https://dx.doi.org/10.1016/j.jfineco.2019.05.019

Risk management, firm reputation, and the impact of successful cyberattacks on target firms

Shinichi Kamiya, Jun-koo Kang, Jungmin Kim, Andreas Milidonis, and René Stulz*

July 2019

Abstract

We develop a model where a firm has an optimal exposure to cyber risk. With rational, fully informed agents and with no hysteresis, a successful cyberattack should have no impact on a financially unconstrained target's reputation and post-attack policies. In contrast, when a successful attack involves the loss of personal financial information, there is a significant shareholder wealth loss, which is much larger than the attack's out-of-pocket costs. This excess loss is higher when the attack decreases sales growth more and lower when the board pays more attention to risk management before the attack. Further, an attack decreases a firm's risk appetite as it beefs up its risk management and information technology and decreases the risk-taking incentives of management. Finally, successful cyberattacks adversely affect the stock price of firms in the target's industry. These results imply that successful attacks with personal financial information loss provide adverse information about cyber risk to target firms, their stakeholders, and their competitors.

Keywords: Cyber risk, Cyberattack, Risk management, Reputation, Firm value, Stakeholders

JEL Classification: G14, G32, G34, G35

* Kamiya and Kang are from the Nanyang Business School, Nanyang Technological University, Singapore (Email: skamiya@ntu.edu.sg and jkkang@ntu.edu.sg, respectively); Kim is from the School of Accounting and Finance, Hong Kong Polytechnic University, Hong Kong (Email: jungmin.kim@polyu.edu.hk); Milidonis is from the Department of Accounting and Finance, University of Cyprus, Cyprus (Email: andreas.milidonis@ucy.ac.cy); and Stulz is from NBER and Fisher College of Business, Ohio State University, USA (Email: Stulz.1@osu.edu). We are grateful to an anonymous referee, Claudia Biancotti, Andrei Gonçalves, Jan Jindra, Christos Makridis, William Schwert (editor), and seminar participants at Hong Kong Polytechnic University, Kent State University, Korea University, Massey University, Renmin University of China, and the SEC for their useful comments. We are also grateful to participants at the 2018 International Conference on Asia-Pacific Financial Markets, the 2018 SFS Cavalcade Asia-Pacific Conference, and the 2019 American Economic Association Annual Meeting.

1. Introduction

Firms have a wide variety of stakeholders, such as customers, employees, and suppliers. Some of these stakeholders trust firms with personal data that may involve financial information. Firms are exposed to cyber risk and, as a result, the personal data entrusted to them may be hacked and stolen. In a survey, more than half of the CEOs expect cybersecurity and data breaches to threaten stakeholder trust in their industries over the next five years.[1] Firms could choose not to be exposed to cyber risk, but they would not be competitive doing so and likely would not be able to function. As a result, they choose to be exposed to some level of cyber risk, and some attacks take place and succeed.

When a firm's stakeholders observe an unexpected event that affects the firm, they may decide not to transact with the firm on terms as favorable to it as those that they agreed to before the event. For instance, if a firm discloses a product defect that has already been fully resolved, customers may still only be willing to buy its products at a lower price to account for the fact that the firm may not be as reliable or trustworthy as they thought it was. The loss that a firm suffers when stakeholders demand better terms to transact with it following an unexpected event that makes the firm more risky to transact with for stakeholders is called a reputation loss (see Karpoff, 2012). We show that the risk of reputation loss can be cast as the outcome of an optimal risk management strategy. This contribution of our paper is quite general and holds beyond the case of cyber risk.

Consider a firm whose stakeholders know its loss distribution for cyberattacks.[2] Before an attack, stakeholders require better terms from the firm because they are exposed to the risk of attacks. This requirement from stakeholders causes the firm to spend more on risk management to decrease the risk of attacks, as by doing so it improves the terms on which it transacts with stakeholders. However, after an attack, as long as neither the firm nor its stakeholders find out from the attack that the loss distribution is

[1] See "Risk in Review 2017 Study," PwC (April 2017), p. 21.

