ante cyber risk may already be focused on cyber risk issues, that is, cybersecurity, data breaches, or data privacy. Thus, we would not expect to see substantive changes in cyber risk oversight for these firms.

The above discussion suggests we state our third hypothesis in the null form:

HYPOTHESIS 3. *Boards of directors of firms with greater ex ante cyber risk exposure, on average, are equally likely to change their oversight of cyber risk after the approval of the GDPR as firms with lesser ex ante cyber risk exposure.*

4. Sample Selection, Data Sources and Description of Data

Sample Selection

Table 1 panel A provides a description of our sample selection. Using the Compustat/CRSP merged database, we begin with 5,595 firms with a fiscal year ending in 2014. We eliminate 923 non-U.S. firms and 1,056 firms with missing control variables in our pre-period. These control variables are from Compustat, Audit Analytics, and BoardEx. We remove 998 and 509 firms with missing Forms DEF14A (proxy statements) over the pre- and post- time periods, respectively, with the pre-period being the last proxy statement prior to June 15, 2015 [D1] and the post-period being the first proxy statement after May 25, 2016 [D18]. We remove 16 firms that were cyber-attacked between 2005 and 2014; Kamiya et al. (2018) document an increase in board risk management for victims of cyber-attacks in the two-year period following the attack. The data for identifying these attacks are from the Privacy Rights Clearinghouse's (PRC) database, which collects information from required disclosures of data breaches from various sources including the State Security Breach Notification Laws, the SEC Cybersecurity Disclosure Guidance for Form 8-K disclosures, and the Health Insurance Portability and Accountability Act (HIPAA). Our final sample consists of 2,093 firms, which we use in our cross-sectional regression analyses.

Table 1 panel B contains summary statistics for our sample. Consistent with other papers using BoardEx data, there is a wide range of firm and board characteristics. For example, although the mean *Total Assets* is $8.7 billion, firm assets range from $3.76 million to $856.2 billion. Similarly, only 71% of firms use a *Big Four* auditor, a percentage substantively lower than for firms in the S&P 500 alone. In terms of board structure, the average board size is 8.66 directors and each board, on average, is comprised of 78% independent directors.

Board Risk Oversight and Directors with Cyber/IT Expertise

We use disclosures on risk oversight and director skills from the firm's DEF14A (proxy statement) to create measures of board oversight and director skills related to cyber risk. In December 2009, the SEC adopted a new regulation, effective from February 2010 onward, mandating firms to provide more detailed information in their annual Form DEF14A about the risk oversight function of their boards (SEC 2009a). In describing these rules, the SEC noted they "were persuaded by commenters who noted that risk oversight is a key competence of the board, and that additional disclosures would improve investor and shareholder understanding of the role of the board in the organization's risk management practice" (SEC 2009b).

The regulation requires the proxy statement to discuss the board's role in "managing the material risks facing the company" (our underline). It also asks firms to describe how its board monitors risk, providing the company "the flexibility to describe how the board administers its risk oversight function, such as through the whole board, or through a separate risk committee, or the audit committee" (SEC 2009b, 44). Many firms responded to the new regulation by providing a detailed list of the material risks they face, as well disclosing how the board oversees the management of each risk. For example, from Amazon's 2013 Proxy Statement:

> "***Risk Oversight***. As part of regular Board and committee meetings, the directors oversee executives' management of risks relevant to the Company. While the full Board has overall responsibility for risk oversight, the Board has delegated responsibility related to certain risks to the Audit Committee and the Leadership Development and Compensation Committee. The Audit Committee is responsible for overseeing management of risks related to our financial statements and financial reporting process, ***data privacy and security***, business continuity, and operational risks, the qualifications, independence, and performance of our independent auditors, the performance of our internal audit function, and our compliance with legal and regulatory requirements" (our bolded italic).

The new rule also mandates firms to describe in more detail a director's expertise. The new items to be disclosed include the "particular experience, qualifications, attributes or skills that led the board to conclude that the person should serve as director for the company as of the time that a filing containing this disclosure is made with the Commission" (SEC 2009b, 34).

To create our variables, we do a combination of textual analysis followed by hand-collection. As Kim and Starks (2016) note, the flexibility incorporated within the regulation makes the tool of technical analysis inexact due to the difficulty of finding a clear textual pattern within any section of the Form DEF14A. Specifically, we go over the paragraphs in the Form DEF14A that include the keywords "cyber," "information technology," or "data privacy." If they do not represent the meaning we intend to capture, we drop the observation. For instance, several "data privacy" keywords are related to companies' stock grants instead of protecting consumer data. For those sentences referencing a specific director, we download the respective Form DEF14A and manually read the original paragraph in the filing to collect the name of the director that possesses cyber, information technology, or data privacy skills. We then search for this director in the proxy statement to obtain committees assignments.[7]

We create three types of variables: Cybersecurity awareness, director expertise in IT/Cyber, and board/committee monitoring of cyber risk. In terms of cybersecurity awareness, *CyberAwarenessDEF14A* is an indicator if the proxy statement contains the keyword "cyber" at least once and *CyberCountDEF14A* counts the number of times the keyword "cyber" is mentioned throughout the proxy statement. As Table 2 panel A shows, prior to the initiation of the GDPR proposal period, 10.70% of firms in our sample mentioned "cyber" at least once in their proxy statements, with an average of 0.18 mentions throughout the full sample.

In terms of how the board allocates its oversight of cybersecurity and data privacy, we create variables based on the firm's discussion in the Form DEF14A. *MonBoDOnly* is an indicator if the monitoring duties are given to the board as a whole; *MonAudComm*, *MonRiskComm*, and

[7] For those sentences addressing risk oversights, we read the proxy statements to understand the board or committee delegations regarding cyber risk. For instance, some boards require directors' training regarding cybersecurity, but they do not explicitly delegate the cyber risk monitoring roles; in these cases, we exclude them from risk monitoring.

MonTechComm are indicators if the monitoring explicitly is given to the audit committee, risk committee, or technology committee, respectively. In panel A, we find that 8.93% of the proxy statements in the pre-period explicitly assign cyber risk or data privacy oversight to the board and/or one of its committees (*MonBoD/Comm*). More granularly, the percentage of cyber risk or data privacy monitoring primarily done by the board itself is 2.48%, by the audit committee 3.39%, by the risk committee 1.48%, by the technology committee 1.15%, and 0.67% by other committees. The designation of the audit committee as the overseer of cyber risk is consistent with the NYSE's requirement that the audit committee is responsible for "discussing policies with respect to risk assessment and risk management" (NYSE Listed Company Manual Section 303A.07(b)(iii)(C); see also Lanz 2014).

In terms of director expertise, we look at each director's biography and list of qualifications in the Form DEF14A and label that director a cyber or IT expert if we find a background in information technology, cyber, or data privacy. Our designation is consistent with Adams et al. (2018) and Kim and Starks (2016). As panel A shows, the percentage of boards with at least one expert in the pre-GDPR period is 17.34%, with 11.32% of audit committees having at least one cyber/IT expert.

5. Board Monitoring of Cyber Risk Before and After the Approval of GDPR

Hypothesis 1 examines if boards change their oversight of cyber risk in response to the passage of the GDPR.

First Differences

We begin by examining the unconditional changes in our output variables. As Table 2 panel A shows, the form DEF14A filings show a sharp increase in board focus on cyber risk between the pre- and post-GDPR periods. The percentage of firms mentioning "cyber" (*CyberAwenessDEF14A)* increases from 10.70% to 23.12%, and the average number of mentions

(*CyberCountDEF14A*) grows from 0.18 times to 0.53 times. A t-test for the difference in percentages yields p-values less than 0.01.

In terms of director expertise, the percentage of boards with at least one cyber expert (*ExpBoD*) increases from 17.34% to 23.36%, with all three committees taking on new cyber experts. T-tests for differences in percentages are significant at the 0.01 levels for change in the experts on the board and the audit committee, and at the 0.10 level for changes on the risk and technology committees.

The Risk Oversight section of the proxy statement reveals a large increase in boards being given a cyber risk oversight function. The percentage of firms assigning cyber risk oversight to the board and/or a board committee (*MonBoD/Comm*) almost doubles from 8.93% to 17.30%, with the three main board committees, audit, risk and technology, showing large increases in cyber oversight. T-tests for differences between pre- and post-period means are all significant at the 0.01 levels.

To control for other variables that might be related to our output variables, we estimate the following regression:

$$BdAttribute_{jt} = \beta_0 + \beta_1 Post + \Sigma\, Control_{jt} + \mathrm{FEIND} + \varepsilon_{jt}, \qquad (1)$$

where $BdAttribute_{jt}$ is the board attribute for firm j at time t, and *Post* is a dummy variable equal to one in the post-period and 0 in the pre-period. The regression controls for various factors previously found to be correlated with cyber risk or data breaches — firm size, internal control weaknesses, institutional ownership, being audited by a Big Four firm, and whether the firm pays cash dividends (Hilary et. al. 2016; Kamiya et al. 2018; Liu 2020). We also include other board attributes, specifically, board size and board independence. *FEIND* are industry fixed effects for the 12 Fama-French industries (Fama and French 2014) to control for the possibility that a change in board attribute for firm j is due to overall changes in its industry. All regression models use robust standard errors for the estimation of coefficients to alleviate concerns of normality and homogeneity of the variances of the residuals. See Appendix 1 for all variable definitions.

Table 2 panel B presents summary statistics from these regressions. After controlling for other factors, we find significantly positive coefficients on *Post* for regressions on the levels in cyber focus (columns 1 and 2), cyber/IT experts on the board (column 3) and assigning cyber risk oversight to the board and/or one of board committees (columns 7-10). Thus, we show evidence consistent with boards unconditionally focusing more effort and director expertise towards monitoring cyber risk after the approval of the GDPR. With respect to our control variables, these changes are positively related to firm size and the percentage of independent directors, and to the amount of institutional ownership and leverage in some but not all specifications. Similarly, the changes are negatively related in some specifications to cash paid in dividends and whether the firm uses a Big Four accounting firm.

Difference-in-Differences Regressions: Treatment and Control Groups

The unconditional change in board attributes shows that, after the passage of the GDPR, boards increased their focus and monitoring of cyber risk, and also changed their composition by adding directors with cyber expertise. However, these changes might be related to other factors or trends related to cyber risk and not to the passage of the GDPR. One way of examining this alternative explanation is to perform a difference-in-differences regression, thus comparing the group of firms that are treated by the new regulation (Treatment group) to those firms that are relatively unaffected by the new regulation (Control group).

We therefore seek a control sample of firms that already had been under a data privacy cyber risk regulatory regime prior to the approval of the GDPR. Since these firms were regulated in the pre-GDPR period, their pre-period boards should be more aligned with monitoring cyber risks.

Thus, we would expect to see fewer changes in board oversight for these firms. One such group of firms is U.S. healthcare companies, which, since 1996, are covered under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA is a health insurance privacy act, and it protects the privacy and security of electronic health records. All health insurance companies and health care providers are required to follow the laws within the Act. Our treatment group, by default, consists of firms in all other industries.[8]

We employ the following regression:

$$BdAttribute_{jt} = \beta_0 + \beta_1 Treated_j + \beta_2 Post + \beta_1 (Treated_j \; X \; Post) + \Sigma \; Control_{jt} + \varepsilon_{jt}, \qquad (2)$$

where *Treated* is equal to one for all firms not in the healthcare sector and to zero for all firms in the healthcare sector (Fama-French Code = 12). The other variables are defined as before. Equation (2) does not contain industry fixed effects since our treatment and control samples are divided by industry.

