The Current State of Cyber Insurance and Regulation in the Context of Investment Efficiency and Moral Hazard: A Literature Review

Asligul Erkan-Barlow
Brenda P. Wells-Dietel

Widespread use of internet and computer networks exposes businesses to a new type operational risk, cyber risk, which needs to be managed diligently. Efficacy of cyber risk management depends on both allocating sufficient resources to mitigate and utilizing cyber insurance policies to transfer this risk. While the cost of cybersecurity investments reflected in a firm's short-term earnings immediately, the prevention benefits are difficult to quantify and spread over a long period. Managers, who are compensated heavily with stocks and stock options, have financial incentives delay investments in data security to report higher short-term earnings. Most board directors lack the tecnical expertise to monitor top management team's cybersecurity-related decisions and alleviate such myopic behavior. As a corollary, firms rely heavily on insurance policies to manage cyber risk in today's digital economy.

Although the increase in the number of insurers and premiums written suggests growth in the industry, cyber policies represent less than one percent of the insurance market. The increase in loss ratios, the decrease in available limits, and the implementation of more restrictive coverage suggest that it is getting more difficult to find cyber insurance and customers have to pay more for less coverage. More than half of all cyberattacks target small and medium size firms with almost sixty percent of them having to close their doors within six months of experiencing an incident. Since these firms not only create tax revenue but also supply products and services and provide jobs in their local communities, cyberattacks not only threaten their existence but also have severe consequences for consumers, wage earners, and the entire economy.

There are regulatory frameworks both in the United States and even more stringently in the European Union. These attempts, however, seem to fail negating the increasing trend in the number of cyberattacks. This study contributes to the cybersecurity literature and practice in several ways. First, it provides the most recent and comprehensive review of the different strands of cybersecurity literature. Second, it evaluates the current state of the cyber insurance market and elaborates on the issues related to the offering of these high-risk and expensive policies from the perspective of both insurance providers and customers. Third, we observe the current state of the regulatory environment both in the United States and in the European Union. In conclusion, we argue that a socially optimal level of regulation is needed but yet to be enacted to govern security in cyberspace, to reduce the cyber risk exposure of businesses and insurers, and to protect consumers and the overall economy.

The Current State of Cyber Insurance and Regulation in the Context of Investment Efficiency and Moral Hazard: A Literature Review

Asligul Erkan-Barlow
Brenda P. Wells-Dietel[1]
Department of Finance & Insurance
College of Business
East Carolina University

ABSTRACT

This manuscript systematically reviews several strands of literature on cybersecurity and draws attention to the possible moral hazard problem associated with managers' choices on information security-related investments. First, a careful synthesis of the literature shows that managers have incentives to behave myopically and to defer investments in data security to meet the financial market's earnings expectations. Second, although adequate cyber risk management involves both risk mitigation and risk transfer, risk transfer through the purchase of cyber insurance is problematic. Despite the increase of insurers and written premiums suggesting growth in the cyber insurance industry, the most recent industry reports point out the increase in loss ratios, the decrease in available cyber insurance limits, and the implementation of more restrictive coverage as a sign of insurers controlling their risk exposure. Finally, existing regulatory frameworks in the U.S. and the European Union (EU) do not negate the trend of increasing numbers of cyberattacks. In conclusion, we argue that an optimal level of regulation is needed but has yet to be enacted to reduce the cyber risk exposure of businesses and insurers, as well as to protect consumers and the overall economy.

JEL Classification: G21, G32

Keywords: Cybersecurity, cyberattacks, bank profitability, bank ownership, bank size

1. Corresponding author

Introduction

Companies across industries have been using e-commerce at an increasing rate. While digital economy participants benefit from accessing larger consumer markets and increasing sales, they also collect and analyze their customers', suppliers', and employees' personal information to successfully maneuver their operations in cyberspace. Consequently, data have become one of the most valuable business assets to be managed and stored securely, making firms' computer networks vulnerable to cyberattacks. Thus, today's digital economy exposes all participants to a new type of operational risk, namely cyber risk. Cyber risk is a difficult-to-quantify risk category where the perception of risk diverges from the reality of risk (Eling & Zhu, 2018). An example of a cyber risk is a data breach, upon which the breached organization must warn those whose data was compromised and take steps to mitigate loss from the breach.

Allocating sufficient financial resources to cyber risk management depends on the cost-and-benefit analysis (Gordon & Loeb, 2002; 2006a). This task is challenging since cyberattacks' probability, timing, and severity involve high uncertainty (Schneier, 2008; Farahmand et al., 2013). This study focuses on the current state of cyber insurance and regulation. Specifically, we provide insights on cyber risk mitigation by investing in cybersecurity, risk transfer by purchasing cyber insurance, the problems associated with these two methods, and the potential role of regulatory intervention in alleviating these problems.

The unique cost-benefit aspect of cybersecurity investments (Chai et al., 2011) makes justifying the measurable and explicit monetary costs against the immeasurable and implicit prevention benefits difficult (Kwon & Johnson, 2014; Benaroch, 2018). As a result, managers are likely to underinvest in cybersecurity (Gordon et al. 2003a) and increase firms' cash holdings to combat tangible and intangible costs after experiencing a cyberattack (Garg, 2020). From an agency theory perspective, incentive alignment can explain managers' reluctance to invest in cybersecurity (Farahmand et al., 2013). For example, stock- and option-based compensation encourage executives to behave myopically and postpone long-term investments to meet shareholders' short-term earnings expectations (Stein, 1989; Bebchuk & Stole, 1993; Graham et al., 2005; Ladika & Sautner, 2020). These incentives may also influence the decision to invest in cybersecurity since cyber events are random, and prevention benefits may or may not materialize.

The empirical evidence presented in the literature regarding the stock market's reaction to cyberattacks supports this argument. For example, Gordon et al. (2011) show that investors penalize firms more harshly when a cyberattack interrupts operations than when it compromises customer information. Chai et al. (2011) also document that investors reward firms more generously when cybersecurity investment aims to increase sales over improving information technology security. The lack of investor sentiment toward cyberattack announcements, combined with the motivation of executives to increase their wealth, results in cyber insurance emerging as a viable hedging strategy to mitigate this specific risk. Cyber risk is partially alleviated with the purchase of cyber liability insurance. However, traditional liability policies, such as the general liability form, do not provide adequate coverage for cyber-related losses.

Cyber liability insurance evolved from general liability insurance in the 1990s. By 2010, it had become mainstream and evolved to include both first-party and third-party losses. There are up to 15 separate insuring agreements in a cyber policy, with claims normally involving multiple insuring agreements (Coalition, 2023). Cyber insurance forms are not standardized and vary from carrier to carrier (Coalition, 2023). There are at least three problems associated with this method.

First, the insurability of cyber risk may be problematic due to the interconnected nature of information security systems in cyberspace (Ogut et al., 2011; Beiner et al., 2015; Eling et al., 2020). All firms adopt standard technologies, making them vulnerable to the same incidents (Baer & Parkinson, 2007). Cyber incidents may be highly correlated between firms, violating the independence condition to insure against any risk (Ogut et al., 2011; Beiner et al., 2015). As a result, cyber insurance policies are high-risk products, which makes them challenging for insurance firms to price.

Second, cyber insurance providers face adverse selection and moral hazard problems that stem from information asymmetries (Gordon et al., 2003b; Beiner et al., 2015). There is a strong possibility that firms with higher exposure to cyber risk and weaker information systems security will obtain cyber insurance. Also, being insured may exacerbate managers' myopic behavior and allow them to focus more on damage control if and when they experience a breach instead of allocating funds to prevent such a random event. This approach may render firms' computer networks even more vulnerable to cyberattacks and increase the likelihood of experiencing a breach. Insurance companies attempt to combat these problems by requiring upfront cyber risk assessment, which increases insurance costs. They also set high deductibles and low coverage limits to hold insured firms accountable for their risk prevention practices. These mechanisms, however, reduce the value of purchasing insurance.

Finally, cyber insurance contracts may not cover all losses after a firm experiences a data breach. Firms may suffer indirect and intangible losses such as litigation expenses and reputational losses for years after a cyberattack. As a result, firms do not have incentives to invest in risk prevention or transfer risk, which renders their cyber risk management inefficient. Instead, firms increase their cash holdings and liquidity several years after experiencing a cyber incident to be prepared for unforeseen expenses (Boasiako & Keefe, 2020; Garg et al., 2020). Shareholders do not penalize firms for inadequate risk management since they can lower their cyber risk exposure by holding a diversified portfolio of assets. In this scenario, firms' customers are the only stakeholders with higher exposure and less protection against the risk of having their personal information compromised, and they bear the most severe consequences. For example, in 2017 alone, 158 million social security numbers were exposed, due to which victims were denied credit cards and loans, experienced increases in the interest rates on their existing credit cards, and were unable to get a job or lost a current position (Identity Theft Resource Center, 2017).