[2] The main measurement tool of operational risks is the loss distribution that is a convolution of a frequency distribution function and a severity distribution function.

different from what they believed it to be, a financially unconstrained firm should not suffer a reputation loss from the cyberattack and thus firm policies should not change. In this case, the cyberattack is the realization of a risk that stakeholders were fully aware of when they dealt with the corporation.

In this paper, we use a comprehensive sample of disclosed cyberattacks on public corporations involving data breaches from 2005 to 2017 to investigate the impact on corporations of successful cyberattacks. We find that on average a successful cyberattack (i.e., an external attack that breaches the firm's defenses) with loss of personal financial information decreases shareholder wealth by 1.09% in the three-day window around the cyberattack. Contrary to the prediction of a simple full-information rational expectations model, we find that successful cyberattacks have potentially economically large reputation costs in that the shareholder wealth loss far exceeds the out-of-pocket costs from the attack. In aggregate, we find that for a subset of 75 first-time attacks with negative abnormal returns, the total shareholder wealth loss is $104 billion, but the direct out-of-pocket costs of the attacks that we can identify (e.g., investigation and remediation costs, legal penalties, and regulatory penalties) are only $1.2 billion. It follows that out-of-pocket costs explain almost none of the shareholder wealth losses caused by cyberattacks.

We provide a simple model grounded in the risk management literature to examine the economic implications of successful cyberattacks. We show that a risk-neutral firm finds it optimal to invest in risk mitigation if stakeholders care about firm risk. In the following, we use cyberattack to denote a successful cyberattack for simplicity.[3] We distinguish between cyberattacks that change the firm's and its stakeholders' assessment of the firm's loss distribution of cyberattacks versus those that have no such impact. With the loss distribution unchanged, we show that a firm's loss from a cyberattack should not affect its reputation and future policies if it is not financially constrained. If the loss distribution or more generally the firm's assessment of its risk exposures changes, the firm will adjust its policies to its new understanding of the loss distribution. If the new loss distribution is less favorable for stakeholders than the previous one, the firm suffers a reputation loss. The change in the assessment of the loss distribution

[3] Throughout the paper, we use the words "cyberattacks" and "attacks" interchangeably.

may be rational – the result of new information becoming available – or can be due to behavioral reactions to adverse outcomes that were believed to have an extremely low probability. As the loss distribution becomes less favorable, the firm increases its expenditures to decrease the probability of an attack, invests more in risk management, and decreases its willingness to take other risks. We test these predictions by examining the costs of cyberattacks (i.e., adverse effects on shareholder value), the extent of the reputational loss from cyberattacks, and post-attack changes in firm policies.

To provide systematic evidence on the impact of successful cyberattacks, we use data breach events caused by cyberattacks reported to the Privacy Rights Clearinghouse (PRC) over the period 2005 to 2017. Studying security breaches that result in the loss of personal information obtained from the PRC has an important advantage compared to using other types of data breaches because firms must disclose such breaches to affected persons in a timely manner under the State Security Breach Notification Laws. Although it is possible that an attacked firm in our sample withheld the information about the discovery of the incident and delayed its announcement to the public, the disclosure requirements mandated by the data breach notification laws help alleviate potential sample underreporting biases that may occur in other studies using data breaches without such reporting requirements.[4] Our sample includes a homogenous sample of attacks as it only includes attacks initiated by outside parties. Specifically, we include only successful malicious external actions, such as hacking and malware. We exclude other incidents associated with internal errors or failure to follow data handling policies (e.g., internal fraud, unintended disclosure, the loss of portable device, the loss of stationary device, and physical loss) as these events are not the result of attacks on computers and computer networks by outsiders.

[4] For example, using the data breaches covered in the Audit Analytics cyber-attacks database and the VCDB VERIS database, Amir, Levi, and Livne (2018) examine the extent to which firms withhold information on cyberattacks. Their sample includes data breaches that do not involve the loss of personal information (and thus are not subject to the Security Breach Notification Law) as well as "Confidentiality" events that potentially involve the loss of personal information.