Figure 1 presents parallel trend analyses from 2012 through 2017. We collect data from the proxy statements for the pre-period years of 2012-2015, and on the first post-period year, 2017. Parallel trends assume that any divergence in the output variable in the post-period is not attributable to a divergence beginning in the pre-period. Figures 1 panel A and 1 panel B present

[8] Some financial companies already were regulated with respect to consumer privacy rights before the GDPR. The Fair Credit Reporting Act (FCRA) mandates credit rating companies to offer consumers the rights to ask for a credit score, to dispute incomplete or inaccurate information, and to give consent before reports are provided to a third party. The Gramm-Leach-Bliley Act (GLBA) requires financial companies to explain their information-sharing practices to their customers when offering consumer financial products. On March 1, 2017, the New York Department of Financial Service (NYDFS) adopted Cybersecurity Regulation, suggesting that the previous regulations on the finance companies were insufficient. In contrast, subsequent state-level data privacy regulations usually exempt the healthcare industry (e.g., California Consumer Privacy Act (CCPA) 1798.145.(4)(c)(1)), suggesting that the HIPAA regulation was sufficient or comparable to these regulations. In a robustness test, we replicate Table 3 but exclude all finance companies, and find all results hold, suggesting that the observed board changes are not driven by the financial companies making changes anticipating the Cybersecurity Regulation by NYDFS.

the percentage of firms with the term "cyber" in their proxy statements and the mean number of times "cyber" appears, respectively. As the figures show, from 2012-2015, the trends of the non-healthcare (treatment) and healthcare (control) firms track very closely to each other. However, in 2017, we see large divergences, with the treatment group showing greater growth than the control group. Figure 1 panel C shows the percentage of boards with at least one director with cyber/IT expertise. The pre-period trends are similar for the non-healthcare and healthcare firms; both groups exhibit a rise in cyber expertise on the board in 2017, although we see no obvious divergence in growth rates between groups. Figure 1 panel D presents the percentage of proxy statements assigning cyber risk monitoring to the corporate board and/or a board committee. Similar pre-period trends are found for the treatment and control firms. In 2017, we observe an increase in risk assignment for both groups, with the non-healthcare industry firms showing a greater rise than the healthcare industry firms. Thus, for the four output variables shown in Figure 1, the assumption of pre-period parallel trends holds.

Table 3 contains summary statistics for regression (2). We focus on the coefficients for the interactive term, *Treated X Post*. A significantly positive coefficient is consistent with a greater increase in the board attribute for the non-healthcare vis-à-vis the healthcare firms after the passage of the GDPR. As columns (1) and (2) show, the change in the use of the term "cyber" between the pre- and post-periods is greater for non-healthcare firms. Thus, firms in industries not already regulated with respect to data privacy experience a sharper increase in their awareness of cyber risk than firms already under regulation. In addition, as columns (7), (8), and (10) show, the explicit assignment of cyber risk to the overall board or to the risk committee grows at a greater pace for the non-healthcare firms than for the healthcare firms in the post-period. In contrast, we see no evidence of a differential in the growth rates of placing a cyber/IT expert on the board or on one of its cyber risk monitoring committees for firms in the healthcare or non-healthcare fields (columns 3-6). Thus, the increase in director cyber expertise that we found in Table 2 is similar across both groups of firms. The significantly positive coefficient on *Post* for the regression on Δ*ExpBoD* is consistent with this observation.[9]

In summary, the difference-in-differences results are consistent with boards of firms in non-regulated industries adapting quickly to changes in cyber risk. In the year immediately following the passage of the GDPR (but prior to actual implementation), boards in non-regulated industries significantly changed their focus and board/committee assignments in ways consistent with them increasing their oversight of the increase in cyber risk.

6. Cross-sectional Variations in Board Responses to the GDPR

In this section, we examine two cross-sectional variations in board responses to GDPR passage. First, we discern whether greater business exposure to the EU correlates with board changes. Since the GDPR directly affects EU customers and users only, it is possible that changes in cyber risk board oversight cluster within these firms. Second, we introduce a more global perspective on the effect that the GDPR has on board responsiveness. Specifically, we examine if the firm's cyber risk exposure in the pre-period has an effect on the board's responsiveness to its passage.

EU Exposure

Hypothesis 2 proposes that boards of directors of U.S. firms with larger or smaller EU presences are equally likely, on average, to change their cyber risk oversight after the passage of

[9] As a robustness check to the timing of our analyses, we estimate similar difference-in-differences regressions around the year 2013, with the pre-period encompassing the year 2012 and the post-period being the year 2014. In 2013, there were several major, publicized hacked data breaches against U.S. companies, including Adobe, Dun & Bradstreet, Living Social, Snapchat, Tumblr, and Yahoo. If U.S. companies reacted to these data breaches by instituting changes in the board focus or composition, then we should begin to see our treated firms changing their boards beginning in 2014, a full year before the pre-period we use in this study. Results (untabulated) show this is not true. None of the coefficients on the variable Treated*Post on the same 11 regressions as shown in Table 3 are significantly different from zero at the 0.10 level, with the exception of the regression on *MonRiskComm*, which has a coefficient of 0.02, significant at the 0.10 level (t = 1.81).

the GDPR. To test this hypothesis, we employ a first difference methodology similar to Duchin et al. (2010). Specifically, we estimate the following regression:

$$\Delta BdAttribute_j = \beta_0 + \beta_1 EU_j + \Sigma\ Control_j + \text{FEIND} + \varepsilon_j, \tag{3}$$

where EU_j is a proxy variable for the firm j's pre-period EU exposure. All control variables are measured in the pre-GDPR period. Equation (3) also includes cyber-related board attributes, for example, whether the firm had a cyber or IT expert on the board before the proposal stage.

We measure a firm's EU exposure in three different ways. *Dummy EU Segment* is an indicator if, following FASB Statement 131 and ASC 280, the firm reports at least one customer segment located in one of the 28 EU countries. *%Rev EU Segment* is the percent of total revenues derived from the EU, and *EU Rev Growth* is the EU segment's revenue growth. All data are from Computstat's Segment Report Database. Table 4 panel A contains summary statistics on the three measures. Twenty-five percent of firms have an EU segment; the EU segment, on average, encompasses five percent of total revenues; and the average pre-period growth rate in EU revenues is five. percent. As per GAAP rules, the correlation between a firm reporting a segment and the percent of revenues provided by that segment to overall revenues is very high, 0.7647 (panel B).

Table 5 has the summary statistics for equation (3). None of the coefficients on *EU* are significantly different than zero, with the exception of Δ*MonBoD* in panel B*,* which is significantly positive at the 0.10 level. Thus, our results do not support the view that our documented changes in board focus and composition are driven by the firm having an EU presence. It appears, instead, that the GDPR's effect on the cyber risk environment encompasses a larger, more diverse group of U.S. firms.

Cyber Risk Exposure

Hypothesis 3 examines whether a firm's pre-period cyber risk exposure is associated, on average, with board changes. To test this hypothesis, we estimate:

$$\Delta BdAttribute_j = \beta_0 + \beta_1 RiskExposure_j + \Sigma\ Control_j\ + \text{FEIND} + \varepsilon_j, \tag{4}$$

where *RiskExposure*$_j$ is a proxy variable for the firm j's pre-period cyber risk exposure. The control variables are the same as for equation (3). All independent variables are measured over the pre-period.

We create four proxy variables for cyber risk exposure. The first two variables are derived from the firm's 2014 10-K report. In 2011, the SEC issued *CF Disclosure Guidance: Topic No. 2 Cybersecurity* (SEC 2011), which states that firms facing "material cyber-related issues" should disclose these issues in their MD&A and in Item 1A, *Risk Factors* in their Form 10-K filings. Berkman et al. (2018) use textual analysis on these disclosures to create cybersecurity awareness scores for a sample of Russell 3000 firms over the period 2012-2016. They present evidence that the market positively values this awareness. We create two variables: *CyberAwareness10K* and *CyberCount10K*. *CyberAwareness10K* takes on a value of one if the 10-K has the keyword "cyber", and zero otherwise. It is similar in spirit to Gordon, Loeb and Sohail (2010), who use the presence or absence of an information security disclosure in the 10-K Report over the 2000-2002 period as their measure of cyber awareness. *CyberCount10K* is the number of times the keyword "cyber" appears in the 10-K Report. Because Berkman et al. (2018) incorporate disclosure length into their scores, *CyberCount10K* is similar to their measure.

MediaCov is an indicator if, during 2014, there is at least one media article (including social media, e.g., Twitter) referencing the firm's "Data Security." These articles are from TruValue Labs Insight360™, a proprietary dataset developed by TruValue Labs, Inc. They use natural language processing and machine learning techniques to glean information from an array of third-party information sources, including traditional and social media. Thus, *MediaCov* encompasses cybersecurity and data privacy characteristics of the firm.

Our last proxy is *CAR,* the Fama-French five-factor cumulative abnormal return (Fama and French 2014) for each firm over the 18 events surrounding the passage of the GDPR (See Appendix 3). CARs rely on the efficient market theory, which assumes that stock market participants aggregate and transmit information about the GDPR into market prices. Since we examine risk, we interpret a firm's CAR as partially reflecting the market's assessment of how the GDPR changes the cyber risk profile of the firm. Thus, a drop in stock price surrounding the passage of the GDPR, i.e., a negative stock price reaction, is consistent with the market seeing the GDPR as increasing the company's risk. We hypothesize that changes in board cyber risk oversight are negatively related to a firm's CAR.[10]

As Table 4 panel A shows, 42% of firms in the pre-period had a 10-K disclosure relating to cyber risk, with an average of 1.48 disclosures per firm. Nineteen percent of firms had media coverage relating to cybersecurity or data privacy. The average CAR over the passage period was 0.45%, although the median firm had a CAR of -0.05%. Our four cyber risk exposure variables capture different measures of risk, as evidenced by their correlation coefficients being within the -0.01 and .020 ranges (untabulated).

Table 6 contains summary statistics on equation (4). The implications across the four panels are fairly consistent. *Ex ante* cyber risk is positively related to Δ*CyberAwarenessDEF14A* and Δ*CyberCountDEF14A* throughout the table, consistent with boards increasing their focus on cyber risk after the approval of GDPR for firms with higher pre-period cyber risk. To check whether this finding is a reflection of a mechanical relation between firms disclosing similar information about

[10] Relating the CAR to changes in board behavior is consistent with theoretical papers proposing that managers (the board) learn from information embedded in stock prices when making corporate decisions (Dow and Gorton 1997; Dye and Sridhar 2002). Chen et. al. (2006) and Edmans et al. (2017) present empirical evidence consistent with this hypothesis.

cyber risk in the 10-Ks and proxy statements, we calculate the correlations between the proxy and 10-K items. As Table 4 panel C shows, the correlations between the source of the cyber risk disclosures range from 0.17 to 0.34, thus rejecting the view that we have a mechanical association. In addition, we control for the pre-period level of board cyber awareness, cyber/IT expertise, and monitoring in the regression analyses. Inclusion of these variables help alleviate concerns of high correlations between the cyber awareness in 10-K and DEF14A influencing our results.

Looking further at Table 6 (columns 3-6), we find evidence that boards more likely add a director with cyber/IT expertise (panels A, B, and D), or to the risk (panel A) or audit committees (panel D) for firms with greater ex ante cyber risk. Further, consistent with Ormazabal (2010), who shows that boards monitor risk both as a whole and through committees, we find that firms with higher ex ante cyber risk are more likely to increase the assignment of overseeing cyber risk to the board and/or to the audit or risk committee (columns 7-10). We conclude that, cross-sectionally, firms facing higher cyber risk exposures prior to the proposal stage of the GDPR are more likely to change their boards' focus, composition, and monitoring assignment towards monitoring cyber risk after the passage of the GDPR.

7. Consequences of GDPR and Changes in Board Focus, Composition and Monitoring

Our main results are consistent with boards increasing their cyber risk monitoring. In this section, we examine whether these changes are associated with future reductions in the firm's cyber risk. Specifically, we look at future cyber-attacks and data breaches, as well as data security media coverage. We also examine overall future consequences of the GDPR, that is, the extent to which firms include information about the GDPR in their Forms 10-K, and whether other jurisdictions subsequently adopt GDPR-like laws and regulations.