As the negative consequences of cyberattacks expand to public and government security, some regulatory attempts aim to prevent these events and protect personal information. The European Union (EU) has adopted the General Data Protection Regulation (GDPR), which is considered the most harmonic and stringent law and much superior to the existing regulations in the U.S. On the other hand, the federal

government in the U.S. introduced a new public law in 2017 to provide local and state officials, law enforcement officers, prosecutors, and judges with education on cyber and other related crimes, as well as methods for investigation and responding to cyberattacks.[2] In 2018, all 50 states and the District of Columbia passed legislation requiring private and government entities to inform the public about cyberattacks.[3] Moreover, the New York State Department of Financial Services (DFS) cybersecurity regulation, which requires financial institutions to implement a cybersecurity program, became effective in 2017. The U.S. Securities and Exchange Commission's (SEC's) Office of Compliance Inspections and Examinations announced its *Cybersecurity and Resiliency Observations* report in 2020. This report discusses the importance of information security for the integrity of financial markets and customers' data protection while drawing attention to the role of corporate boards and senior executives in developing and conducting risk management strategies and governance measures.

Although these attempts show that the regulatory agencies recognize cybersecurity as a significant threat, their guidelines are not obligatory except for the disclosure requirement when a cyberattack occurs. From a regulatory standpoint, firms are encouraged to follow guidelines to develop and implement cybersecurity programs and to make announcements when they experience a breach. Understandably, over-sharing information regarding cybersecurity practices may render firms' computer networks vulnerable to cyberattacks. In the current state, however, it is impossible to determine how much effort firms exert to prevent these incidents and how much they rely on insurance to transfer the risk. Market participants, especially consumers, are in the dark unless firms voluntarily share information, especially after a data breach.[4] In this study, we join prior researchers and propose that an optimal regulatory intervention is needed to ensure information security in cyberspace (Ogut et al., 2011; Beiner et al., 2015; Lam, 2016; Eling et al., 2020).

Overall, this study makes several contributions to cybersecurity literature. First, to our knowledge, our manuscript provides the most recent and comprehensive review of the different strands of cybersecurity literature to point out possible moral hazard problems associated with cyber risk management. Second, we assess the current state of the cyber insurance market and discuss the issues related to offering these high-risk and expensive policies. Third, we observe the current state of the regulatory environment both in the U.S. and in the EU and assess the need for a socially optimal level of regulation to govern security in cyberspace. We argue that insurance companies, businesses, consumers, and the overall economy may benefit from a carefully designed cybersecurity regulation.

We discuss the economics of cyber risk and cybersecurity in the next section. Section 3 reviews the literature on market reaction to cyberattack announcements. Section 4 discusses the impact of information security breaches on firm outcomes.

2. The final version of the Strengthening State and Local Cyber Crime Fighting Act of 2017 became a public law on November 2, 2017.

3. National Conference of State Legislators lists the statewide breach disclosure laws on the following website: *https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx*.

4. Following a data breach in 2020, American International Group (AIG) did not provide many details and only stated in their 2021 annual report that they maintain cyber insurance and acknowledge cyber risk as another form of operational risk.

Section 5 elaborates on board governance issues around cybersecurity. Section 6 outlines issues that make purchasing and offering cyber insurance a challenge for firms and insurers. Section 7 observes the regulatory environment around the world and assesses the need for new regulations. Finally, Section 8 provides our concluding remarks and discusses the efficacy of proposed cyber regulation methods.

The Economics of Cyber Risk and Cybersecurity

Information security has become a growing concern in today's cyber economy since companies rely on digital transactions and possess extensive personal data, making their information systems susceptible to cyber incidents. Cyberattacks may have different motivations, such as unauthorized intrusions to access customer and employee information or using malware or ransomware to make the company website unavailable to customers (Cavusoglu et al., 2004). Furthermore, hackers may have political motivations or aim to attract negative attention to attacked firms (Goldman, 2012). While financial motives drive some attacks, some are caused by espionage (Lending et al., 2018). Regardless of the underlying motivation, cyberattacks cause substantial financial and reputational damage. TJX, a U.S. department store corporation, suffered $256 million in losses from a cyberattack in 2007 when hackers accessed more than 45 million credit and debit card numbers (Kerber, 2007). Losses from the attack included computer system repair, lawsuits and investigation costs, as well as other claims. Target Corporation reported a net expense of $17 million and a possible adverse effect on its sales in the fourth quarter of 2013, as well as civil lawsuits and investigations by state and federal agencies, after a cyberattack. Equifax, a consumer credit reporting agency, experienced a breach in 2017 that exposed the private information of 160 million accounts, costing the firm $700 million and lowered its value by $4 billion. The Colonial Pipeline, the most extensive pipeline system for refined oil products in the U.S., paid nearly $5 million in ransom to hackers who disrupted the firm's operations and the East Coast's fuel supply. In 2021, the cost of cyber crimes in the most affected 10 states alone was nearly $4 billion (Statista, 2022c).

As the traditional brick-and-mortar business model transformed into a "click-and-mortar" form (Cavusoglu et al., 2004), cyber risk is considered to be like other conventional operational risks that businesses were exposed to in the pre-internet era (Lanz, 2016). Specifically, cyber risk refers to the "operational risks to information and technology assets that affect the confidentiality, availability or integrity of information or information systems" (Beiner et al., 2015). Data breaches may occur for various reasons, such as the actions of insiders, failures of information technology (IT) systems or internal processes, or external events (Cebula and Young, 2010).[5] Among the five most common incidents experienced by U.S. companies only in 2021, network intrusions account for 56% of all cyberattacks, followed by phishing attacks at 24%,

5. Privacy Rights Clearinghouse categorizes data breaches into eight groups: UNKN (unknown or not enough information about the breach to know how exactly the information was exposed), CARD (fraud involving debit and credit cards not via hacking), STAT (stationary computer loss, which is lost, inappropriately accessed, discarded or stolen computer or server not designated for mobility), PORT (portable device or lost, discarded, or stolen laptop, PDA, smartphone, memory stick, CDs, hard drive, data tape), PHYS (physical: paper documents that are lost, discarded, or stolen), DISC (unintended disclosure not involving hack, intentional breach, or physical loss), INSD (insider or employee, contractor, or customer), and HACK (hacked by an outside party or infected by malware).

involuntary disclosures at 8%, systems failures at 7%, and stolen or lost physical devices or records at 5% (Statista, 2022a).

In response to the increased number and magnitude of cyber incidents, cybersecurity-related expenditures have also increased in the past few years. According to the Hiscox Cyber Readiness Report (2022), the mean cybersecurity spending among its respondents has been up 250% since 2019. Gartner (2021) shows spending on information security and risk management has grown worldwide from $133.8 billion in 2020 to $150.4 billion in 2021. Nevertheless, the number of cyber incidents also increased over the same period. Hiscox (2022) shows a 7% increase in U.S. firms reporting a cyberattack in 2021. Moreover, Statista (2022d) displays that cybersecurity spending increased from $27.4 billion in 2010 to $66 billion in 2018, and the number of cyber incidents increased from 662 to 1,175 (Statista, 2022b). These statistics suggest that firms spend more money on cybersecurity collectively but still experience cyberattacks, so they may not be allocating sufficient resources to the right IT assets. From a similar point of view, Weill and Ross (2004) emphasize the importance of prioritization and knowing how much and where to invest for effective IT governance.

Another notable fact related to information security investments is that cyber risk is a difficult-to-quantify risk category (Eling & Zhu, 2018). To manage this new business risk appropriately, managers must effectively assess cyber risk, adopt mitigations, and create recovery processes (Kumar et al., 2008; Sipes et al., 2016). Allocating financial resources to such cybersecurity activities depends on their cost and benefit aspects (Gordon and Loeb, 2002; 2006a). Nevertheless, cyber risk is the most common area where the perception of risk diverges from the reality of risk. The uncertainty regarding the severity, probability, and timing of cyberattacks (Schneier, 2008; Farahmand et al., 2013) makes it difficult to estimate the cost of data breaches. Even after spending on information security, cyber incidents may still occur due to intentional attacks and unintentional firm and customer behavior (Lee et al., 2011). Thus, quantifying the monetary benefit of investing in cybersecurity, which aims to prevent or minimize the damage that may arise only if a breach occurs, is difficult.

Unlike the implicit benefits of information security investments that may or may not occur later, the costs of these investments are explicit and immediate. For example, any capital expenditure on hardware, software, and people can be considered cybersecurity spending (Gordon and Loeb, 2006b). This unique cost-benefit aspect renders cybersecurity investment a challenge (Chai et al., 2011) for managers. Since managers cannot easily justify the tangible costs to both the firm and its customers (Lee et al., 2011) against the intangible benefits (Kwon and Johnson, 2014; Benaroch, 2018), they may defer cybersecurity investment until a cyberattack occurs (Gordon et al. 2003a). Consistent with this view, Lam (2016) shows firms underinvest in attack prevention and overinvest in damage control when the cybersecurity provider is responsible for all the damages. Overall, there are mounting concerns regarding the efficiency of investments (Srinidhi et al., 2015; Benaroch, 2018) and how firms use their limited cybersecurity budgets (Moore et al., 2015).

Market Reaction to Cyberattacks

We turn to the literature on market reaction to understand why managers might defer cybersecurity spending and possibly cause investment inefficiencies. Agency theory postulates that differences in risk preferences of insurance managers and investors cause a conflict of interest between the two groups. Investors generally tolerate higher risk since they can diversify idiosyncratic risk away (Rajgopal & Shevlin, 2002). Managers are risk-averse and reluctant to undertake risky projects because they cannot diversify firm-specific risk due to having human capital invested in the firm (Jensen & Meckling, 1976, Srinidhi et al., 2015). Thus, separating ownership and control may cause investment inefficiencies that could damage the firm's market value (Jensen & Murphy, 1990). Compensating managers with stocks and options (equity incentives hereafter) is considered a remedy for possible underinvestment problems. Giving managers fractional ownership in the firm may alleviate agency problems by aligning their interests with those of investors (Fama & Jensen, 1983; Core & Guay, 1999). This strategy, however, may fail because equity incentives in the compensation package make managers' wealth a function of their firms' stock price (Burns & Kedia, 2006).