We first examine which firms are more likely to be affected by cyberattacks. Our likelihood analysis shows that firms are more likely to experience cyberattacks when they are larger, included in the list of *Fortune* 500 companies, financially less constrained, more highly valued, and have more intangible assets. We also find that cyberattacks are more likely to occur in firms operating in industries that are less competitive. Firm-level corporate governance characteristics, such as CEO-chair duality, the proportion of outside directors on the board, and board size, do not predict the likelihood of cyberattacks. Lastly, firms that pay more attention to risk management at the top, which we measure using the information reported in BoardEx about the existence of a risk management committee on the board, are less likely to be attacked.

Next, we analyze market reactions to the announcement of cyberattacks. A cyberattack is costly for a firm as it is likely to lead to expenses on systems, to remediation and mitigation costs, to litigation costs, perhaps to fines, and possibly to a reputation loss as stakeholders may no longer be willing to deal with the firm on the same terms. Consequently, we expect a negative abnormal return for firms that announce a cyberattack. Consistent with this expectation, we find a significant mean cumulative abnormal return (CAR) of -0.84% during the three-day window around cyberattack announcements for our full sample of personal information loss. With a mean market value of about $58.93 billion for our sample of attacked firms, this translates into an average value loss of $495 million per attack. Attacks involving the loss of personal financial information have a worse CAR (-1, 1), as it is -1.09%, while those that do not involve the loss of personal financial information do not have a significant cumulative abnormal return. The impact of cyberattacks is especially negative when attacked firms are older and when they do not have evidence of board attention to risk management (measured by whether the board or a board committee explicitly has the role of monitoring firm risks and risk management) as the abnormal return is lower by 4 percentage points for such firms. However, we find no consistent evidence that the stock-price reaction is worse for financially constrained firms.

The earlier literature that attempts to measure reputational loss proceeds in either one of two ways. Some studies follow Jarrell and Peltzman (1985) and Karpoff and Lott (1993) and treat the reputational

loss as a residual, namely the upper-bound for that loss is the unexplained market loss. We use this approach first. Other studies use a direct approach to explore reputational losses by assessing the impact on earnings or on stakeholder relationships (e.g., Graham, Li, and Qiu, 2008; Murphy, Shrieves, and Tibbs, 2009). We also use this direct approach. In addition, in contrast to most of the literature, we assess directly whether the investor-based measure of residual loss estimated from the residual approach is consistent with ex post changes using the direct approach.

Specifically, we investigate the determinants of the excess of shareholder wealth losses over the out-of-pocket costs (hereafter, the "excess loss"). As in Karpoff, Lee, and Martin (2008), our estimate of the excess loss is an upper bound for reputation losses that the shareholders suffer. Our model with no learning cannot explain our finding that the excess loss makes up almost all of the shareholder wealth losses. In our model, the excess loss is positive when the firm and its stakeholders learn from the attack that the loss distribution of cyberattacks is worse than they believed and when they learn from the attack about the firm more generally. For instance, the new information could lead to a general decrease in trust of the firm.

To assess the importance of reputation costs in cyberattacks, we investigate whether stakeholders deal with the firm differently after the attack. For instance, if customers believe that the firm has become riskier, we would expect them to reduce their demand for the firm's products, so that the firm's sales growth would fall. We also examine the changes in a firm's investment in risk management in the post-attack period and the contagious effects of cyberattacks on industry competitors to assess whether the firm, stakeholders, and industry competitors learn about cyber risk from the attack.