Future Effect of Board Changes: Reduction in Cyber-attacks and Cyber Breaches

We test for a negative association between changes in our 11 board monitoring variables and the future incidence of a cyber-attack or data breach. Following other papers examining cyber-attacks/data breaches (e.g., Kamiya et al. 2018; Liu 2020), we use the Privacy Rights Clearinghouse database to identify firms with breach incidents. It is a database that collects voluntary disclosures of cyber-attacks and data breaches for firms and public entities. We collect this data for our sample of firms over the 2017-2019 period. If any firm-year contains an attack or breach, then *Incidence* equals one, otherwise it is equal to zero. We sequentially estimate a probit and a logit model, in which *Incidence* is the dependent variable and the main independent variable of interest is one of the 11 board change variables (focus, composition or monitoring assignment) over the GDPR passage period (2014-2016). We control for *Size*, *Big Four*, *InstOwn*, *ICW*, *Leverage*, *BoardSize*, *%IndDir*, and *PaidCashDiv* at the end of 2016, as well as the number of cyber-attacks and data breaches during 2015 and 2016.

Table 7 panel A contains summary statistics for the nine regressions that we are able to estimate.[11] As the panel illustrates, the incidence of a firm disclosing a cyber-attack or data breach over 2017-2019 is negatively related to seven of the nine board change variables. Specifically, *Incidence* is negatively associated with changes in board focus *(*Δ*CyberAwarenessDEF14A* and Δ*CyberCountDEF14A*), cyber expertise *(*Δ*ExpBoD*, and Δ*ExpTechComm*) and monitoring assignment *(*Δ*MonBoD*, Δ*MonBoDOnly*, Δ*MonRiskComm*, and Δ*MonTechComm*). These findings are robust to both the Probit and Logit model specifications. Thus, we document a negative association between board changes during the passage of the GDPR and future cyber-attacks or data breaches.

[11] We are unable to estimate the models with Δ*ExpAudComm* and Δ*ExpRiskComm* due to a lack of substantive variation in both the dependent *(Incidence*) and each of these two independent variables. As Table 2 Panel A shows, the number of audit and risk committees that experienced increases in cyber/IT experts were few, and, consistent with other papers, the number of cyber-attack/data breaches during this time period are relatively scarce. Thus, the intersection between those firms with an increase in cyber expertise and cyber-attacks/data breaches was zero for both groups.

Future Effect of Board Changes: Reduction in Subsequent Media Attention on Data Security

As before we use media attention of a firm's data security, as collected by TruValue Labs, as a measure of the firm's cyber risk exposure. Recall that TruValue Labs collects media articles from traditional and online (e.g., Twitter) sources. Thus, their coverage encompasses cybersecurity and data privacy characteristics of the firm.

Table 7 panel B presents summary statistics for Poisson regressions of *Media Attention* on changes in boards' cyber focus, expertise, and monitoring assignment. *Media Attention* is the number of media stories over the years 2017 through 2019. We estimate *Media Attention* using a Poisson distribution due to the random arrival of these events. Our control variables are the same as those used in panel A, except that we control for media attention in the years 2012-2014 instead of pre-period cyber-attacks. Similar to the last section, we expect improvements in board monitoring to be associated with a reduction in future cyber risk; thus, using cross-sectional regressions, we predict negative coefficients on each of the 11 board change variables.

Overall, the empirical results in panel B are consistent with our prediction. The coefficients on Δ*ExpRiskComm* and Δ*ExpTechComm* are significantly negative at the 0.01 levels, indicating a negative association between the board adding an IT/cyber expert to either its risk or technology committee and the number of media articles about data security. In terms of board monitoring, the coefficients on Δ*MonRiskComm* and Δ*MonTechComm* are significantly negative at the 0.01 levels, suggesting a negative association between increased monitoring of cyber risk on the risk and technology committees and future levels of *Media Attention*. We note, however, a significantly positive coefficient on Δ*MonBoD,* and no associations between the changes in cyber awareness variables and future media coverage of data security. Despite these disparate findings, we interpret our regression results as being supportive of the view that cyber-related board changes surrounding the passage of the GDPR are associated with a reduction in a firm's future cyber risk.

Future Effect of Passage of the GDPR: GDPR in the Firm's 10-K Filing

Item 101 of Regulation S-K requires the disclosure of material information pertaining to the registrant's business, and Item 105 provides for the discussion of material factors that make an investment in the registrant speculative or risky. Thus, if the advent, initiation, or application of the GDPR affects (or may affect) the firm's business or riskiness in a material way, then one or both of these sections in the Form 10-K will contain disclosures about the GDPR. We examine each firm's Form 10-K and, using textual analysis, we see if the acronym "GDPR" or the phrase "General Data Protection Regulation" appear in the firm's document. Figure 2 illustrates the timeline of these disclosures. As the figure shows, for our sample, the mention of GDPR in the Form 10-K ramps up from 1.5% in 2016 and 4.3% in 2017 (the transition stage) to 17.3% in 2018 and 24.5% in 2019 (the effective stage). Thus, by 2019, close to one-quarter of all firms in our sample consider the GDPR to have a material effect on their business environment.

Future Effect of Passage of the GDPR: Brussels Effect

Bradford (2012) presents evidence that the EU acts as a first mover in instituting new laws and regulations that protect its citizens. She calls this the "Brussels Effect," a moniker derived from Brussels being the seat of the EU. As of July 2021, 48 non-EU countries or jurisdictions (e.g., Hong Kong) have adopted (34) or are considering (14) laws or regulations similar to those contained in the GDPR by year. Notably, although the United States is not within the list of countries adopting GDPR-type laws, 15 U.S. states have approved (12) or are discussing (3) similar laws as of July 2021. The proliferation of this data privacy movement is consistent with the GDPR spawning a future enhancement of the cyber risk environment on a global basis.

Summary

In summary, we present evidence of a reduction in a firm's cyber risk emanating from changes in board cyber risk monitoring around the enactment of the GDPR. Specifically, we document a negative link between board monitoring and the firm's subsequent cyber risk, as evidenced by a reduction in the incidence of cyber-attacks or breaches, and media coverage of data security. We also show that U.S. firms responded to the passage of the GDPR by increasingly including discussions in the Form 10-K of its impact on the risk and business environment of the firm.

8. Robustness Checks

We perform some robustness checks on our specifications. Equations (3) and (4) use the change in the board attributes as their dependent variables, but include control variables at pre-period levels. This specification allows for the possibility that a change in a board attribute is due to the actual value of the control variable and not to its change**.** We change this specification by using changes in control variables instead of levels. One advantage of using changes is that since the pre- and post-periods are 2014 and 2016, respectively, differences in control variables act as firm fixed effects. A disadvantage is that because we measure changes over a two-year window, the size of the changes is relatively small, giving us little cross-sectional variation. We find that using a changes specification has minimal effect on our overall findings. All coefficients on the EU exposure variables remain insignificantly different from zero, with the exception of the regression on Δ*CyberAwareness10K* for the *Dummy EU Segment*, which is significantly positive at the 0.05 level. Thus, our finding that board changes are not related to its EU exposure remains the same. Similarly, we find qualitatively similar results when analyzing the impact of ex ante cyber risk on changes in board cyber oversight when using changes in control variables instead of levels.

We also supplement our analysis of *ex ante* cyber risk by including all cyber risk variables in one regression instead of using them one at a time, as in Table 6. We omit *CyberCount10K* because it is highly correlated with *CyberAwareness10K.* Our results with the three remaining variables are the same as those in Table 6. Thus, our finding that the ex ante risk of the firm impacts the change in cyber risk oversight between the pre- and post-GDPR period remains unchanged.

9. Summary and Suggestions for Future Research

This paper examines how boards change their cyber risk oversight around the passage of the GDPR in 2016. We find that boards adapt quickly to the change in the cyber risk landscape by focusing more on cyber risk, adding directors with cyber/IT expertise, and increasingly assigning cyber risk to the board and/or to their board committees. These results hold both unconditionally as well as in a difference-in-differences framework. We also find that boards in firms with higher ex ante cyber risk adapt more quickly, a finding consistent with the GDPR reflecting an unexpected change in the cyber risk environment. Having a large EU presence, however, is not related to board changes, suggesting that the ramifications of the GDPR are more global, i.e., not confined to firms with large footprints in the EU.

We also examine some of the consequences of these board changes, as they relate to firms' future cyber risks. If the changes in board focus, composition and monitoring are effective in attenuating future cyber risks, then we should see a negative association between board changes and these future risks. If these changes are merely cosmetic, then there will be no systematic associations. Our empirical results are consistent with the first view. Both the incidence of cyber-attacks or data breaches and the number of media stories on a firm's data security decline after its board enhances its monitoring of cyber risk.

Cyber risk is part of a rapidly changing risk environment. Our finding that boards of large U.S. firms are able to pivot their agenda and board expertise quickly after the passage of the GDPR is an indicator of the flexibility and efficacy of their corporate governance systems. That these changes occurred prior to the SEC mandating better disclosures of cyber risk (SEC 2018) or to COSO explicitly recognizing cyber risk as a distinct board agenda risk item (COSO 2019) can be seen as a contradiction of the view that boards inherently are ineffective monitors of top management (e.g., Boivie et al. 2017). Future research may wish to examine board reactions to other pressing, nascent components of enterprise risk, for example, climate change, pandemics, or human capital, to see how truly adaptable boards are. Understanding the board’s role in managing changes in firm risk is critical for stakeholders when assessing their firm’s ability to create and preserve value.

References

Adams, R. B., A. C. Akyol, and P. Verwijimeren. 2018. Director skill sets. *Journal of Financial Economics* 130 (3): 641-62.

Agrawal, A., Knoeber, C. R. 2001. Do some outside directors play a political role? *The Journal of Law and Economics* 44 (1): 179-98.

Amir, E., S. Levi, and T. Livne. 2018. Do firms underreport information on cyber-attacks? Evidence from capital markets. *Review of Accounting Studies* 23 (3): 1177-1206.

Aridor, G., Y-K. Che, and T. Salz. 2021. The effect of privacy regulation on the data industry: Empirical evidence from GDPR. Working paper, Columbia University and MIT.

Armstrong, C. S., J. E. Core, and Guay, W. R. 2014. Do independent directors cause improvements in firm transparency? *Journal of Financial Economics* 113 (3): 383-403.

Berkman, H., J. Jona, G. Lee, and N. Soderstrom. 2018. Cybersecurity awareness and market valuations. *Journal of Accounting and Public Policy* 37 (6): 508-26.

Bernile, G., V. Bhagwat, and S. Yonker. 2018. Board diversity, firm risk, and corporate policies. *Journal of Financial Economics* 127 (3): 588-612.

Boivie, S., M. K. Bednar, R. V. Aguiliera, and J. L. Andrus. 2017. Are boards designed to fail? The implausibility of effective board monitoring. *Academy of Management Annals* 10 (1): 319-407.

Bradford, A. 2012. The Brussels effect. *Northwestern University Law Review* 107 (1): 1-68

Bryan, D., M. Liu, S. Tiras, and Z. Zhuang. 2013. Optimal versus suboptimal choices of accounting expertise on audit committees and earnings quality. *Review of Financial Studies* 18 (4): 1123-58.

Chen, Q., I. Goldstein, and W. Jiang. 2006. Price informativeness and investment sensitivity to stock price. *The Review of Financial Studies* 20 (3): 619-50.

Cohen, J. R., U. Hoitash, G. Krishnamoorthy, and A. M. Wright. 2014. The effect of audit committee industry expertise on monitoring the financial reporting process. *The Accounting Review* 89 (1): 243-73.

Coles, J. L., N. D. Daniel, and L. Naveen. 2008. Boards: Does one size fit all? *Journal of Financial Economics* 87 (2): 329-56.