Investors form their opinions about a firm by evaluating its current earnings (Stein, 1989). Firms face negative publicity (Bowen et al., 1995) and experience a decline in stock price (Ali & Kallapur, 2001; Skinner & Sloan, 2002) when they announce earnings that are lower than expected. Thus, managers are under pressure[6] to produce earnings that meet expectations because their wealth changes in response to stock price changes, making equity-based compensation a double-edged sword (Goldman & Slezak, 2006). To prevent unfavorable changes, managers may take excessive risks to maintain an upward trend in stock price, which may eventually destroy firm value, shareholder wealth, and image (Jensen, 2002). They may even distort their firms' financial performance to increase the market value to achieve personal gains (Collins & Hribar, 2000; Watts & Zimmerman, 1978). It is known that managers sometimes manipulate financial statements to exaggerate their firms' earnings (Cheng & Warfield, 2005; Bergstresser & Phillippon, 2006). More importantly, they may manage real activities by decreasing research and development (R&D), advertising, and maintenance expenditures, selling profitable assets, and postponing new projects (Herrmann et al., 2003; Cohen & Zarowin, 2010; Graham et al., 2005) to meet current earnings benchmarks at the expense of their firms' future value.

Managers may be facing a similar dilemma when making cybersecurity-related investment decisions. Not investing in cybersecurity, indeed, renders firms vulnerable to cyberattacks. Some empirical evidence suggests that investors react negatively to a firm's cyberattack announcements (Campbell et al., 2003; Cavusoglu et al., 2004; Goel & Shawky, 2009; Gatzlaff & McCullough, 2010). The adverse market reaction is stronger for internet firms (Hovav & D'Arcy, 2003) and firms with higher growth opportunities. Investors even seem to pay attention to how attacked firms announce this bad news. For example, Gaztlaff and McCullough (2010) show that investors react more negatively when breached firms refuse to provide details of the incidents. Thus, there is reason to believe managers would allocate sufficient funds to cybersecurity to

6. A 2017 National Association of Corporate Directors (NACD) survey points out that activist shareholders prefer and, therefore, pressure firms to focus on increasing short-term gains over long-term goals.

prevent attacks and avoid any loss in their firms' market value, which would negatively affect their wealth.

Indeed, a rational manager would invest in information security as long as the cost of the investment is less than the expected cost of a possible breach (Chai et al., 2011). However, determining what is sufficient when investing in cybersecurity is problematic because it is difficult to estimate the probability of these attacks and their cost (Schneier, 2008). Another challenge associated with these investments is justifying their cost when their benefit is uncertain. First, calculating the return on information security investment is difficult due to data limitations (Chai et al., 2011). Second, cyber incidents may still occur even after firms undertake such investments (Lee et al., 2011). Moreover, cybersecurity investment requires allocating financial resources, which will reduce reported earnings immediately. Knowing investors are not fond of declining profits, managers may gamble and defer cybersecurity investments until after a breach occurs instead of taking a guaranteed hit on their wealth.

Furthermore, the market seems to be getting more insensitive to cybersecurity incidents over time (Gordon et al., 2011; Yayla & Hu, 2011). Although earlier studies document significant negative reaction to breach announcements, more recent empirical evidence yields contradicting results (Yayla & Hu, 2011). For example, Gordon et al. (2011) find that investors' negative reaction to cyberattack news was not statistically significant after 2002. Even before then, investors penalized firms more harshly when a cyberattack involved interrupting the firm's operations than when it compromised customer information. Investors reward firms more generously when the goal of cybersecurity investment is to increase sales than to improve IT security (Chai et al., 2011) and when firms are early adopters of new security measures (Bose and Leung, 2013). Moreover, Hinz et al. (2015) document that although there is a decline in the stock prices of attacked companies in the short term, the market's perception of systemic risk remains unaffected in the long term. In fact, investors may not be the only group getting insensitive to cyber incidents. Mikhed and Vogan (2018) show that bank customers adopt their own security measures, but they do not change their credit usage. These findings suggest that managers, whose compensations include short-term incentives that tie their wealth to their firm's stock price, have personal motives to defer cybersecurity investments to meet investors' higher earnings expectations. Managers may maintain this approach until a cyberattack occurs since empirical evidence shows declining market sensitivity to data breach announcements.

Firm Reaction to Cyberattacks

The discussion in the previous section points out a possible decline in shareholders' sensitivity to cyberattacks. Kamiya et al. (2020) state that shareholders are aware that firms in which they are investing are exposed to cyber risk and may experience attacks. Therefore, there is a level of readiness regarding cyber incidents, which may alleviate investors' adverse reactions. Consistent with this view, Kamiya et al. (2020) argue that financially stable firms should not suffer reputational damage even when a cyberattack occurs as long as the losses are not more significant than what they and their investors expected. Firms indeed face tangible costs, such as informing customers after an attack, marketing, and advertising expenses to restore their public

image, and legal fees if sued. Moreover, firms may face other less visible costs, such as increases in insurance premiums and interruptions in their operations. Firms must position themselves financially since they will pay for these expenses if they experience an attack.

Covering these expenses using external resources may not be feasible since firms may be subject to higher financing costs due to increased risk levels, especially after data breach disclosure laws are passed in their states (Boasiako & Keefe, 2020). Supporting this notion, Kamiya et al. (2020) find that breached firms face higher cash flow volatility, a probability of a decrease in their credit rating, and an increased likelihood of bankruptcy. The empirical evidence Garg (2020) presented shows that firms adjust their financial policies by increasing their cash holdings for up to three years after they experience a cyberattack. Garg (2020) documents a spillover effect where unbreached firms also increase their cash levels when a peer firm in the same industry or its unlisted subsidiary has been attacked. Boasiako and Keefe (2020) provide similar conclusions about firms' liquidity after their states pass disclosure laws or when they experience a breach. Furthermore, the authors show that firms reduce external financing, capital expenditures, and acquisition costs.

These findings collectively suggest that firms adjust several financial policies, such as liquidity management, capital budgeting, and capital structuring. Unfortunately, these financial policy adjustments are not the only consequences breached firms face. Lending et al. (2018) document an approximately 6% decline in sales of nonbanks and a 10% decline in bank deposits. The impact of a breach on the deposit levels of banks becomes especially dramatic upon a significant breach and a financial breach with a 24% and 14% decline, respectively. Kamiya et al. (2020) also find an adverse effect on large firms' sales growth. Interestingly, the authors document a minimal decline in accounting performance which is only a 0.9% decline in the return on assets (ROA) ratio and a 0.7% decline in the cash flows to assets ratio of large banks but not for their overall sample.

These outcomes are consistent with those of an earlier study, where Ko and Dorantes (2006) show the only significant decline in ROA is in the third quarter following a breach. These results imply that although the top lines of income statements of breached firms suffer more than their bottom lines. Moreover, Ko and Dorantes (2006) document a significant increase in sales of breached firms in the second, third, and fourth quarters following a breach of 8%, 4%, and 2%, respectively. Unbreached firms in their sample do not experience a significant increase in revenues over the same period, suggesting that breached firms eventually catch up with their peers. These findings, however, might be due to attacked firms passing on breach-related costs to their customers. For example, Huang et al. (2023), in an article published by Harvard Business Review, found that 60% of breached firms have increased their prices. Thus, firms that have experienced cyberattacks may find ways to increase their revenues and protect their profits. Although this approach may create an image that encountering a data breach does not significantly burden a firm financially, it is at the expense of consumers who suffer price increases.

Role of Board Governance for Effective Cyber Risk Management

The discussions in the previous two sections portray that the lack of significant long-term impact of cyberattacks on firms' market and accounting performances allows managers to defer cybersecurity investments. Managers execute the deferral decision by cutting cyber spending to maintain an upward trend in stock price by catering to investors' short-term earnings expectations. Ladika and Sautner (2020) argue that managers act in a short-termism way because they can extract personal benefits by selling their equity holdings in the short term without facing the consequences of their investment decisions in the long term. Such myopic behavior is how the moral hazard problems surrounding cyber risk management and security investments manifest themselves in managerial actions. Agency theory appoints the board of directors as a governing mechanism that can monitor managers and alleviate their tendencies to act in their best self-interests. Consequently, corporate boards should hold top executives accountable for overseeing cybersecurity at their organizations (Rai & Mar, 2014).

Although cyberattacks are of low frequency and high severity (Lee et al., 2011), they are becoming more frequent with even more severe consequences. Since cybersecurity is a growing concern, mitigating cyber risk is beyond the responsibility of solely the IT department (Eling & Schnell, 2016; Rothrock et al., 2018). The entire enterprise requires a systematic approach, including the top managers and the board of directors (Rai & Mar, 2014). Therefore, the board of directors has a strategic role in managing cyber risk effectively. Consistent with this view, Hsu and Wang (2014) show that larger boards, older boards, and boards with some young directors are associated with a lower likelihood of experiencing cyberattacks, benefiting from the diverse organizational and technological know-how. Interestingly, Lending et al. (2018) find that firms whose boards have more financial expertise[7] are less likely to be breached. This result suggests that boards with more financial expertise may assess the costs and benefits of cybersecurity projects more adequately and lead their firms to more productive investments.