We first investigate the sales growth of attacked firms in the post-attack period using a propensity-score-matched sample. Our simple model predicts that attacked firms experience a drop in sales growth as well as profitability if customers learn adverse information about the risk of dealing with the firm. Consistent with this prediction, our difference-in-differences analysis shows that sales growth significantly declines for the three years after the attack. We further find that the impact of cyberattacks on sales growth exhibits substantial cross-sectional variation: large firms experience a significant decrease

in sales growth, while small firms do not. We find a significant, large negative impact of cyberattacks on sales growth for firms operating in the retail industry. Though we do not find an adverse impact of cyberattacks on operating performance in general, they do have an adverse impact on large firms and firms operating in durable goods industries. Moreover, attacked firms experience a decrease in credit ratings. All this evidence is consistent with the existence of a reputation loss for target firms.

We expect customers of firms that pay more attention to risk management to be less likely to learn adverse information about the firm from an attack. All else being equal, these firms would understand their exposure better, so that information from a cyberattack would change their assessment of the loss distribution of cyberattacks less. We use an indicator for the existence of a board committee with risk in its title or mandate to measure the extent of the board's attention to risk management. Consistent with the expectation, we find that firms with a risk committee experience a much lower excess loss, if they incur any excess loss at all.

If a firm's risk management approach was optimal before the cyberattack and the firm learns nothing from the attack, we would not expect the firm's risk appetite and, more generally, its approach to risk management, to change. We find that victims of a cyberattack are more likely to increase board oversight of firm risk. This result suggests that the board and management reassess the firm's risk exposure and the costs of this risk exposure after an attack. For example, management of the attacked firm could conclude that its risk exposures impose greater costs than previously believed and its customers also become more concerned about the risk of cyberattacks as well as other types of risk. In this case, management might want to decrease the firm's risk exposures to persuade its customers to continue to do businesses with it.

If a cyberattack changes the board's assessment of firm risk or its risk appetite, we would also expect the CEO's risk-taking incentives to be adjusted. We find that attacked firms do not reduce the overall level of CEO equity incentives (i.e., the ratio of equity-based compensation to CEO total pay) after a cyberattack. However, attacked firms significantly increase restricted stock grants and reduce option awards, suggesting that they replace stock options with restricted stock and hence reduce the risk-taking incentives of CEOs. Attacked firms also respond to cyberattacks by significantly reducing the ratio of

CEO bonus to total pay.

Finally, we investigate the impact of the disclosure of a firm's cyberattack on its industry competitors to provide further insights into the nature of the reputation loss documented in this study. A reputation loss could occur because it reveals adverse information that is specific to the target. For instance, the attack could reveal that the firm's management is not as good as previously thought. In this case, the disclosure of an attack would be good news for competitors. Alternatively, its disclosure could reveal information about the risk that is common to firms in the industry. For instance, an attack could reveal that attacks are more costly than previously thought, which would affect adversely all firms in the industry. We show that disclosure of an attack adversely affects firms operating in the same industry as the target, so that attacks appear to reveal adverse information that affects all firms in the industry.

Although previous studies also examine the valuation effect of cyberattack announcements, their results are mixed.[5] Many of these studies use samples that suffer from sample selection biases that we attempt to minimize in our study by choosing attacks that are purely external and that have reporting requirements. We also assess out-of-pocket costs and potential reputation losses resulting from the attacks. More importantly, however, our study provides a theoretical framework grounded in modern risk management theory and the theory of firm reputation, which enables us to understand when cyberattacks

[5] Most studies in the information security literature that examine the impact of cyberattacks on the market value of U.S. firms focus on the events that occur in the late 1990s and the early 2000s, and their empirical evidence is inconclusive (Campbell et al., 2003; Garg, Curtis, and Halper, 2003a, 2003b; Hovav and D'arcy, 2003; Cavusoglu, Mishra, and Raghunathan, 2004; Hovav and D'arcy, 2004; Ko and Dorantes, 2006). There are only a limited number of finance and accounting studies that examine the valuation impact of cyberattacks including Cummins, Lewis, and Wei (2006), Gatzlaff and McCullough (2010), Hilary, Segal, and Zhang (2016), Johnson, Kang, and Lawson (2017), Amir, Levi, and Livne (2018), Bianchi and Tosun (2018), Lending, Minnick, and Schorno (2018), and Akey, Lewellen, and Liskovich (2018). Unlike our analyses that focus only on malicious external actions such as hacking and malware, their main analyses include data breaches caused by insiders' mishandling of sensitive information and by theft of laptops and physical devices.