COSO (Committee of Sponsoring Organizations of the Treadway Commission). 2004. Enterprise risk management – Integrated framework. https://www.coso.org/Documents/PR-09292004-ERM-Integrated-Framework.pdf

COSO (Committee of Sponsoring Organizations of the Treadway Commission). 2017. Enterprise risk management – Integrating with strategy and performance. https://www.coso.org/documents/2017-coso-erm-integrating-with-strategy-and-performance-executive-summary.pdf

COSO (Committee of Sponsoring Organizations of the Treadway Commission). 2019. Managing cyber risk in a digital age. https://www.coso.org/Documents/COSO-Deloitte-Managing-Cyber-Risk-in-a-Digital-Age.pdf

Davis, K. E., and F. Marotta-Wurgler. 2019. Contracting for personal data. *New York University Law Review* 94 (4): 662-705

DeFond, M. L., R. N. Hann, R, and X. Hu. 2005. Does the market value financial expertise on audit committees of board of directors? *Journal of Accounting Research* 43 (2): 153-93.

Deloitte. 2018. On the board's agenda: US cyber risk in the boardroom: Accelerating from acceptance to action, https://www2.deloitte.com/content/dam/Deloitte/us/Documents/center-for-board-effectiveness/us-cbe-feb-otba-risk-in-the-boardroom.pdf

Dionne, G., O. M. Chun, and T. Triki. 2019. The governance of risk management: The importance of directors' independence and financial knowledge. *Risk Management and Insurance Review* 22 (3): 247-77.

Dionne, G., and T. Triki. 2005. Risk management and corporate governance: The importance of independence and financial knowledge for the board and the audit committee. Working paper, HEC Montreal.

Dow, J., and G. Gorton. 1997. Stock market efficiency and economic efficiency: Is there a connection? *The Journal of Finance* 52 (3): 1087-129.

Duchin, R., J. Matsusaka, and O. Ozbas. 2010. When are outside directors effective? *Journal of Financial Economics* 96 (2): 195-214.

Dye, R. A., and S. S. Sridhar. 2002. Resource allocation effects of price reactions to disclosures. *Contemporary Accounting Research* 19 (3): 385-410.

Edmans, A., S. Jayaraman, and J. Schneemeier. 2017. The source of information in prices and investment-price sensitivity. *Journal of Financial Economics* 126 (1): 74-96.

Ertimur, Y., F. Ferri, and D. A. Maber. 2011. Reputation penalties for poor monitoring of executive pay: evidence from option backdating. *Journal of Financial Economics* 104 (1): 118-44.

Faleye, O., R. Hoitash, and U. Hoitash. 2018. Industry expertise on corporate boards. *Review of Quantitative Finance and Accounting* 50 (2): 441-79.

Fama, E. F., and K. R. French. 2014. A five-factor asset pricing model. *Journal of Financial Economics* 116 (1): 1-22.

Fama, E. F., and M. C. Jensen. 1983. Separation of ownership and control. *Journal of Law and Economics* 26 (2): 301-25.

Fich, E. M., and A. Shivdasani. 2007. Financial fraud, director reputation, and shareholder wealth. *Journal of Financial Economics* 86 (2): 306-36.

Frankenreiter, J. 2021. The missing California effect in data privacy law. Working paper, Washington University in St. Louis.

Gilson, S. 1990. Bankruptcy, boards, banks, and bondholders: Evidence on changes in corporate ownership and control when firms default. *Journal of Financial Economics* 27 (2): 355-87.

Gordon, L. A., M. P. Loeb, and T. Sohail. 2010. Market value of voluntary disclosures concerning information security. *MIS Quarterly* 34 (3): 567-94.

Gregory, H. J. 2015/2016. A board roadmap for 2016. *Practical Law*, https://content.next.westlaw.com/w-001-0036?transitionType=Default&contextData=(sc.Default)&_lrTS=20180917132921681

Guner, A. B., U. Malmendier, and G. Tate. 2008. Financial expertise of directors. *Journal of Financial Economics* 88 (2): 323-54.

Haislip, J., K. Kolev, R. Pinskerf, and T. Steffen. 2019. The economic cost of cybersecurity breaches: A brad-based analysis. Working paper, Texas Tech University, Baruch College, Florida Atlantic University, and Yale University.

Harris, M., and A. Raviv. 2008. A theory of board control and size. *The Review of Financial Studies* 21 (4): 1797-832.

Hermalin, B., and M. S. Weisbach. 1998. Endogenously chosen boards of directors and their monitoring of the CEO. *American Economic Review* 88 (1): 96-118.

Hilary, G., B. Segal, and M. H. Zhang. 2016. Cyber-risk disclosure: Who cares? Working paper, Georgetown University and Fordham University.

Ittner, C. D., and T. Keusch. 2015. The influence of board of directors' risk oversight on risk management maturity and firm risk-taking. Working paper, University of PennsylvaniaCop and Erasmus University of Rotterdam.

Kamiya, S., J. K. Kang, J. Kim, A. Milidonis, and R. M. Stulz. 2018. What is the impact of successful cyberattacks on target firms? Working paper, Nanyang Technological University, Hong Kong Polytechnic University, University of Cyprus, and The Ohio State.

Kaplan, S., and D. Reischus. 1990. Outside directorships and corporate performance. *Journal of Financial Economics* 27 (2): 389-410.

Kim, S., and A. Klein. 2017. Did the 1999 NYSE and NASDAQ listing standard changes on audit committee composition benefit investors? *The Accounting Review* 92 (6): 187-212.

Kim, D., and L. Starks. 2016. Board heterogeneity of expertise and firm performance. Working paper. The University of Toronto and University of Texas Austin.

Klein, A. 1998. Firm performance and board committee structure. *The Journal of Law and Economics* 41 (1): 275-304.

Lanz, J. 2014. Cybersecurity governance: The role of the audit committee and the CPA. *The CPA Journal*. November: 6-10.

Liu, L. Y. 2020. Do auditors help prevent data breaches? PhD dissertation, University of Chicago.

NACD (National Association of Corporate Directors). 2014. Cyber-risk oversight. https://www.nacdonline.org/files/NACD%20CyberRisk%20Oversight%20Executive%20Summary.pdf

Oesch, D., and F. Urban. 2019. International PCAOB inspections and earnings management transmissions within multinational business groups. Working paper, University of Zurich.

Ormazabal, G. 2010. The role of the board in corporate risk oversight. Working paper, Stanford University.

Piotroski, J. D. and S. Srinivasan. 2008. Regulation and bonding: the Sarbanes-Oxley act and the flow of international listings. *Journal of Accounting Research* 46 (2): 383-425.

SEC. 2009a. *SEC Approves Enhanced Disclosure about Risk, Compensation and Corporate Governance*, https://www.sec.gov/news/press/2009/2009-268.htm.

SEC. 2009b. *Proxy Disclosure Enhancement*, https://www.sec.gov/rules/final/2009/33-9089.pdf.

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.

Srinivasan, S. 2005. Consequences of financial reporting failure for outside directors: Evidence from accounting restatements and audit committee members. *Journal of Accounting Research* 43 (2): 291-334.

Van Peteghem, M., L. Bruynseels, and A. Gaeremynck. 2018. Board diversity: A tale of faultiness and frictions in the board of directors. *The Accounting Review* 93 (2): 339-67.

Wang, C., F. Xie, and M. Zhu. 2015. Industry expertise of independent directors and board monitoring. *Journal of Financial and Quantitative Analysis* 50 (5): 929-62.

Appendix 1: Variable Definitions

Variable Name	Variable Definition	Sources
A. Board Awareness/ Expertise/ Monitoring Variables		
CyberAwarenessDEF14A	Indicator variable if the keyword “cyber” appears at least once in a company’s proxy statement.	Hand collected from Form DEF14A
CyberCountDEF14A	The total number of times the keyword “cyber” appears in a company’s proxy statement.	Hand collected from Form DEF14A
ExpBoD	Indicator variable if the firm has at least one cyber/IT expert on its board.	Hand collected from Form DEF14A
ExpAudComm	Indicator variable if the firm has at least one cyber/IT expert on its Audit Committee.	Hand collected from Form DEF14A
ExpRiskComm	Indicator variable if the firm has at least one cyber/IT expert on its Risk Committee.	Hand collected from Form DEF14A
ExpTechComm	Indicator variable if the firm has at least one cyber/IT expert on its Technology Committee.	Hand collected from Form DEF14A
MonBoD/Comm	Indicator variable if the firm discusses the responsibility of the board or specific committees to monitor cyber/IT risks.	Hand collected from Form DEF14A
MonBoD Only	Indicator variable if the firm discusses the responsibility and explicitly states the board as a whole (rather than delegating to individual committees) monitors cyber/IT risks.	Hand collected from proxy statements
MonAudComm	Indicator variable if the firm discusses the responsibility and explicitly states the board delegates the responsibility of monitoring cyber/IT risks to its Audit Committee.	Hand collected from Form DEF14A
MonRiskComm	Indicator variable if the firm discusses the responsibility and explicitly states the board delegates the responsibility of monitoring cyber/IT risks to its Risk Committee.	Hand collected from Form DEF14A
MonTechComm	Indicator variable if the firm discusses the responsibility and explicitly states the board delegates the responsibility of monitoring cyber/IT risks to its Technology Committee.	Hand collected from Form DEF14A
B. EU Exposure Variables		
Dummy_EU Segment	Indicator variable if the firm reports at least one customer segment is located in one of the 28 European Union countries in year 2014.	Compustat Segment Report
% Rev_EU Segments	The percentage of a company’s sales revenue from all EU segments divided by its total sales revenue in year 2014.	Compustat Segment Report
EU Rev Growth	The companies’ sales revenue from all EU segments in year 2014 over year 2013, subtract one.	Compustat Segment Report
C. Cyber Risk Exposure Variables		
CyberAwareness10K	Indicator variable if the keyword “cyber” appears in a company’s 2014 Form 10-K.	Hand collected from Form 10-K
CyberCount10K	The total number of times the keyword “cyber” appears at least once in a company’s 2014 Form 10-K.	Hand collected from Form 10-K
MediaCov	Indicator variable if the firm has at least one third-party media article related to data security issues in the past twelve months of 12/31/2014.	TruValue Labs Insight 360 TTM database

CAR	Cumulative abnormal returns over the GDPR events line using the Fama-French 5-factor model for the expectation model (Fama and French 2014). The model is estimated as follow using the stock return data from 6/1/2015 to 5/31/2016, inclusively: $R_{jt} - R_{ft} = \beta_{j0} + \beta_{j1}(R_{Mt} - R_{ft}) + \ \beta_{j2}\text{SMB}_t + \beta_{j3}\text{HML}_t + \beta_{j4}\text{RMW}_t + \beta_{j5}\text{CMA}_t + \sum_{k=1}^{18} \delta_{jk} * E_{kt} + \epsilon_{jt}$. E_{kt} indicates the k^{th} GDPR event date, which equals one if a date is an event date and zero otherwise. $CAR_j = \sum_{k=1}^{18} \widehat{\delta_{jk}}$.	CRSP and Kenneth R. French's website
D. Economic Consequence Variables		
GDPRAwareness10K	Indicator variable if the keyword "General Data Privacy Regulation" or "GDPR" appear in a company's Form 10-K**.**	Hand collected from Form 10-K
Media Attention	The number of media stories related to data security issues over the years 2017 through 2019.	TruValue Labs Insight 360 TTM database
Incidence	Indicator variable if the firm has any known cyber-attacks or data breaches over the years 2017 through 2019.	Privacy Rights Clearinghouse database
E. Control Variables		
Size	The natural logarithm of total assets at year-end.	Compustat
Big Four	Indicator variable if the firm has a Big Four auditor.	Compustat
InstOwn	The natural logarithm of one plus the sum of total institutional ownership at year-end.	Thomson Reuters Database
ICW	Indicator variable if the company has a 404 report indicating internal control weakness in the year.	Audit Analytics
Leverage	Total liabilities over total assets at year-end.	Compustat
Board Size	The natural logarithm of the number of board directors at year-end.	BoardEx
%IndDir	The percentage of independent directors at year-end.	BoardEx
PaidCashDiv	Indicator variable if the firm paid cash dividends in the year.	Compustat
PrePdAwareness	Indicator variable if the firm mentions "cyber" keywords in the last proxy statement before the first GDPR event date.	Hand collected from Form DEF14A
PrePdMon	Indicator variable if the firm discusses the responsibility of the board or specific committees to monitor cyber/IT risks in the last proxy statement before the first GDPR event date.	Hand collected from Form DEF14A
PrePdExp	Indicator variable if the firm discloses at least one Cyber/IT expert on its board in the last proxy statement before the first GDPR event date.	Hand collected from Form DEF14A

Appendix 2: Major Provisions of the General Data Protection Regulation (GDPR)

This Appendix presents the main changes GDPR imposes on the regulatory landscape of data security and data privacy, taken directly from the GDPR regulation.