According to popular opinion, firms may avoid cyberattacks when corporate boards ensure executives take cyber risk management seriously. Even the most sophisticated information technologies may fail if firm insiders design operating procedures defectively and are careless about the security procedures within their organizations (Dutta & McCrohan, 2002). For instance, Kamiya et al. (2020) document that the consequences of experiencing a cyberattack are not as severe when boards pay attention to enterprise risk management.[8] On the contrary, firms are more likely to experience data breaches when their boards are busy and do not pay much attention to the subject matter (Lending et al., 2018). Vigilant boards may still harm cybersecurity efficacy if they do not pay special attention to cyber risk management. Kwon et al. (2013) and Lending et al. (2018) find that a larger fraction of independent directors on the board, a standard measurement of board governance strength, is associated

7. Lending et al. (2018) measure board financial expertise as the number of directors on a board who are classified as financial experts.

8. Kamiya et al. (2020) measure board attention risk management using an indicator variable that takes value of one if there is a specific board risk committee.

with a higher possibility of a security breach. Therefore, the board's attention to cybersecurity is far more critical than its monitoring strength alone.

Despite their strategic role, board directors believe that cyber risk is one of the most challenging risks they expect to oversee.[9] Since most directors lack the technical background to handle IT-related issues (Tieman, 2011), they need adequate cybersecurity training (Rothrock et al., 2018), which requires having access to expert opinion and meeting with the IT personnel or executives more frequently (Rai and Mar, 2014). Empirical evidence shows that the involvement of an IT executive in senior management reduces the likelihood of experiencing cyberattacks (Kwon et al., 2013). However, chief information technology officers (CIOs) have similar compensation structures to other top executives. The equity incentives in CIO compensation put them under the same pressure to meet investors' expectations and cause them to cut IT investments to report higher earnings (Turedi & Erkan-Barlow, 2022). Although independent directors on the board do not alleviate this myopic behavior, CEO duality[10] exacerbates it (Turedi & Erkan-Barlow, 2022). These findings suggest that strong corporate governance is necessary but not sufficient alone to achieve effective cyber risk management and investments. Even stringent boards require IT training and special attention to risk management.

Cyber Insurance and the Role of Cyber Insurers

The substantial cost of cyberattacks to the customers of attacked firms and the entire economy requires firms to adopt adequate cyber risk management (CRM) processes. CRM involves applying risk mitigation and transfer methods (Gordon et al., 2003b; Eling et al., 2020). As the previous two sections outline, top managers are compensated with short-term incentives and use their discretion to postpone cybersecurity investments. At the same time, the board of directors needs more technical experience to deal with cybersecurity-related decisions. Moreover, the public good character of cybersecurity contributes to the underinvestment problem (Eling & Schnell, 2016). Individual firms use standard technologies and have computer systems interconnected with other firms (Ogut et al., 2011). As cybersecurity exhibits positive externalities since one firm's investment utility depends on all firms' investments, individual firms are reluctant to invest in risk mitigation processes (Beiner et al., 2015). Consequently, firms resort to cyber insurance policies to manage cyber risk and hedge against potential losses from an information security breach (Gordon et al., 2003b).

On the one hand, obtaining cyber insurance can benefit the firm. First, cyber insurers require an upfront risk assessment which, in return, may increase firm awareness of cybersecurity and encourage self-protection. A cyber resiliency score (CRS) is one way to evaluate how prepared a firm is to handle cyber attacks. Insurers calculate these scores based on data supplied by the insured and scans of the firm's computer system. These scans can find "holes" or other access points that outsiders can penetrate. A

9. According to a survey by the NACD, 41% of board members said the cybersecurity threats will have the greatest effect on their company in the next year. The 2017-2018 NACD Private Company Governance Survey can be found at *https://www.nacdonline.org/analytics/survey.cfm?ItemNumber=60038*.

10. CEO duality is a status when the CEO of the firm is also the chairperson of its board. CEO duality gives the CEO more authority, weakening the strength of board monitoring (Boyd, 1994).

resiliency score can help a firm measure and strengthen its cyber hygiene (Immersive Labs, 2023). Although cyber insurance policy premiums are often expensive (Beiner et al., 2015), firms may lower the cost by adopting risk assessment and mitigation processes within their organizations (Baer & Parkinson, 2007). Furthermore, insurers may encourage appropriate risk management by requiring deductibles that hold firms accountable for some losses when a cyber incident occurs (Gordon et al., 2003b; Ogut et al., 2011). On the other hand, managing cyber risk by transferring it to an insurer is challenging for several reasons. Among other factors, the extant research points out that the randomness of the cyber incidents, the information asymmetry involved with these adverse events, and the limited coverage of cyber insurance policies are noteworthy.

Probability, Severity, and Randomness of Cyber Incidents

Cybersecurity is an area where the perception of security may diverge from the reality of security due to the likelihood of incidents and the severity of the damage they may cause (Schneier, 2008; Farahmand et al., 2013). Even though the potential losses are incredibly high, the probability of experiencing a data breach is very low for individual firms (Lee et al., 2011). As a result, calculating the actuarial value of cyber insurance policies involves high uncertainty for insurance companies (Gordon et al., 2003b). Moreover, the existing information security systems across firms are designed using standard technologies, which render firms vulnerable to the same incidents (Baer & Parkinson, 2007). For example, according to the breached data provided by the Privacy Rights Clearinghouse (PRC), hackers were able to access Experian consumer information through the Bank of Jena, including name, address, date of birth, social security number, and account numbers in 2006. Bloomberg News reporters were able to access and retrieve login information from data-services clients, including Goldman Sachs and JP Morgan Chase in 2013. A programming error at ADP—a company offering online payroll and HR solutions—exposed the names, social security numbers, and other W-2 information of U.S. Airways, McKesson, and City of Houston employees in 2013. In 2017, USA Hoist Company, Mid-American Elevator Company, and Mid-American Elevator Equipment Company experienced a ransomware attack due to using the same server for store employee and vendor information. According to Biener et al. (2015), the independence of threats is necessary to provide insurance against any specific risk. The interconnectedness of computer systems, however, violates this independence requirement (Ogut et al., 2011). Consequently, the low probability, high severity, and high correlation of cyber incidents make pricing cyber policies challenging.

Information Asymmetry

Another factor contributing to the difficulty in cyber insurance pricing is information asymmetry. Unlike common perception, insurance providers do not have an information advantage over individual firms (Bandyopadhyay et al., 2009). Firms that have experienced or have a higher probability of experiencing a cyberattack are more likely to purchase cyber insurance based on some private information that is not available to the insurance provider at the time of contracting (Gordon et al., 2003b; Biener et al., 2015). Insurance companies may alleviate this adverse selection problem

by categorizing firms into risk groups and requiring higher premiums for higher-risk insurance users. The lack of data makes this categorization a challenging task for insurers. As a result, insurance companies often require information security audits at individual firms (Gordon et al., 2003b). An extensive cyber risk assessment before offering a policy increases firms' awareness and may improve their risk mitigation efforts (Biener et al., 2015). However, such risk assessment increases the upfront cost and makes obtaining cyber insurance even more expensive for firms.

In addition to adverse selection, moral hazard constitutes a problem for insurance companies, insured firms, and stakeholders such as customers, suppliers, and industry peers using the same computer networks. The moral hazard problem in the cybersecurity context refers to the insured firms' lack of incentives to exert self-protection and risk mitigation efforts to lower the probability of and the loss associated with experiencing an attack. Insurance providers hedge against this issue by requiring high deductibles (Gordon et al., 2003b) or setting low maximum coverage limits (Biener et al., 2015). These two mechanisms increase the potential liability of insured firms as they will be responsible for some of the costs once a cyber incident happens. In addition, while insured firms usually pay lower premiums when they adopt, maintain, and improve their self-protection measures (Baer & Parkinson, 2007; Eling et al., 2020), insurance providers may increase premiums once a data breach happens (Deloitte, 2016).

Indeed, insurance companies aim to provide monetary incentives for firms to take risk mitigation measures that would lower the likelihood of a breach occurring. Adjusting deductibles and coverage limits, however, may reduce the perceived value of insurance for firms. Furthermore, changing premiums may be an inadequate incentive for firms. Due to the interrelatedness of information security systems and the accumulation of cyber risk, several insured firms may be affected by the same cyberattack (Eling et al., 2020). The benefit derived from investing in cybersecurity for an individual firm is a function of all other firms' awareness and investments in cybersecurity (Biener et al., 2015). As a result, what seems to be a monetary incentive might eventually discourage firms from improving their risk mitigation practices knowing that they may still get attacked and face a premium penalty.