lead to economically significant losses and how firm policies change because of cyberattacks.[6]

The rest of this paper is organized as follows. In Section 2, we examine the theoretical predictions of the impact of cyberattacks on firms. In Section 3, we describe our sample construction and present the distribution of sample events and firm characteristics. In Section 4, we examine the likelihood of firms being attacked using various firm and industry characteristics. In Section 5, we analyze the impact of cyberattacks on shareholder wealth. We then turn to an investigation of whether and how the excess loss that consists of the reputation loss and other costs associated with learning contributes to the wealth impact of cyberattacks in Section 6. In Section 7, we examine whether there is evidence of reputation and learning effects following cyberattacks by examining how sales, risk management, and risk-taking incentives change after a cyberattack. Section 8 shows the impact of cyberattacks on the shareholder wealth of industry competitors. We conclude in Section 9.

2. A theory of the information content of cyberattacks

Consider a firm with value that is a concave function of future profits, so that greater volatility in profits keeping the mean constant decreases the value of the firm. For such a firm, there is value to risk management that decreases the volatility of profits and there exists an optimal level of volatility of profits if risk management actions are costly. The earlier risk management literature focuses on various factors

[6] Several previous papers examine post-breach changes in firm outcomes that are different from those in our study. For example, using all types of breaches including insiders' mishandling of sensitive information, Hilary, Segal, and Zhang (2016) find that attacked firms do not experience any significant changes in operational performance, executive departure likelihood, shareholder clientele, and the amount of disclosure after the breaches. Makridis and Dean (2018) find some evidence on the negative association between breaches and firm productivity using data from the PRC and Department of Health and Human Services from 2005 to 2016. Akey, Lewellen, and Liskovich (2018) and Lending, Minnick, and Schorno (2018) further find that firms significantly increase their investment in corporate social responsibility (CSR) in the years following a breach, and Nordlund (2019) documents that directors in a breached firm experience an increase in the likelihood of turnover.

that make firm value a concave function of future profits, such as bankruptcy costs, taxes, or the cost arising from not being able to fund valuable projects because of financial constraints (see, for instance, Smith and Stulz, 1985; Froot, Scharfstein, and Stein, 1993). In this paper, we focus on the case where this concavity comes from the fact that greater firm volatility imposes costs on stakeholders who deal with the firm, so that if the firm is riskier, stakeholders demand better terms to deal with the firm. The firm faces a tradeoff between the benefit of reducing the risk it imposes on stakeholders and the cost of doing so. As a result, there is an optimal level of risk. When a firm considers how much it should take of a specific risk, it focuses on how much this specific risk contributes to its overall risk, so that the firm's investment in risk management with respect to a specific risk depends on the other risks that it is exposed to.[7] Our model applies generally, so that it has implications for any risk that affects stakeholders, even though we focus on cyber risk.

Operational risk is one form of risk that firms are exposed to. Definitions of operational risk differ, but it is often understood as any risk that disrupts business processes.[8] Operational risks involve both external and internal risks. An earthquake that disrupts production is an operational risk, but so is fraud by employees. Cyber risk is also one type of operational risks.

Firms try to assess operational risk using loss distributions (e.g., Crouhy, Galai, and Marks, 2014) that are the result of the convolution of a frequency distribution and a loss severity distribution. Firms can reduce their exposure to an operational risk by taking risk mitigating actions (e.g., revamping information technology (IT) system defenses, hiring more staff to investigate hacking attempts), but these mitigating actions are costly. As a result, we expect firms to invest more in risk mitigating actions if adverse outcomes from cyberattacks (e.g., loss of sales, recovery costs of IT systems, and litigation costs) are costlier to them.

[7] See, for instance, Stulz (2003) and Lam (2014).