Increased Territorial Scope: The GDPR extends the EU's jurisdiction on compliance. Under Article 3, all processing of personal data by controllers and processors for subjects residing in the EU falls under the new regulation, irrespective of whether the processing takes place in the EU or not. Covered activities include the offering of goods or services and the monitoring of behavior that takes place within the EU.

Penalties: Organizations in breach of GDPR can be fined up to four percent of annual global revenues or €20 Million (whichever is greater). This is the maximum fine that can be imposed for the most serious infringements. There is a tiered approach to fines, e.g., a company can be fined two percent for not having their records in order (GDPR Article 83). It is important to note that these rules apply to both controllers and processors – meaning "clouds" are not exempt from GDPR enforcement.

Consent**:** Under Article 7, the conditions for consent have been strengthened. Companies must ask for it in an intelligible and easily accessible form, using clear and plain language. The request for consent must be clear and distinguishable from other matters. The ability to withdraw consent must be as easy as it is to give it.

Breach Notification**:** Breach notification is mandatory when a data breach is likely to "result in a high risk to the rights and freedoms of natural persons" (GDPR Article 34). This must be done within 72 hours of first having become aware of the breach. Data processors are required to notify their customers, the controllers, "without undue delay" after first becoming aware of a data breach (GDPR Article 33).

Right to Access**:** Article 15 contains the right for data subjects to obtain from the data controller confirmation whether, where , and for what purpose their personal data are being processed . Further, the controller must provide the data subject a copy of their personal data, free of charge, in an electronic format.

Right to be Forgotten**:** The right to be forgotten (Article 17) entitles the data subject to have the data controller erase personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data. The conditions for erasure, as outlined in Article 17, include the data no longer being relevant to original purposes for processing, or a data subject withdrawing consent.

Data Portability**:** Data subjects have the right to receive their personal data in a "commonly used and machine-readable format" (GDPR Article 20).

Privacy by Design**:** Privacy by design calls for the inclusion of data protection from the onset of the designing of systems. Specifically: "The controller shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation" (GDPR Article 24). Furthermore, Article 5 calls for controllers to hold and process only the data strictly necessary for the completion of its duties (data minimization).

Data Protection Officers**:** The appointment of a data protection officer (DPO) is mandatory only for those controllers and processors whose core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale, or of special categories of data, or data relating to criminal convictions and offenses. The primary role of the DPO is to ensure that their organization processes the personal data of their staff, customers and any other data subject in compliance with the applicable data protection rules.

Appendix 3: GDPR Events

Event	*Dates*	*Stages*	*Description*
D1	6/15/15	Proposal	The Council of the EU approved its version in Its First Reading allowing the regulation to pass into the final stage of legislation known as the "Trilogue"
D2	6/24/15	Trilogue	The First Trilogue Meeting: Package approach; Agreement on the overall roadmap for Trilogue negotiations; General method and approach for delegated and implementing acts
D3	7/14/15	Trilogue	The Second Trilogue Meeting: Territorial Scope (Article 3); Representative (Article 25); International Transfers (Chapter V) with related definitions
D4	9/16/15	Trilogue	First Day of the Third Trilogue Meeting: Data Protection Principles (Chapter II); Data Subjects Rights (Chapter III); Controller and Processor (Chapter IV)
D5	9/17/15	Trilogue	Second Day of the Third Trilogue Meeting: Data Protection Principles (Chapter II); Data Subject Rights (Chapter III); Controller and Processor (Chapter IV)
D6	9/29/15	Trilogue	First Day of the Fourth Trilogue Meeting: Data Protection Principles (Chapter II); Data Subjects Rights (Chapter III); Controller and Processor (Chapter IV)
D7	9/30/15	Trilogue	Second Day of the Fourth Trilogue Meeting: Data Protection Principles (Chapter II); Data Subjects Rights (Chapter III); Controller and Processor (Chapter IV)
D8	10/15/15	Trilogue	The Fifth Trilogue Meeting: Independent Supervisory Authorities (Chapter VI); Cooperation and Consistency (Chapter VII)
D9	10/28/15	Trilogue	The Sixth Trilogue Meeting: Independent Supervisory Authorities (Chapter VI); Cooperation and Consistency (Chapter VII)
D10	11/11/15	Trilogue	First Day of the Seventh Trilogue Meeting: Objectives and Material Scope (Chapter I): Specific Regimes (Chapter IX)
D11	11/12/15	Trilogue	Second Day of the Seventh Trilogue Meeting: Objectives and Material Scope (Chapter I); Specific Regimes (Chapter IX)
D12	11/24/15	Trilogue	The Eight Trilogue Meeting: All open issues From Chapter I to IX
D13	12/10/15	Trilogue	The Ninth Trilogue Meeting: Delegated and Implementing Acts (Chapter X); Final Provisions (Chapter XI); Remaining issues
D14	12/15/15	Trilogue	The Parliament and European Council come to an agreement
D15	4/8/16	Approval	GDPR is adopted by the Council of the European Union
D16	4/14/16	Approval	GDPR is adopted by the European Parliament
D17	5/4/16	Approval	The GDPR is published in the Official Journal of the European Union
D18	5/25/16	Approval	GDPR effectively becomes law

TABLE 1

Sample and summary statistics

Panel A: Sample selection

	Number of Firms
Number of firms in Compustat CRSP Merged Database at the year ended	5,595
Less: Non-US firms	-923
Less: Number of firms with missing control variables in the pre-period	-1,056
Less: Number of firms with missing proxy statements in the pre-period	-998
Less: Number of firms with missing proxy statements in the post-period	-509
Less: Number of firms that were cyber-attacked between 2005 and 2014	-16
Number of firms for the cross-sectional tests	2,093

Panel B: Descriptive statistics

Variables	N	Mean	Std. Dev.	Min	Median	Max
Total Assets (in $million)	2,093	8,686.24	39,721.77	3.76	1,213.85	856,240.00
Big Four	2,093	0.71	0.45	0.00	1.00	1.00
Institutional Ownership	2,093	0.49	0.39	0.00	0.58	1.00
ICW	2,093	0.04	0.20	0.00	0.00	1.00
Leverage	2,093	0.57	0.26	0.06	0.56	1.27
PaidCashDiv	2,093	0.57	0.50	0.00	1.00	1.00
Number of Board Directors	2,093	8.66	2.47	4.00	8.00	24.00
%IndDir	2,093	0.78	0.13	0.18	0.80	1.00

Notes:

Panel A describes our sample selection, and panel B reports the descriptive statistics.

TABLE 2

GDPR and corporate boards' cyber focus, expertise, and monitoring assignment in the pre- and post-GDPR periods

Panel A: Univariate analysis

		Pre-GDPR		Post-GDPR		T-test of the Mean
Variables	N	Mean (a)	S.D.	Mean (b)	S.D.	(b)-(a)
CyberAwarenessDEF14A	2,093	10.70%	30.92%	23.12%	42.17%	12.42% ***
CyberCountDEF14A	2,093	0.18	0.74	0.53	1.60	0.35 ***
ExpBoD	2,093	17.34%	37.87%	23.36%	42.32%	6.02% ***
ExpAudComm	2,093	11.32%	31.70%	11.85%	32.33%	0.53% ***
ExpRiskComm	2,093	1.43%	11.89%	1.58%	12.46%	0.15% *
ExpTechComm	2,093	1.00%	9.97%	1.29%	11.29%	0.29% *
MonBoD/Comm	2,093	8.93%	28.53%	17.30%	37.83%	8.37% ***
MonBoD Only	2,093	2.48%	15.57%	4.06%	19.74%	1.58% ***
MonAudComm	2,093	3.39%	18.11%	9.46%	29.27%	6.07% ***
MonRiskComm	2,093	1.48%	12.08%	2.82%	16.56%	1.34% ***
MonTechComm	2,093	1.15%	10.65%	2.34%	15.12%	1.19% ***

Panel B: Multivariate analysis

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)
VARIABLES	Cyber Awareness DEF14A	Cyber Count DEF14A	Exp BoD	Exp Aud Comm	Exp Risk Comm	Exp Tech Comm	Mon BoD/ Comm	Mon BoD Only	Mon Aud Comm	Mon Risk Comm	Mon Tech Comm
Post	0.34***	0.11***	0.05***	0.01	-0.00	-0.00	0.08***	0.02**	0.06***	0.01*	0.01
	(7.21)	(8.24)	(3.45)	(0.56)	(-0.00)	(-0.62)	(6.12)	(2.49)	(6.91)	(1.76)	(1.62)
Size	0.12***	0.03***	0.03***	0.01***	0.01***	0.01***	0.02***	0.00	0.01***	0.00	0.01***
	(6.57)	(7.04)	(5.47)	(2.60)	(3.15)	(2.89)	(5.08)	(1.10)	(3.75)	(1.47)	(2.84)
Big Four	-0.07	-0.01	-0.02	-0.01	-0.00	-0.00	-0.00	-0.01	0.02*	-0.01	-0.01*
	(-1.51)	(-0.51)	(-1.10)	(-0.57)	(-1.31)	(-1.44)	(-0.32)	(-1.00)	(1.89)	(-1.33)	(-1.85)
InstOwn	0.00	0.06**	-0.07**	-0.04	0.00	-0.00	0.06***	0.02**	0.02	0.02**	0.00
	(0.05)	(2.19)	(-2.35)	(-1.64)	(0.21)	(-0.66)	(2.88)	(2.07)	(1.40)	(2.08)	(0.40)
ICW	-0.10**	-0.01	-0.02	-0.01	-0.00	-0.00**	-0.00	-0.00	-0.00	0.01	-0.00
	(-2.53)	(-0.49)	(-0.50)	(-0.39)	(-1.30)	(-2.54)	(-0.02)	(-0.18)	(-0.23)	(1.00)	(-0.27)
Leverage	-0.09	-0.01	-0.03	-0.00	0.01***	0.01	0.01	-0.02*	-0.00	0.01*	0.02**
	(-1.35)	(-0.57)	(-1.06)	(-0.04)	(3.28)	(1.47)	(0.55)	(-1.94)	(-0.12)	(1.77)	(2.10)
BoardSize	0.15*	0.06**	0.11***	0.07***	0.02**	-0.01	0.04	0.01	-0.00	0.03**	0.01
	(1.91)	(1.98)	(3.82)	(3.24)	(2.05)	(-0.78)	(1.44)	(0.59)	(-0.13)	(2.33)	(1.12)
%IndDir	0.77***	0.31***	0.40***	0.23***	0.01	0.01	0.13***	0.01	0.07**	0.03	0.04***
	(6.34)	(6.77)	(7.76)	(5.51)	(0.63)	(0.43)	(3.00)	(0.55)	(2.03)	(1.50)	(2.92)
PaidCashDiv	-0.11**	-0.01	-0.01	-0.03*	-0.00	0.00	-0.00	-0.00	-0.01	0.00	-0.00
	(-2.27)	(-0.86)	(-0.68)	(-1.73)	(-0.55)	(0.28)	(-0.05)	(-0.59)	(-0.92)	(0.47)	(-0.48)
Number of Firm-years	3,700	3,700	3,700	3,700	3,700	3,700	3,700	3,700	3,700	3,700	3,700
Adjusted R-squared	0.08	0.11	0.06	0.03	0.03	0.01	0.07	0.01	0.04	0.03	0.01

Notes:

This table examines whether boards' cyber focus, expertise, and monitoring assignment change around the passage of the GDPR. Appendix 1 summarizes whether and the number of times firms mention "cyber" in their Forms DEF14A, whether companies have directors with cyber/IT expertise on their boards or specific committees, and whether companies explicitly assign cyber risk monitoring tasks to their boards or specific committees in the periods before versus after the passage of the GDPR. We also report differences in means between the pre- and post-GDPR periods. The pre-GDPR period is the last Form DEF14A before the first GDPR event date (6/15/2015); the post-GDPR period is the first Form DEF14A after the last GDPR event date (5/25/2016). Panel B presents multivariate analyses on the regressions on cyber awareness, expertise, and monitoring, controlling for firm risks and corporate governance characteristics as they may also lead to changes on the board structures. We also control for industry fixed effects according to Fama-French 12 industry categories to capture unobservable industry trends. The "Post" indicator is a dummy variable equals to one when the observation is in the post-GDPR period described above. Because of the availability of the control variables, the number of firms in Panel B is reduced to1,850 (3,700 for two periods). Refer to Appendix 1 for variable definitions and data sources. Robust t-statistics are reported in parentheses. *, **, and *** represent significance levels of 0.10, 0.05, and 0.01 respectively.