Cyber Insurance Coverage

Insurance companies alleviate the high uncertainty by underwriting policies with high deductibles and low coverage, reducing the value of cyber insurance to firms seeking protection against losses (Biener et al., 2015). High premiums make cyber insurance unobtainable, especially for small- and medium-sized firms (Betterley, 2013). Moreover, the highly correlated nature of cyber risks among firms creates difficulty for insurers and insured firms. First, firms cannot promptly identify breaches and quantify losses due to the interconnectedness of information security systems (Ogut et al., 2011). Second, firms cannot prove their risk mitigation efforts to insurers since cyberattacks may still occur even after employing self-protection measures (Lee et al., 2011). Third, firms do not fully disclose their unique risk mitigation practices to maintain the effectiveness of their security systems since cyber intruders may use this information. Despite paying high premiums, firms often have difficulty receiving full compensation for their losses once a breach occurs (Ogut et al., 2011).

In addition to these factors, most commercial property and liability insurance policies protect against immediate damages to physical assets (Eling & Schnell, 2016). In contrast, firms may face a plethora of tangible and intangible costs following cyber incidents (Garg, 2020). The intangible costs include damage to the firm reputation, marketing, and advertising expenses to rebuild public relations, attorney and litigation fees in case of a lawsuit, disruptions in firms' operations, and loss of revenue (Deloitte, 2016). Cyber insurance policies usually do not cover these indirect costs that firms may incur when they experience a cyberattack. Wojcik (2012), for example, points out that firms may not always get insurance compensation when they lose proprietary information and trade secrets after a breach. Similarly, Gatzlaff and McCullough (2012) show that insured firms are not covered for the reputational damage they face. The intangibility of these costs makes the loss estimation problematic because they are hard to quantify and may occur years after experiencing a cyber incident.

Recent Developments in the Cyber Insurance Market

The problem of cyber risk is partially alleviated with the purchase of cyber liability insurance. However, traditional liability policies, such as the general liability form, do not provide adequate coverage for cyber-related losses. Cyber liability insurance evolved from general liability insurance in the 1990s, and it had become mainstream and evolved by the 2010s to include both first-party and third-party losses. Specifically, cyber insurance policies provide first-party coverage against losses that stem from various types of cyber incidents and third-party liability coverage for damages suffered by other entities (Coalition, 2023). There are up to 15 separate insuring agreements in a cyber policy, with claims typically involving multiple insuring contracts (Coalition, 2023). Cyber insurance forms are not standardized and vary from carrier to carrier. For example, some policies include notification and credit monitoring services when cyber incidents expose sensitive customer information such as credit card data, social security numbers, or medical data (Coalition, 2023). That said, these policies generally do not insure for the loss of intellectual property such as patents, software, and copyrights, loss of electronic device due to employee fault or negligence (Insuropedia, 2023), loss of future revenue, brand, and reputational damage, and management liability such as employment, discrimination, claims of directors and officers (Coalition, 2023).

According to the 2022 *Cyber Claims Study* by NetDiligence, the days of poor reporting and low incident figures are long gone. This study compiles claims data provided by many insurer participants including AIG, Allied World, AXA XL, Hiscox, Liberty Mutual, Swiss Re, Travelers, and Zurich NA (NetDiligence, 2022, p. 48). According to this report, the lack of data argument is a misconception. Therefore, there is now substantial claims data available due to insurers paying more attention to hiring technical security experts and collecting incident data (NetDiligence, 2022, p. 68). Although this information is not consolidated for quantitative analysis, it is available and allows insurers to assess company risk characteristics and better manage the underwriting task. In addition to more claims data being available, there is also substantial growth in the insurance market with respect to total direct premiums written. A report on the 2022 cyber insurance market, prepared by the National Association of

Insurance Commissioners (NAIC),[11] shows that the 152 insurer groups domiciled in the U.S. reported $4.82 billion in direct written premiums for cyber coverage, including cybersecurity alone and part of a package. The 2021 report shows that 141 insurer groups reported $2.75 billion in direct premiums written.[12] These numbers suggest that there was a 7.8% increase in the number of insurer groups participating and a striking 75.3% increase in direct written premiums from 2020 to 2021.

Despite its growth, the cyber insurance market is a relatively small portion of the total insurance market with $2.25 billion cyber insurance premiums representing only 0.38% of the $727 billion premiums in the property/casualty (P/C) direct premiums in the U.S. (NAIC, 2021). Also, while this upward trend implies growth in the cyber insurance market, only the top 20 groups represent most of the market activity, writing 83% of the total premiums (NAIC, 2022). Another important metric is the loss ratio for insurers, which is calculated as the ratio of the sum of insurance claims paid and loss adjustment expenses to the premiums earned. This ratio shows how much an insurance company paid on claims relative to the premiums earned. The average loss ratio of the top 20 groups in the cyber insurance market had increased steadily from 32.4% in 2017 to 66.9% in 2020 and had a slight decrease to 66.4% in 2021. According to the NAIC, this slight decrease is due to the substantial increase in the total premiums written. A healthy loss ratio for an insurance company is usually around the 60-70% range. Therefore, while the increase in the loss ratios may not be alarming at first glance, the loss ratios range for the top 20 insurers widened from 24.6-114.5% to -0.5-130.6%, suggesting increased volatility.

The Bottom Line

According to recent market data, there is a growing list of cyber insurance providers, more claims data available may enable better assessment of company-specific cyber risk, and more total written premiums in the cyber insurance market. In spite of the increase in demand for cyber insurance and the appearance of growth in the market, however, the substantial increase in the number of cyberattacks and ransomware makes cyber insurance a less attractive business for insurers (Johansmeyer, 2022). Johansmeyer (2022) states that cyber insurance is becoming harder to find, and many companies have to spend more money to purchase cyber insurance for less coverage. As a corollary, although the trade-off for firms, initially, seems to be between allocating resources to risk mitigation by investing in cybersecurity and purchasing cyber insurance to transfer cyber risk (Gordon and Loeb, 2002; Eling et al., 2020), a third option emerges as waiting until a breach happens and preparing for damage control. In other words, while obtaining cyber insurance causes firms to underinvest in attack prevention, less than complete coverage of losses may cause firms to overinvest in damage control (Lam, 2016). For example, Target Corporation experienced a data breach in 2013 and reported $191 million in pre-tax breach-related expenses and $46 million in expected insurance proceeds, resulting in net expenses of $145 million (Target Corporation, 2014, pg. 17). As a result, firms often increase their cash and liquidity

11. The NAIC collects data each year from insurance companies providing cybersecurity coverage through the property/casualty (P/C) annual statement cybersecurity and identity theft supplement.

12. The direct written premiums had changed from $1.89 billion in 2017 to $2.02 billion in 2018 and to $2.26 billion in 2019.

levels after a breach to be prepared for such potential costs (Garg, 2020; Boasiako & Keefe, 2021). This behavior persists in the following three years after a breach and spills over to the peer firms in the same industry, even if they are not breached (Garg, 2020). Maintaining high levels of liquidity, however, may exacerbate agency problems associated with free cash flows (Jensen, 1983).

Regulatory Oversight on Cybersecurity

Regardless of why managers defer cybersecurity investments, cyberattacks cause substantial damage to the world economy, and their negative impact spreads to the public. According to the Center for Strategic and International Studies (CSIS), almost $600 billion of the world's gross domestic product is lost annually to cybercrime, a near 32% increase from $455 billion reported in 2014 (Lewis, 2018). A report published by the Council of Economic Advisers (CEA) in February 2018 shows that cyberattacks cost the U.S. economy between $57 and $109 billion in 2016 alone. The CEA report touches on the issue of cybersecurity investment inefficiency and states, "Cybersecurity is a common good; lax cybersecurity imposes negative externalities on other economic entities and private citizens. Failure to account for these negative externalities results in underinvestment in cybersecurity by the private sector relative to the socially optimal level of investment." (2018, p.1). Farahmand et al. (2013, p. 240) offer valuable insights on the topic by elaborating on the incentive misalignment issue and identifying four scenarios[13] in which a manager's decision to invest (or not to invest) in information security has different underlying reasons or consequences. The authors argue that in cases where a corporate entity is the decision maker, and society is the consequence bearer, the government should correct incentive misalignment through regulations and laws.

Cybersecurity Regulation in the U.S.

Several steps are taken to prevent these malicious cyber events and protect private information. For example, former President Bill Clinton established the Commission on Critical Infrastructure Protection in 1996 to create and implement a national policy to protect these infrastructures against cyber threats (Lukasik, 1998). Later, the federal Financial Services Modernization Act of 1999 (also known as the federal Gramm-Leach-Bliley Act [GLBA]) requires financial institutions to protect sensitive data and disclose their information-sharing practices with their consumers. Among these financial institutions are banks, credit unions, insurance companies, and even retailers and automobile dealers that offer credit as part of their business. These institutions must describe how they will use, share, and protect their customers' private information and allow them to opt out of information sharing if they choose. Cybersecurity-related

13. Farahmand et al. (2013, p. 240) list these scenarios as follows: 1. Manager X can decide to invest (or not to invest) in better information security, and the unit that X manages looks less (more) profitable by the amount spent. The organizational reward system ties X's bonus to the profitability of the unit that X manages. 2. X decides to recommend and request the deployment of an intrusion detection system, as a result of which the workload of Y (possibly Y = X) increases because of the maintainance of the system and handling of false intrusion alarms. 3. X decides to underspend in (or underdeploy) security technologies, and a serious break-in occurs causing O to suffer considerable damage to its reputation as a result of media coverage and lawsuits by customers of O whose private data were compromised. 4. X decides to considerably invest in (or deploy) security technologies, and no break-in occurs.

incidents have become an increasing concern for the entire economy, especially for financial institutions, which are exposed to cyber risk almost 300 times more than their nonfinancial peers (Boston Consulting Group, 2019).

In response to these concerns, the SEC and the Financial Industry Regulatory Authority (FINRA) issued guidelines in 2015. These guidelines suggest that financial institutions assess their cybersecurity preparedness and develop resilient cybersecurity programs. Earlier in 2011, the SEC issued a disclosure guideline requiring publicly traded companies to include and discuss cyber risk as another business risk item in their annual filings. Later in 2018, the SEC updated the original guideline to prevent any insider trading attempt on cybersecurity-related information that is not known to the public yet. Finally, in 2020, the SEC issued its *Cybersecurity and Resiliency Observations* report, which discusses how protecting personal information and data is crucial for the integrity of financial markets and their participants.

These legislations and policies aim to avoid cyberattacks and minimize damage when they occur. Unfortunately, none require disclosing standardized data consistent across entities that can produce meaningful information to peer firms, customers, society, and policymakers. As of 2018, all 50 states and the District of Columbia require private and government entities to inform the public when they experience a data breach. In practice, firms disclose breach-related information to the attorney general's office[14] in their respective states. Disclosed information, however, lacks any standardization or uniformity that could help academic researchers and policymakers investigate the causes and consequences of such events.

Perhaps the most comprehensive set of rules is imposed by the New York State DFS. The agency recently updated its cybersecurity regulation, requiring financial institutions to implement a cybersecurity program effective in 2017. New obligations for financial institutions are currently in a comment period, which began on Aug. 8, 2022. If these rules become effective, Class A[15] companies will be subject to additional requirements such as annual independent cybersecurity audits, the existence and the independence of a senior information systems officer, additional board reporting and expertise, and an annual compliance certification approved by the chief executive officer. This new update is exciting because it will hold corporate boards and senior executives accountable for the cybersecurity practices at their firms. Nevertheless, there are several issues associated with these obligations. First, it is not certain when these new obligations will be signed into rules and become effective. Second, it is unclear how much information these firms will be required to disclose following the new commitments. Finally, firms with fewer than 2,000 employees and less than $1 billion in revenues will be exempt from these new rules.

Cybersecurity Regulation in the European Union

The EU started focusing on the information security issue with the European Data Protection Directive in 1995 to protect individuals and boost consumer trust by regulating

14. The PRC compiles the information disclosed by breached firms to the attorney general's offices in their states and makes this data available to the public on *https://privacyrights.org/data-breaches* that can be downloaded as an Excel file. The file contains a column label as "description of incident," which includes details of each breach.

15. The New York State DFS defines a Class A company as an entity with more than 2,000 employees and more than $1 billion in average gross annual revenue over the last three years.

the processing and free movement of personal data. Although the U.S. dominated the arena of cybersecurity for almost two decades starting in 1996 with the establishment of former President Clinton's Commission on Critical Infrastructure Protection, the EU started taking aggressive steps toward data privacy issues in 2011 by publishing an opinion statement to kickstart a comprehensive approach to protect personal data. The European Parliament adopted the GDPR in 2014 and established the European Data Protection Board (EDPB) in 2015, which is responsible for making sure the GDPR is applied consistently throughout the EU.

Later, in 2016, the GDPR entered into force with a wide range of existing and new data protection rights, including enabling individuals to request their personal data to be deleted from the collecting organizations' systems. The European Council proposed two new regulations in 2017 that obliged organizations to implement security measures to protect personal data and allowed them to process only necessary personal information for a specified purpose. Member states were required to transpose the Data Protection Directive into national legislation by 2018. At this stage, organizations processing personal data were required to develop information and communication systems and technologies that complied with privacy principles and ensured the data was protected by design. After giving a two-year adjustment period to member states, the GDPR was recognized as law across the EU, replacing the 1995 Data Protection Directive.

As of May 2018, the GDPR required organizations, whose activities involve the use of sensitive personal data on a large scale, to appoint a data protection officer (European Commission, n.d.-b). In compliance with the directive, while the operator of essential services (OES) must implement the required technical and organizational security measures and notify national authorities of serious incidents, the member states must establish a national point of contact to coordinate with other member states and establish "computer security incident response teams." Member states must also issue binding instructions to OES to alleviate weaknesses, assess other member states' compliance with the directive, and compel them to provide information including evidence of implementation. In addition to OES, digital service providers are subject to the same security and notification requirements.

Finally, the EU established the EU Cybersecurity Agency (ENISA) and adopted the EU Cybersecurity Act in 2019, which became effective in 2021. The EU Cybersecurity Act introduced a cybersecurity certification framework for products, services, and processes. This certification assists organizations in the prevention and detection of cyber incidents, and helps companies respond and recover from them. Companies operating in the EU, including U.S.-based companies, must certify their products and services. This certificate, recognized across the EU, "will make it easier for businesses to trade across borders" (European Commission, n.d.-a). Within the GDPR framework, data protection violations are subject to substantial fines and penalties. These fines are designed to be proportionate and dissuasive for each incident and can be up to €20 million (a minimum of €10 million for less severe incidents), or, in terms of an undertaking, 2-4% of their global turnover depending on the severity. The fines are applied in addition to or instead of corrective remedies to adjust the data processing

to comply with the GDPR and may impose limitations such as a ban on data processing (Intersoft Consulting, n.d.).

Trends in Cybersecurity Landscape

Although the EU appears to have a more stringent approach to cybersecurity and data protection, the *Cyber Readiness Report* published by Hiscox (2022) portrays a different view. Table 1 summarizes some important statistics from this report by country. Looking at the percentage of businesses that experienced a cyberattack, the largest increases are in the Netherlands, Ireland, and the U.S., while the smallest increases are in France, Belgium, and Germany. There is a slight decline in Spain. Looking at the median cost of cyberattacks, a similar trend is observed. Again, the largest increases are in the Netherlands, Ireland, and the U.S., while there is a decline in France and Germany. That said, the Netherlands, Spain, and France experienced the largest increase in ransomware attacks, while Ireland and Germany experienced the smallest increase, and France experienced a decline. The percentage of businesses that experienced a ransomware attack remained the same in the U.S. Focusing on the cyber insurance uptake, the percentages range between 58–69%, whereas Ireland, Germany, Spain, and the U.S. appear to be relying more on risk transfer. While the proportion of IT budget allocated to cybersecurity appears to be comparable among these nations, it appears that businesses increased their cybersecurity budget by 3% in Belgium and Germany, but only 1% in Ireland and in the U.S.

Table 1: Country Comparisons Hiscox Cyber Readiness Report 2022

	Experienced a cyberattack (%)		Median cost of all cyberattacks ($000)		Experienced a ransomware attack (%)		Cyber insurance uptake (%)		Proportion of IT budget for cybersecurity (%)	
	2021	2022	2021	2022	2021	2022	2021	2022	2021	2022
Belgium	42	43	12	10	19	15	58	59	21	24
France	49	52	18	17	14	19	57	61	20	22
Germany	46	46	24	21	19	21	64	67	21	24
Ireland	39	49	8	17	16	19	64	69	21	22
Netherlands	41	57	12	18	13	26	55	58	22	24
Spain	53	51	12	12	14	22	63	66	22	24
U.S.	40	47	10	19	17	17	65	65	23	24

While ransomware, supply chain attacks, and phishing are the most concerning threats in the EU, cyberattacks, identity fraud, and automotive hacking are the top three issues in the U.S. (Nuvias, 2023). These statistics show that cybersecurity is a global concern, and cyber incidents occur even in European countries where there are more stringent regulations. Although the EU and the U.S. have different approaches to data privacy and security, they started cooperating to prevent ransomware attacks and issued a joint statement in 2021. Nevertheless, cyberattacks remain a challenge for businesses across the world. Among others, the most striking observation from Table 1 is that there is heavy reliance on risk transfer through purchasing cyber insurance, and only a quarter of IT budget is allocated to cybersecurity in leading nations in Europe and

the U.S. This observation further supports the moral hazard argument with respect to underinvesting in cybersecurity and inefficient cyber risk management. As a result, we join the researchers who call for an optimal level of regulation.

Conclusion (With a Call for Regulation)

In today's digital economy, cyber risk is considered a new type of firm operational risk that requires the attention of the entire organization. The current disclosure requirements do not go beyond reporting a breach once it happens. Regulatory agencies publish CRM guidelines, but firms must take voluntary action to follow them. In other words, because CRM is not mandated, firms end up having to decide for themselves if they want to follow CRM guidelines, and they seek to hedge against cyber risk by purchasing insurance which has serious limitations. The NAIC (2022) indicates that cyber insurance premiums are rising, there is a 68% increase in the number of data breaches from 2020 to 2021 and implies these changes may be reflected in the cyber insurance prices with a 10-30% increase in the last quarter of 2020 and may be carried over to 2022. In addition to the increase in prices, the cyber insurance limits have also dropped from $10 million in 2019 to $5 million in 2020, then to $1-3 million in 2021. In addition to writing less business, insurers are adopting more strict underwriting processes and implementing more restrictive coverage terms to control their cyber risk exposure.