TABLE 3

Difference-in-differences analysis of GDPR's impact on changes on boards' cyber focus, expertise, and monitoring assignments

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)
VARIABLES	Cyber Awareness DEF14A	Cyber Count DEF14A	Exp BoD	Exp Aud Comm	Exp Risk Comm	Exp Tech Comm	Mon BoD/ Comm	Mon BoD Only	Mon Aud Comm	Mon Risk Comm	Mon Tech Comm
Post	0.09	0.03	0.06*	0.03	-0.01**	-0.00	0.01	-0.01	0.05**	-0.01	0.00
	(1.31)	(0.83)	(1.68)	(1.22)	(-2.40)	(-0.07)	(0.53)	(-0.79)	(2.28)	(-1.46)	(0.09)
Treated	-0.08	-0.04*	0.04	0.05**	-0.00*	-0.00	-0.01	-0.00	0.00	-0.01*	-0.01
	(-1.58)	(-1.67)	(1.35)	(2.16)	(-1.71)	(-0.82)	(-0.34)	(-0.36)	(0.38)	(-1.83)	(-0.97)
Treated X Post	0.29***	0.10***	0.00	-0.02	0.01	-0.00	0.07***	0.03**	0.02	0.02**	0.01
	(4.00)	(2.91)	(0.07)	(-0.66)	(1.41)	(-0.01)	(2.59)	(1.97)	(0.95)	(2.45)	(0.81)
Size	0.11***	0.03***	0.02***	0.01*	0.01***	0.00**	0.02***	0.00	0.01***	0.00**	0.00***
	(6.59)	(6.77)	(3.93)	(1.65)	(3.70)	(2.26)	(5.10)	(1.07)	(3.66)	(2.45)	(2.75)
Big Four	-0.02	0.00	0.01	0.01	-0.01***	-0.00	0.00	-0.01	0.02***	-0.02***	-0.01*
	(-0.55)	(0.36)	(0.94)	(1.14)	(-2.62)	(-0.32)	(0.12)	(-1.05)	(2.63)	(-2.71)	(-1.83)
InstOwn	-0.10***	-0.01	-0.01	-0.01	-0.00**	-0.00**	0.00	-0.00	-0.00	0.01	-0.00
	(-2.64)	(-0.50)	(-0.42)	(-0.38)	(-2.15)	(-2.35)	(0.10)	(-0.02)	(-0.13)	(0.81)	(-0.36)
ICW	-0.08	-0.01	-0.04*	-0.01	0.02***	0.00	0.01	-0.02*	-0.00	0.02***	0.02**
	(-1.23)	(-0.38)	(-1.71)	(-0.57)	(3.99)	(0.84)	(0.68)	(-1.85)	(-0.34)	(3.37)	(2.39)
Leverage	0.01	0.04**	-0.02	-0.01	-0.01	0.00	0.04***	0.02**	0.02	0.00	0.00
	(0.17)	(2.44)	(-1.06)	(-0.89)	(-1.51)	(0.16)	(2.76)	(1.99)	(1.58)	(0.53)	(0.36)
BoardSize	0.01	0.01*	0.01***	0.01***	0.00**	-0.00	0.01*	0.00	-0.00	0.00**	0.00
	(1.62)	(1.71)	(3.33)	(2.82)	(2.19)	(-0.63)	(1.87)	(1.10)	(-0.08)	(2.22)	(0.99)
%IndDir	0.88***	0.33***	0.41***	0.23***	0.00	0.01	0.13***	0.01	0.06*	0.02	0.04***
	(7.19)	(7.14)	(8.27)	(5.75)	(0.30)	(0.60)	(2.80)	(0.32)	(1.88)	(1.09)	(3.24)
PaidCashDiv	-0.12**	-0.01	-0.04**	-0.05***	0.00	-0.00	0.01	0.00	-0.01	0.01**	-0.00
	(-2.40)	(-0.97)	(-2.52)	(-3.34)	(1.30)	(-0.50)	(0.65)	(0.37)	(-1.14)	(2.35)	(-0.22)
Constant	-1.21***	-0.39***	-0.36***	-0.18***	-0.05***	-0.02*	-0.24***	-0.01	-0.12***	-0.07***	-0.07***
	(-7.59)	(-9.35)	(-7.96)	(-4.81)	(-3.87)	(-1.84)	(-6.14)	(-0.24)	(-3.98)	(-4.44)	(-4.88)
Number of Firm-years	3,700	3,700	3,700	3,700	3,700	3,700	3,700	3,700	3,700	3,700	3,700
Adjusted R-squared	0.06	0.09	0.04	0.02	0.02	0.01	0.06	0.00	0.03	0.02	0.01

Notes:

This table uses a difference-in-differences method to examine whether corporate boards' cyber focus, expertise, and monitoring assignment change after the passage of the GDPR. Because HIPAA, a stringent privacy regulation, already regulates healthcare firms before the GDPR, we identify companies in the healthcare industry as a control group for the GDPR treatment. The output variables, *Post*, the control variables, and the sample sizes are the same as in Table 2, Panel B. *Treated* is a dummy equal to one when the sample company does not belong to the healthcare industry, according to the Fama-French 12 industry categories. *Treated X Post* is the primary variable of interest. Refer to Appendix 1 for variable definitions and data sources. Robust t-statistics are reported in parentheses. *, **, and *** represent significance levels of 0.10, 0.05, and 0.01 respectively.

TABLE 4

Descriptive statistics and correlation of cross-sectional variables

Panel A: Descriptive statistics

Variable	N	Mean	S.D.	Min	Median	Max
Dummy_EU Segment	2,093	0.25	0.43	0.00	0.00	1.00
% Rev_EU Segments	2,093	0.05	0.11	0.00	0.00	0.54
EU Rev Growth	2,093	0.05	0.45	-1.00	0.00	6.12
CyberAwareness10K	2,093	0.42	0.49	0.00	0.00	1.00
CyberCount10K	2,093	1.48	3.36	0.00	0.00	53.00
MediaCov	2,093	0.19	0.39	0.00	0.00	1.00
CAR	2,093	0.45%	11.24%	-54.91%	-0.05%	132.71%

Panel B: Correlations among companies' EU exposure variables in the pre-GDPR period

	Dummy_EU Segment	% Rev_EU Segments	EU Rev Growth
Dummy_EU Segment	1.0000		
% Rev_EU Segments	0.7647 ***	1.0000	
EU Rev Growth	0.2229 ***	0.2049 ***	1.0000

Panel C: Correlations among companies' cyber awareness in 10-K and DEF14A in the pre-GDPR period

	Cyber Awareness10K	Cyber Count10K	Cyber AwarenessDEF14A	Cyber CountDEF14A
CyberAwareness10K	1.0000			
CyberCount10K	0.5175 ***	1.0000		
CyberAwarenessDEF14A	0.3411 ***	0.1708 ***	1.0000	
CyberCountDEF14A	0.2608 ***	0.1845 ***	0.7078 ***	1.0000

Notes:

This table reports the descriptive statistics (Panel A), the Pearson correlations among the three EU exposure variables (Panel B), and the Pearson correlations among the cyber awareness variables from the firms' 10-K and proxy statements (Panel C). All variable definitions are in Appendix 1. Except for the CAR, all the other cross-sectional variables are measured in the pre- GDPR period, i.e., in 2014. *, **, and *** represent significance levels of 0.10, 0.05, and 0.01 respectively.

TABLE 5

GDPR and changes in corporate boards' cyber awareness, expertise, and monitoring depending on firms' EU exposures

Panel A: EU exposure proxy #1: Dummy variable if the firm reports an EU segment

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)
VARIABLES	ΔCyber Awareness DEF14A	ΔCyber Count DEF14A	ΔExp BoD	ΔExp Aud Comm	ΔExp Risk Comm	ΔExp Tech Comm	ΔMon BoD/ Comm	ΔMon BoD Only	ΔMon Aud Comm	ΔMon Risk Comm	ΔMon Tech Comm
Dummy_EU Segment	0.01	-0.03	0.02	-0.00	-0.00	-0.00	0.00	0.02	-0.00	-0.01	-0.00
	(0.54)	(-0.41)	(1.41)	(-0.49)	(-1.53)	(-1.06)	(0.09)	(1.60)	(-0.22)	(-0.92)	(-0.06)
Number of Firms	2,093	2,093	2,093	2,093	2,093	2,093	2,093	2,093	2,093	2,093	2,093
Adjusted R-squared	0.12	0.05	0.08	0.01	0.01	-0.00	0.14	0.05	0.05	0.01	0.01

Panel B: EU exposure proxy #2: % of revenues from the EU segment

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)
VARIABLES	ΔCyber Awareness DEF14A	ΔCyber Count DEF14A	ΔExp BoD	ΔExp Aud Comm	ΔExp Risk Comm	ΔExp Tech Comm	ΔMon BoD/ Comm	ΔMon BoD Only	ΔMon Aud Comm	ΔMon Risk Comm	ΔMon Tech Comm
% Rev_EU Segments	0.02	-0.14	0.07	-0.01	-0.00	0.00	0.05	0.08*	-0.02	-0.03	0.03
	(0.28)	(-0.61)	(1.15)	(-0.98)	(-1.44)	(0.09)	(0.68)	(1.72)	(-0.39)	(-1.06)	(0.91)
Number of Firms	2,093	2,093	2,093	2,093	2,093	2,093	2,093	2,093	2,093	2,093	2,093
Adjusted R-squared	0.12	0.05	0.08	0.01	0.01	0.00	0.14	0.05	0.05	0.01	0.01

Panel C: EU exposure proxy #3: The EU segment's revenue growth

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)
VARIABLES	ΔCyber Awareness DEF14A	ΔCyber Count DEF14A	ΔExp BoD	ΔExp Aud Comm	ΔExp Risk Comm	ΔExp Tech Comm	ΔMon BoD/ Comm	ΔMon BoD Only	ΔMon Aud Comm	ΔMon Risk Comm	ΔMon Tech Comm
EU Rev Growth	-0.01	-0.01	0.03	0.00	-0.00	0.00	-0.01	-0.00	-0.01	0.01	-0.00
	(-0.79)	(-0.36)	(1.59)	(0.05)	(-0.67)	(0.46)	(-0.94)	(-0.42)	(-0.65)	(1.20)	(-0.15)
Number of Firms	2,093	2,093	2,093	2,093	2,093	2,093	2,093	2,093	2,093	2,093	2,093
Adjusted R-squared	0.12	0.05	0.08	0.01	0.01	0.00	0.14	0.05	0.05	0.01	0.01

Notes:

This table examines whether the GDPR's impact on the changes in corporate boards' cyber awareness, expertise, and monitoring vary based on companies' business exposures to the EU market. We use different variables to proxy for companies' EU exposures: Panel A uses the EU Segment dummy variable, which equals one if the company reports a business segment in the EU or any of its 28 union countries. Panel B uses the percentage of a company's revenue from all EU segments divided by its total revenue. Panel C uses the EU segment's revenue growth rate from 2013 to 2014. In all regression analyses, we control for the same set of control variables and industry fixed effects as in Table 2, Panel B at the end of 2014. Further, we control for the pre-GDPR period board cyber awareness, expertise, and monitoring to capture the mean reversal effects. Refer to Appendix 1 for variable definitions and data sources. Robust t-statistics are reported in parentheses. *, **, and *** represent significance levels of 0.10, 0.05, and 0.01 respectively.