According to Comerford (2022), demand for cyber insurance is increasing due to the growing number of cyber incidents, where more than half of all cyberattacks target small- and mid-size businesses (Morgan, 2020). That said, 91% of small business owners do not have cyber insurance because: 1) they do not realize they need it; 2) they do nt understand the coverage; or 3) they think their property, casualty, and business interruption policies cover cyber-related incidents. Furthermore, due to increase in prices, businesses have to pay for more insurance and receive less coverage. From a small business perspective, the cost of a data breach for a company with fewer than 500 employees had increased from $2.35 million in 2020 to $2.98 million in 2021. Unfortunately, 60% of small companies close their doors within six months of experiencing a cyber incident (Johnson, 2019). Small businesses play an important role in the economy by providing jobs, creating tax revenue, and supplying products and services to local communities. Any threat to their vitality has severe consequences to consumers and the economy as a whole, which further support the need for optimal cybersecurity regulation to reduce the likelihood and the economic impact of cyberattacks.

References

Ali, A., & Kallapur, S. (2001). Securities price consequences of the Private Securities Litigation Reform Act of 1995 and related events. *The Accounting Review, 76,* 431–460.

Baer, W.W., & Parkinson, A. (2007). Cyberinsurance in IT security management. *IEEE Security and Privacy, 5*(3), 50–56.

Bandyopadhyay, T., Mookerjee, V.S., & Rao, R.C. (2009). Why IT managers don't go for cyber-insurance products? *Communications of the ACM, 52*(11), 68–73.

Bebchuk, L., & Stole, L. (1993). Do short-term objectives lead to under- or overinvestment in long-term projects? *The Journal of Finance, 48*, 719–729.

Beiner, C., Eling, M., & Wirfs, J.H. (2015). Insurability of cyber risk: An empirical analysis. *The Geneva Papers, 40*, 131–158.

Benaroch, M. (2018). Real option models for proactive uncertainty-reducing mitigations and applications in cybersecurity investment decision making. *Information Systems Research, 29*(2), 315–340.

Bergstresser, D., & Philippon, T. (2006). CEO incentives and earnings management. *Journal of Financial Economics, 80*(3), 511–529.

Betterley, R.S. (2013). Pricing in microinsurance markets. *World Development, 41*(1), 132–144.

Boasiako, K.A., & Keefe, M.O. (2020). Data breaches and corporate liquidity management. *European Financial Management, 27*(3), 528–551.

Bose, I., & Leung, A. (2013). The impact of adoption of identity theft countermeasures on firm value. *Decision Support Systems, 55*, 753–763.

Boston Consulting Group. (20, June 2019). *Global Wealth 2019: Reigniting Radical Growth.* https://www.bcg.com/publications/2019/global-wealth-reigniting-radical-growth

Bowen, R. M., DuCharme, L., & Shores, D. (1995). Stakeholders' implicit claims and accounting method choice. *Journal of Accounting and Economics, 20*(3), 255–295.

Boyd, B. K. (1994). Board control and CEO compensation. *Strategic Management Journal, 15*(5), 335–344.

Burns, N., & Kedia, S. (2006). The impact of performance-based compensation on misreporting. *Journal of Financial Economics, 79*(1), 35-–67.

Campbell, K., Gordon, L., Loeb, M., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security, 11,* 431-448.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. *International Journal of Electronic Commerce, 9*(1), 69–104

Cebula, J.J., & Young, L.L. (2010). *A taxonomy of operational cyber security risk,* Software Engineering Institute, Carnegie Mellon University. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=9395

CEA. (2018). *The cost of malicious cyber activity to the U.S. economy.* https://www.hsdl.org/?view&did=808776

Chai, S., Kim, M., & Rao, H.R. (2011). Firms' information security decisions: Stock market evidence of investment behavior. *Decision Support Systems, 50*, 651–661.

Cheng, Q., & Warfield, T. (2005). Equity incentives and earnings management. *The Accounting Review, 80,* 441–476.

Coalition. (2023). *What is cyber liability insurance?* https://www.coalitioninc.com/topics/what-is-cyber-insurance

Cohen, A., & Zarowin, P. (2010). Accrual-Based and Real Earnings management Activities around Seasoned Equity Offerings. *Journal of Accounting and Economics, 50*, 2–19.

Collins, D., & Hribar, P. (2000). Earnings-based and accrual-based market anomalies: one effect or two? *Journal of Accounting and Economics, 29,* 101–123.

Comerford, L. (2022). The value of cyber insurance for small businesses. *Security Magazine*. https://www.securitymagazine.com/articles/97724-the-value-of-cyber-insurance-for-small-businesses#:~:text=It's%20common%20for%20small%20businesses

Core, J., & Guay, W. (1999). The use of equity grants to manage optimal equity incentive levels. *Journal of Accounting and Economics, 28*(2), 151–184.

Deloitte. (2016). *Beneath the surface of a cyberattack: A deeper look at business impacts*. https://www2.deloitte.com/us/en/pages/risk/articles/hidden-business-impact-of-cyberattack.html

Dutta, A., & McCrohan, K. (2002). Management's role in information security in a cyber economy. *California Management Review, 45*(1), 67–87.

Eling, M., & Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance? *The Journal of Risk Finance, 17*(5), 474–491.

Eling, M., & Zhu, J. (2018). Which insurers write cyber insurance? Evidence from the U.S. property and casualty industry. *Journal of Insurance Issues, 41*(1), 22–56.

Eling, M., McShane, M., & Nguyen, T. (2020). Cyber risk management: History and future research directions. *Risk Management Insurance Review, 24*, 94–125.

European Commission. (n.d.-a). The EU Cybersecurity Act. Retrieved on June 4, 2023. from https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

European Commission. (n.d.-b). The History of the General Data Protection Regulation. Retrieved on June 4, 2023 from https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

Fama, E. F., & Jensen, M. C. (1983). Separation of ownership and control. *Journal of Law and Economics, 26*(2), 301–325.

Farahmand, F., Atallah, M., & Spafford, E. (2013). Incentive Alignment and Risk Perception: An Information Security Application. *IEEE Transactions on Engineering Management, 60*(2), 238–246.

Garg, P. (2020). Cybersecurity breaches and cash holdings: Spillover effect. *Financial Management, 49*(2), 503–519, doi:10.1111/fima.12274

Gartner. (2021, May 17). *Gartner Forecasts Worldwide Security and Risk Management Spending to Exceed $150 Billion in 2021* [Press release]. https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwide-security-and-risk-managem

Gatzlaff, K.M., & McCullough, K.A. (2010). The effect of data breaches on shareholder wealth. *Risk Management and Insurance Review, 13*(1), 61–83.

Gatzlaff, K.M., & McCullough, K.A. (2012). Implications of privacy breaches for insurers. *Journal of Insurance Regulation, 31,* 195–214.

Goel, S., & Shawky, H. (2009). Estimating the market impact of security breach announcements on firm values. *Information & Management, 46*, 404–410.

Goldman, D. (2012, March 22). 'Hacktivists' stole 58% of thieved data in 2011. *CNNMoney*. https://money.cnn.com/2012/03/22/technology/hacktivists-verizon-data-breach-report/index.htm

Goldman, E., & Slezak, S. L. (2006). An equilibrium model of incentive contracts in the presence of information manipulation. *Journal of Financial Economics, 80*(3), 603–626.

Gordon, L., & Loeb, M. (2002). The economics of cybersecurity information security investment. *ACM Transactions on Information and System Security, 5*(4), 438–457.

Gordon, L., & Loeb, M. (2006a). *Managing Cybersecurity Resources: A Cost-Benefit Analysis.* McGraw-Hill.

Gordon, L., & Loeb, M. (2006b). Budgeting process for information security expenditure, *Communications of the ACM 29, 1*, 121–126.

Gordon, L., Loeb, M., & Lucyshyn, W. (2003a). Information security expenditures and real options: a wait-and-see approach. *Journal of Computer Security, 19*(2), 1–7.

Gordon, L., Loeb, M., & Sohail, T. (2003b). A Framework for using insurance for cyber-risk management. *Communications of the ACM, 46*(3), 81–85.

Gordon L., Loeb M., & Zhou L. (2011). The impact of information security breaches: Has there been a downward shift in costs? *Journal of Computer Security, 19, 33*–56, doi 10.3233/JCS-2009-0398

Graham, J. R., Harvey, C. R., & Rajgopal, S. (2005). The economic implications of corporate financial reporting. *Journal of Accounting and Economics, 40*(1-3), 3–73.

Herrmann, D., Inoue, T., & Thomas, W. B. (2003). The sale of assets to manage earnings in Japan. *Journal of Accounting Research, 41*(1), 89–108.

Hiscox. (2022). *Cyber Readiness Report.* https://www.hiscoxgroup.com/sites/group/files/documents/2022-05/22054%20-%20Hiscox%20Cyber%20Readiness%20Report%202022-EN_0.pdf

Hinz, O., Nofer, M., Schiereck, D., & Trilling, J. (2015). The influence of data theft on the share prices and systematic risk of consumer electronics companies. *Information and Management, 52*, 337–347.

Hovav, A., & D'Arcy, J. (2003). The impact of denial-of-service attack announcements on the market value of firms. *Risk Management Insurance Review, 13*(3), 32–40.

Hsu, C., & Wang, T. (2014). Exploring the association between board structure and information security breaches. *Asia pacific journal of information systems, 24*(4), 531–557.

Huang, K., Wang, X., Wei, W., & Madnick, S. (2023, May 4). The devastating business impacts of a cyber breach. *Harvard Business Review.* https://hbr.org/2023/05/the-devastating-business-impacts-of-a-cyber-breach

Identity Theft Resource Center. (2017, October 2). *Identity theft: The aftermath 2017.* https://www.idtheftcenter.org/post/new-itrc-aftermath-survey-uncovers-the-strong-emotional-toll-identity-theft-plays-on-its-victims/

Immersive Labs. (2023). *The Immersive Labs Cyber Resiliency Score.* https://www.immersivelabs.com/the-score/#:~:text=Overview-,The%20Resilience%20Score%20is%20a%20single%20value%20that%20an%20organization,Their%20overall%20cyber%20resilience

Insuropedia. (2023.) *What are the common exclusions of cyber risk insurance?* https://securenow.in/insuropedia/what-are-common-exclusions-cyber-risk-insurance/#:~:text=Patent%2C%20software%2C%20and%20copyright%20infringement,policy%20does%20not%20cover%20these

Intersoft Consulting. (n.d.). *GDPR Fines / Penalties.* Retrieved on June 4, 2023 from https://gdpr-info.eu/issues/fines-penalties/

Jensen, M.C. (1986). Agency costs of free cash flow, corporate finance, and takeovers. *The American Economic Review, 76*(2), 323–329.

Jensen, M. C. (2002). Value maximization, stakeholder theory, and the corporate objective function. *Business Ethics Quarterly, 12*(2), 235–256.

Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics, 3*(4), 305–360.

Jensen, M. C. & Murphy, K. J. (1990). Performance pay and top-management incentives. *Journal of Political Economy, 98*(2), 225–264.

Johansmeyer, T. (2022, March 10). The cyber insurance market needs more money. *Harvard Business Review*. https://hbr.org/2022/03/the-cyber-insurance-market-needs-more-money

Johnson, R. (2019, January 2). 60 percent of small companies close within 6 months of being hacked. *Cybercrime Magazine.* https://cybersecurityventures.com/60-percent-of-small-companies-close-within-6-months-of-being-hacked/

Kamiya, S., Kang, J., Kim, J., Milidonis, A., & Stulz, R. (2020). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics, 139*:3, 719–749, doi:10.1016/j.jfineco.2019.05.019

Kerber, R. (2007, August 15). Cost of data breach at TJX soars to $256m. Suits, computer fix add to expenses. *The Boston Globe*. http://archive.boston.com/business/articles/2007/08/15/cost_of_data_breach_at_tjx_soars_to_256m/

Ko, M., & Dorantes, C. (2006). The impact of information security breaches on financial performance of the breached firms: An empirical investigation. *Journal of Information Technology Management, 17*(2), 13-22.

Kumar, R., Park, S., & Subramaniam, C. (2008). Understanding the Value of Countermeasure Portfolios in ISS. *Journal of MIS, 25*(2), 241–279.

Kwon, J., & Johnson, M.E. (2014). Proactive versus reactive security investments in the healthcare sector. *MIS Quarterly, 38*(2), 451–471.

Kwon, J., Ulmer, J., & Wang, T. (2013). The association between top management involvement and compensation and information security breaches. *Journal of Information Systems, 27*(1), 219–36.

Ladika, T., & Sautner, Z. (2020). Managerial short-termism and investment: Evidence from accelerated option vesting. *Review of Finance, 24*(2), 305–344.

Lam, W. (2016). Attack-prevention and damage-control investments in cybersecurity. *Information Economics and Policy, 37*, 42–51.

Lanz, J. (2016). Communication of Cybersecurity Risks to the Audit Committee. *CPA Journal, 86*(5), 6–10.

Lee, Y., Kauffman, R., & Sougstad, R. (2011). Profit-maximizing firm investment in customer information security. *Decision Support Systems, 51*, 904–920.

Lending, C., Minnick, K., & Schorno, P. (2018). Corporate governance, social responsibility, and data breaches. *The Financial Review, 53:2*, 413–455, doi: 10.1111/fire.12160

Lewis, J. A. (2018, February 21). *Economic impact of cybercrime – no slowing down.* The Center for Strategic and International Studies. https://www.csis.org/analysis/economic-impact-cybercrime#:~:text=The%20report%20concludes%20that%20close,losses%20at%20about%20%24445%20billion

Lukasik, S. (1998). Review and analysis of the report of the President's Commission of Critical Infrastructure Protection. *Stanford University, Freeman Spagli Institute, Center for International Security and Cooperation*. https://cisac.fsi.stanford.edu/publications/review_and_analysis_of_the_report_of_the_presidents_commission_on_critical_infrastructure_protection.

Mikhed, V., & Vogan, M. (2018) How data breaches affect consumer credit. *Journal of Banking and Finance, 88,* 192–207, doi: 10.1016/j.jbankfin.2017.12.002

Moore, T., Dynes, S., & Chang, F. (2015). How CISOs manage cybersecurity investment: Insights from the field. *Security Intelligence*. https://securityintelligence.com/how-cisos-manage-cybersecurity-investment--insights-from-the-field.

Morgan, S. (2020). Cybercrime to cost the world around $10.5 trillion annually by 2023. *Cybercrime Magazine*. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

National Association of Insurance Commissioners. (2021). *Cyber insurance market report*. https://content.naic.org/sites/default/files/inline-files/cmte-c-report-cybersecurity-insurance-market-211020.pdf

National Association of Insurance Commissioners. (2022). *Cyber insurance market report.* https://content.naic.org/sites/default/files/cmte-c-cyber-supplement-report-2022-for-data-year-2021.pdf.

NetDiligence. (2022). *Cyber Claims Study 2022 Report*. https://netdiligence.com/wp-content/uploads/2022/10/NetD_2022_Claims_Study_1.0_PUBLIC.pdf.

Nuvias. (2023). *Cybersecurity Perspectives: Europe vs. USA*. https://www.nuvias.com/en-us/cybersecurity-perspectives-europe-vs-usa/

Ogut, H., Raghunathan, S., & Menon, N. (2011). Cyber security risk management: Public policy implications of correlated risk, imperfect ability to prove loss, and observability of self-protection. *Risk Analysis, 31*(3), 497–512.

Rai, S., & Mar, S. (2014, December). Cybersecurity and the board. *Internal Audit*. pp. 21–23.

Rajgopal, S., & Shevlin, T. (2002). Empirical evidence on the relation between stock option compensation and risk taking. *Journal of Accounting and Economics, 33*(2), 145–171.

Rothrock, R., Kaplan, J., & Van der Oord, F. (2017, November 16). The board's role in managing cybersecurity risks. *MIT Sloan Management Review*. pp. 12–15.

Schneier, B. (2008, January 18). *The Psychology of Security (Part 1)*. [online essay] https://www.schneier.com/essays/archives/2008/01/the_psychology_of_se.html

Sipes, E., James, J., & Zetoony, D. (2016). Current data security issues for financial services firms. *Journal of Investment Compliance, 17*(3), 55–59.

Skinner, D. J., & Sloan, R. G. (2002). Earnings surprises, growth expectations, and stock returns or don't let an earnings torpedo sink your portfolio. *Review of Accounting Studies, 7*(2), 289–312.

Srinidhi, B., Yan, J., & Kumar, G.T. (2015). Allocation of resources to cybersecurity: The effect of misalignment of interest between managers and investors. *Decision Support Systems, 75*, 49–62.

Stein, J. C. (1989). Efficient capital markets, inefficient firms: A model of myopic corporate behavior. *The Quarterly Journal of Economics, 104*(4), 655–669.

Statista. (2022a). *Cyber crime: attacks experienced by U.S. companies 2021*. https://www.statista.com/statistics/293256/cyber-crime-attacks-experienced-by-us-companies/#statisticContainer. Accessed on September 7, 2022.

Statista. (2022b). *Cybercrime: number of compromises and victims in U.S.* https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/

Statista. (2022c). *Financial cybercrime losses in the U.S. 2021*. https://www.statista.com/statistics/234993/us-states-with-the-largest-losses-through-cybercrime/

Statista. (2022d). *Spending on cybersecurity in the United States 2010-2018*. https://www.statista.com/statistics/615450/cybersecurity-spending-in-the-us/

Target Copration. (2014). *Target 2014 Annual Report - 10-K*. https://corporate.target.com/getmedia/ce16ceb0-3600-46c0-9dc5-47b303250fff/Target-2014-Annual-Report.pdf

Tieman, L. (2011, November 14). Why your board of directors can't sleep on IT. *CFO*. https://www.cfo.com/governance/2011/11/why-your-board-of-directors-cant-sleep-on-it/

Turedi, S., & Erkan-Barlow, A. (2022). CIO equity compensation and IT investment: the moderating role of board monitoring and evidence of managerial myopia. *Review of Behavioral Finance, Advance online publication*. https://doi.org/10.1108/RBF-04-2022-0118

Watts, R., & Zimmerman, J. (1978). Towards a positive theory of the determination of accounting standards. *The Accounting Review, 53,* 112–134.

Weill, P., & Ross, J. (2004). *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*. HBS Press.

Wojcik, J. (2012). Cyber insurance not always enough. Business Insurance, 46(16), 4.

Yayla, A. A., & Hu, Q. (2011). The impact of information security events on the stock value of firms: The effect of contingency factors. *Journal of Information Technology, 26*(1), 60–77.