TABLE 6

GDPR and changes in corporate boards' cyber awareness, expertise, and monitoring assignment depending on firms' cyber risk exposures

Panel A: RE proxy #1: Dummy variable if firms mention "cyber" keywords in pre-GDPR 10-K reports

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)
VARIABLES	ΔCyber Awareness DEF14A	ΔCyber Count DEF14A	ΔExp BoD	ΔExp Aud Comm	ΔExp Risk Comm	ΔExp Tech Comm	ΔMon BoD/ Comm	ΔMon BoD Only	ΔMon Aud Comm	ΔMon Risk Comm	ΔMon Tech Comm
CyberAwareness10K	0.03*	0.06	0.05***	0.00	0.00*	0.00	0.03**	0.00	0.03**	-0.00	0.00
	(1.72)	(1.23)	(3.31)	(1.03)	(1.69)	(0.26)	(2.20)	(0.32)	(2.42)	(-0.43)	(0.30)
Number of Firms	2,093	2,093	2,093	2,093	2,093	2,093	2,093	2,093	2,093	2,093	2,093
Adjusted R-squared	0.12	0.06	0.08	0.02	0.01	0.00	0.14	0.05	0.05	0.01	0.01

Panel B: RE proxy #2: Number of "cyber" keywords in pre-GDPR 10-K reports

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)
VARIABLES	ΔCyber Awareness DEF14A	ΔCyber Count DEF14A	ΔExp BoD	ΔExp Aud Comm	ΔExp Risk Comm	ΔExp Tech Comm	ΔMon BoD/ Comm	ΔMon BoD Only	ΔMon Aud Comm	ΔMon Risk Comm	ΔMon Tech Comm
CyberCount10K	0.01***	0.05*	0.00**	0.00	-0.00	-0.00	0.00*	0.00	0.00	0.00	-0.00
	(2.85)	(1.80)	(2.05)	(0.82)	(-1.60)	(-0.43)	(1.67)	(0.06)	(0.57)	(0.89)	(-0.27)
Number of Firms	2,093	2,093	2,093	2,093	2,093	2,093	2,093	2,093	2,093	2,093	2,093
Adjusted R-squared	0.12	0.06	0.08	0.02	0.01	0.00	0.14	0.05	0.05	0.01	0.01

Panel C: RE proxy #3: Dummy variable if firms have "data security" related media news pre-GDPR

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)
VARIABLES	ΔCyber Awareness DEF14A	ΔCyber Count DEF14A	ΔExp BoD	ΔExp Aud Comm	ΔExp Risk Comm	ΔExp Tech Comm	ΔMon BoD/ Comm	ΔMon BoD Only	ΔMon Aud Comm	ΔMon Risk Comm	ΔMon Tech Comm
MediaCov	0.02	0.31**	0.02	0.00	0.00	-0.00	-0.02	-0.02**	0.00	0.00	-0.01
	(0.77)	(2.51)	(1.22)	(0.60)	(0.91)	(-0.62)	(-0.93)	(-2.09)	(0.14)	(0.31)	(-0.46)
Number of Firms	2,093	2,093	2,093	2,093	2,093	2,093	2,093	2,093	2,093	2,093	2,093
Adjusted R-squared	0.12	0.06	0.08	0.01	0.01	0.00	0.14	0.05	0.05	0.01	0.01

Panel D: RE proxy #4: Firm's CAR

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)
VARIABLES	ΔCyber Awareness DEF14A	ΔCyber Count DEF14A	ΔExp BoD	ΔExp Aud Comm	ΔExp Risk Comm	ΔExp Tech Comm	ΔMon BoD/ Comm	ΔMon BoD Only	ΔMon Aud Comm	ΔMon Risk Comm	ΔMon Tech Comm
CAR	-0.15**	-0.44***	-0.11**	-0.04**	-0.00	0.01	-0.01	0.01	-0.01	-0.03*	-0.01
	(-2.56)	(-2.66)	(-2.27)	(-2.03)	(-1.44)	(0.83)	(-0.15)	(0.42)	(-0.32)	(-1.79)	(-0.74)
Number of Firms	2,093	2,093	2,093	2,093	2,093	2,093	2,093	2,093	2,093	2,093	2,093
Adjusted R-squared	0.12	0.05	0.08	0.02	0.01	-0.00	0.14	0.05	0.05	0.01	0.01

Notes:

This table examines whether the GDPR's impacts on the changes in corporate boards' cyber awareness, expertise, and monitoring assignment vary based on companies' ex ante risk exposures (RE). We use four RE proxy variables, illustrated in the titles of Panel A to Panel D. In all regression analyses, we control for the same set of control variables and industry fixed effects as in Table 2, Panel B at the end of 2014. Further, we control for the pre-GDPR period board cyber awareness, expertise, and monitoring to capture the mean reversal effects. Refer to Appendix 1 for variable definitions and data sources. Robust t-statistics are reported in parentheses. *, **, and *** represent significance levels of 0.10, 0.05, and 0.01 respectively.

TABLE 7

Changes in corporate boards' cyber focus, expertise, and monitoring assignment and firm's subsequent cyber risks

Panel A: Changes in boards' cyber focus, expertise, and monitoring assignment and firms' subsequent cyber-attacks/data breaches

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)
Dependent Variables	Subsequent Cyber-attack/Data Breach (**Incidence**)										
Independent Variables	ΔCyber Awareness DEF14A	ΔCyber Count DEF14A	ΔExp BoD	ΔExp Aud Comm	ΔExp Risk Comm	ΔExp Tech Comm	ΔMon BoD/ Comm	ΔMon BoD Only	ΔMon Aud Comm	ΔMon Risk Comm	ΔMon Tech Comm
Probit Model	-0.60***	-0.25***	-0.22*	-	-	-0.41**	0.30	-0.40**	-0.27	-0.27**	-0.31***
	(-5.30)	(-4.12)	(-1.77)			(-2.15)	(0.81)	(-2.18)	(-1.54)	(-2.44)	(-2.98)
Number of Firms	1,862	1,862	1,862	NA	NA	1,862	1,862	1,862	1,862	1,862	1,862
Pseudo R-squared	0.30	0.30	0.29	NA	NA	0.29	0.29	0.29	0.29	0.29	0.29
Logit Model	-1.62***	-0.69***	-0.77**	-	-	-1.28**	1.16	-0.83**	-1.00*	-0.85**	-0.86***
	(-5.14)	(-4.02)	(-1.98)			(-2.08)	(1.05)	(-1.99)	(-1.74)	(-2.07)	(-2.65)
Number of Firms	1,862	1,862	1,862	NA	NA	1,862	1,862	1,862	1,862	1,862	1,862
Pseudo R-squared	0.31	0.31	0.30	NA	NA	0.29	0.30	0.29	0.30	0.29	0.29

Panel B: Changes in boards' cyber focus, expertise, and monitoring assignment and subsequent media attention on data security

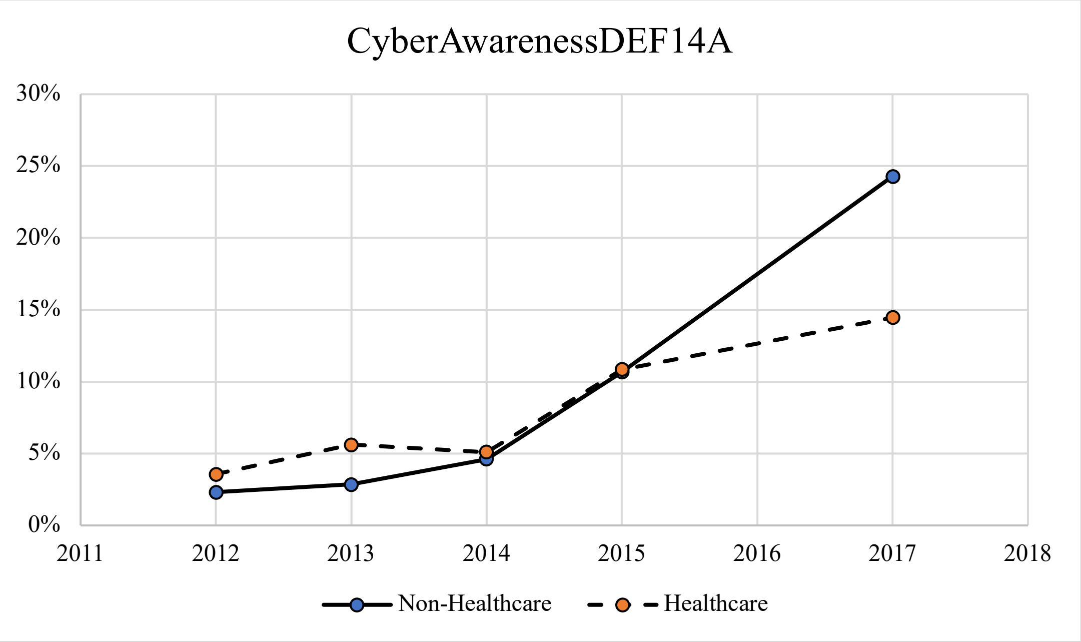
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)
Dependent Variables	Subsequent Media Attention regarding Data Security (***Media Attention***)										
Independent Variables	ΔCyber Awareness DEF14A	ΔCyber Count DEF14A	ΔExp BoD	ΔExp Aud Comm	ΔExp Risk Comm	ΔExp Tech Comm	ΔMon BoD/ Comm	ΔMon BoD Only	ΔMon Aud Comm	ΔMon Risk Comm	ΔMon Tech Comm
Poisson Model	0.74	0.01	0.06	0.57	-1.72***	-5.50***	-0.41	1.55**	1.02	-0.34***	-3.56***
	(1.18)	(0.32)	(0.33)	(0.74)	(-3.78)	(-9.47)	(-1.17)	(2.05)	(1.38)	(-2.82)	(-3.61)
Number of Firms	1,969	1,969	1,969	1,969	1,969	1,969	1,969	1,969	1,969	1,969	1,969
Pseudo R-squared	0.46	0.44	0.44	0.44	0.44	0.62	0.45	0.49	0.46	0.49	0.55

Notes:

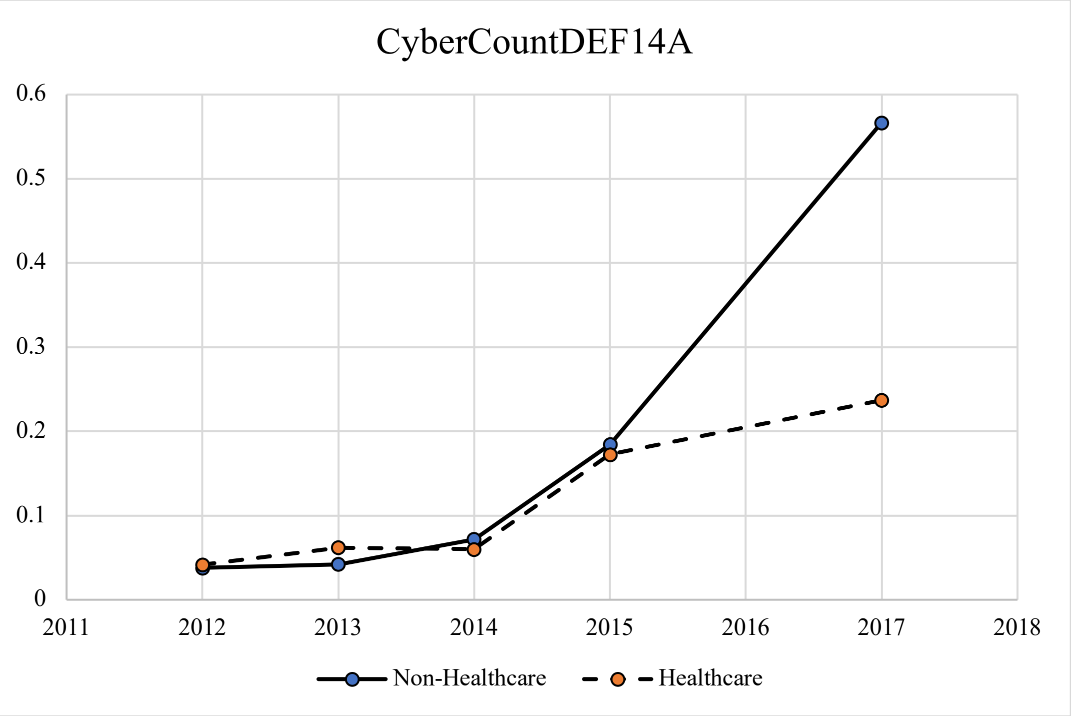
This table examines whether the changes in corporate boards' cyber focus, expertise, and monitoring assignment have any economic consequences. In Panel A, we regress firms' subsequent cyber-attack /data breach incidence over the years 2017-2019 on the changes in corporate boards' cyber focus, expertise, and monitoring assignment from the pre-GDPR period to the post-GDPR period (i.e., our dependent variable in Tables 5 and 6) using different models. In Panel B, we conduct the same regression analysis, but using the subsequent media attention between 2017 and 2019 as the output variable. In both panels, we control for *Size*, *Big Four*, *InstOwn*, *ICW*, *Leverage*, *BoardSize*, *%IndDir*, and *PaidCashDiv* at the end of 2016. We also control for the cyber-attack/data breach incidences in 2015 and 2016 in Panel A and the number of media articles regarding data security between 2012 and 2014 in Panel B. We do not include the industry fixed effects in either panel to avoid the incidental parameter bias in non-linear panel models. Refer to Appendix 1 for variable definitions and data sources. Robust t-statistics are reported in parentheses. *, **, and *** represent significance levels of 0.10, 0.05, and 0.01 respectively.

Figure 1 Parallel trend analysis for the difference-in-differences test of GDPR's impact on corporate boards' cyber focus, expertise, and monitoring

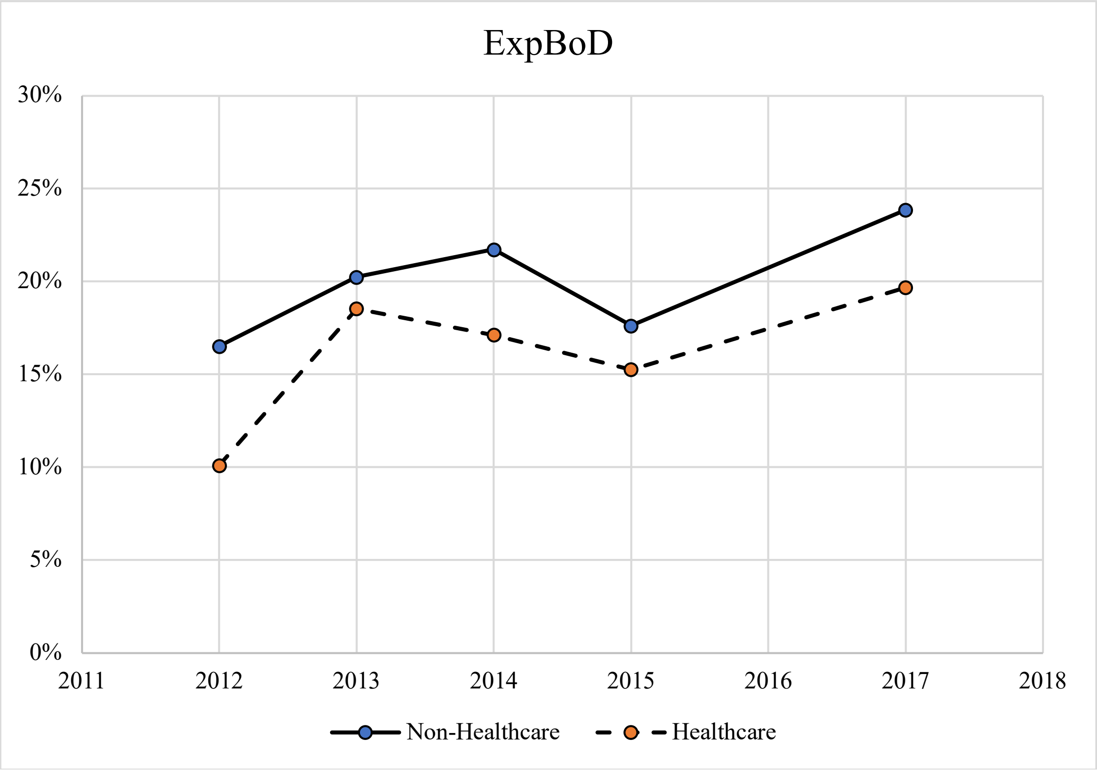
Panel A: Percentage of firms having corporate boards' awareness of cyber issues for non-healthcare vs. healthcare firms



Panel B: Average number of "cyber" keywords per firm in DEF 14A for non-healthcare vs. healthcare firms



Panel C: Percentage of firms having board directors with cyber/IT expertise for non-healthcare vs. healthcare firms



Panel D: Percentage of firms assigning cyber risk monitoring to corporate boards and committees for non-healthcare vs. healthcare firms

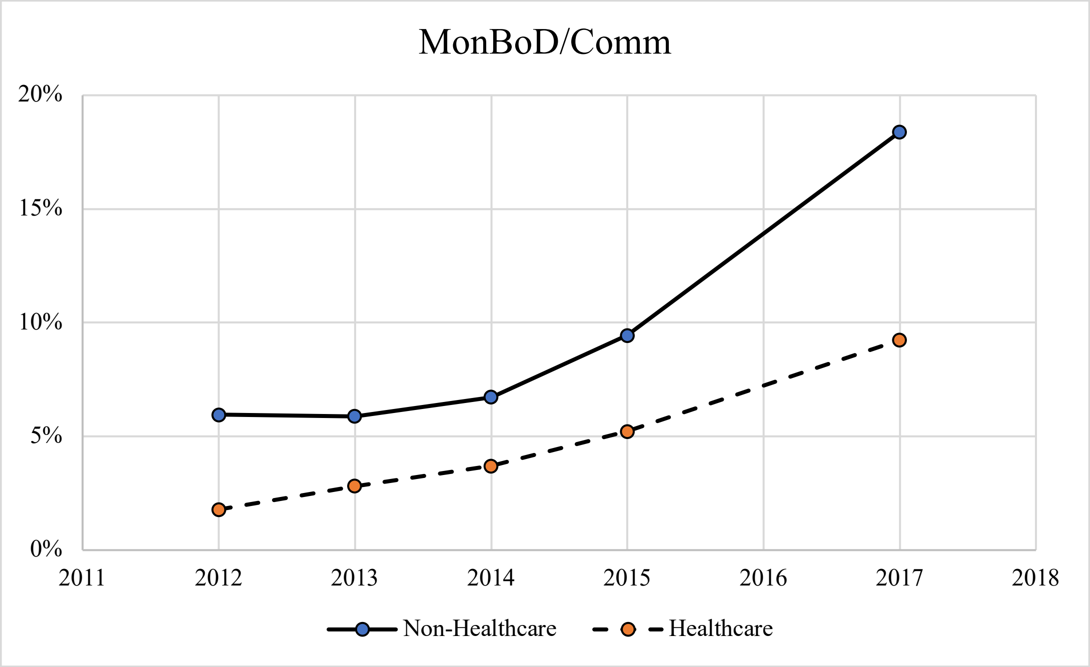
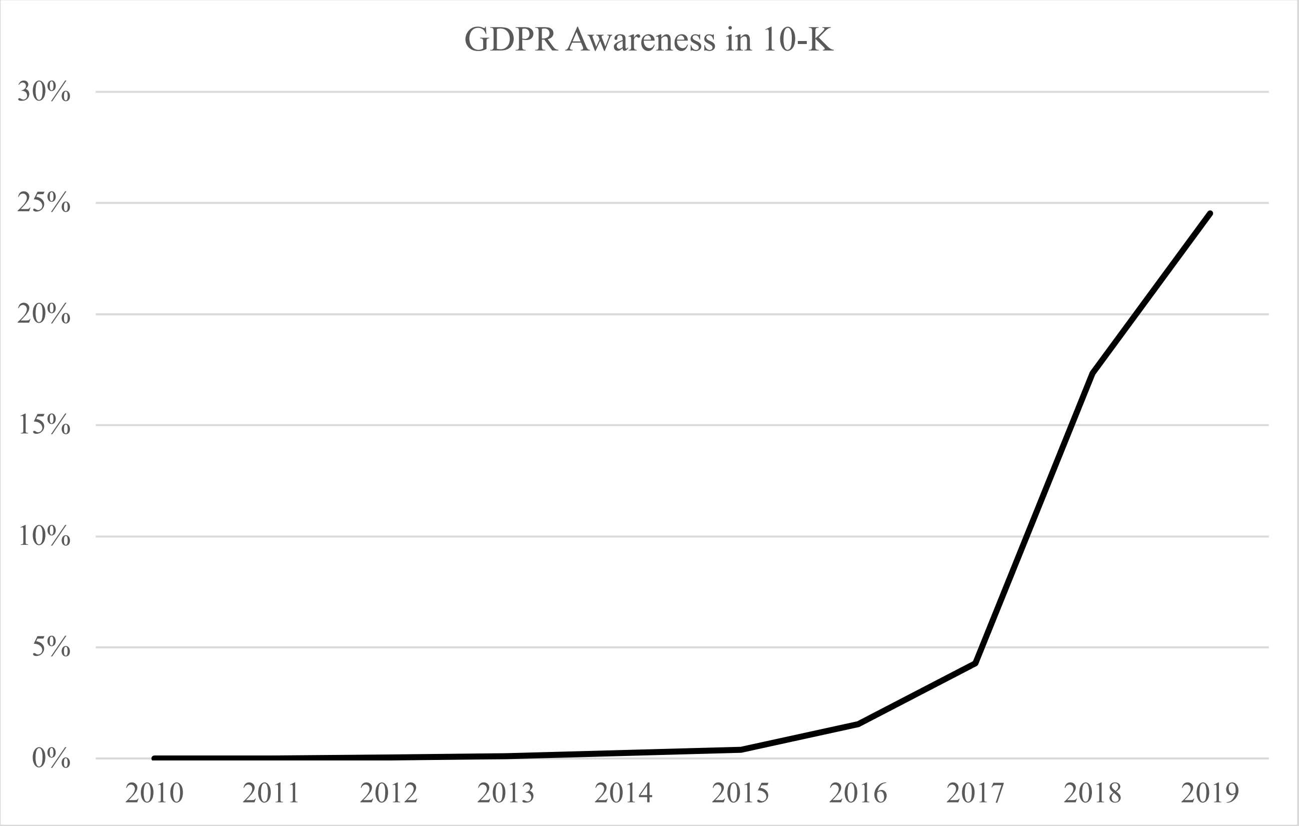


Figure 2 Percentage of firms mentioning “GDPR” or “General Data Protection Regulation” in their 10-K reports


GDPR Awareness in 10-K