[8] "Operational risk is the risk that people, processes, or systems will fail, or that an external event (e.g., earthquake, fire) will negatively impact the company" (Lam, 2014, p. 31).

In the remainder of this section, we explore the information content of the announcement of a successful cyberattack in a model where the firm chooses an optimal level of exposure to cyber risk. In the first part of the section, we consider the case where all stakeholders are fully informed about the firm's optimization problem and the loss distribution of cyber risk is constant, so that the loss distribution is the same before and after an attack. We then examine the case where the loss distribution changes because of an attack and firms reassess their risks more generally based on information learned from the attack. In the third part of the section, we study the case where information revealed through the attack is contagious in that it affects the value of industry competitors of the attacked firm. In the last part of the section, we present our testable hypotheses.

2.1. The case of full information and constant loss distribution

We consider the problem of a single firm deciding how much to invest in risk management (i.e., risk mitigating actions). Financial markets are assumed to be perfect and the firm is an all-equity firm. The firm lives one period and the discount rate is zero for simplicity. The firm has valuable databases that could be hacked. An attack can take place both at the beginning and at the end of the period. Initially, the firm invests in risk management to mitigate the risk of an attack at the beginning of the period. Given the level of the investment in risk management, nature decides whether an attack happens or not. After observing the attack, firm stakeholders decide on the terms on which they will deal with the firm. These terms depend on the risk of an attack at the end of the period. The firm can reduce the risk of an end-of-period attack through investments in risk management before stakeholders commit to terms. The firm liquidates at the end of the period. The loss to the firm of an attack is the loss to equity holders.

The probability of a successful attack is $p^B \in [0, 1]$ for an attack at the beginning of the period and p^E for an attack at the end of the period. These probabilities depend on the level of the firm's investment in risk management to decrease the likelihood of an attack. For each attack risk, the cost of maintaining a risk management program to keep the probability of being hacked at $p = p^B$ or p^E is equal to $Q(p)$, which

is a decreasing ($Q' < 0$) and convex ($Q'' > 0$) function of p with $\lim_{p \to 0} Q(p) = \infty$. Intuitively, it is costlier to maintain a lower probability of being hacked and improving risk management becomes increasingly more expensive as the probability of being hacked gets closer to zero, so that it is effectively impossible to fully eliminate the risk of being hacked.

The total loss of firm value from an attack, which is the equity loss, is *TL* for the attack at the beginning of the period and TL^E for the attack at the end of the period. For now, *TL* is the sum of two distinct costs: out-of-pocket costs, *OPC,* and a reputation loss, *RL*. We assume that a successful cyberattack results in out-of-pocket costs that are identical and fixed irrespective of whether the attack occurs at the beginning or at the end of the period. The out-of-pocket costs correspond to direct expenses necessitated by the attack, such as costs of fixing the IT systems, compensating stakeholders for losses if any, paying fines, and so on. Given a fixed cost *OPC*, *RL* is endogenously determined and hence *TL* is also endogenously determined.

For now, the only risk that stakeholders care about is the risk of a successful cyberattack. Stakeholders are assumed to be averse to such a risk. The only risk they bear is the risk of an attack at the end of the period. Consequently, they require better terms from the firm as p^E increases. The cost to the firm of these better terms is given by a function $A(p^E)$, an increasing function of p^E with $A(0) = 0$. To simplify the analysis, we assume that this function is linear and increasing in p^E, so that $A(p^E) = A \times p^E$, where A is a positive constant. With our assumptions, an attack at the end of the period has no subsequent impact on the firm's transactions with stakeholders, as it no longer exists afterwards. We further assume that the stakeholders and the firm have the same information, so that they know *OPC*, $A(p^E)$, and $Q(p^E)$.

To determine the probability of an end-of-period attack given our assumptions, we proceed by optimizing firm value immediately after it is determined whether there is a beginning-of-period attack or not. For simplicity, we assume that the firm's objective function is linear with respect to the net present

value of the cost of cyberattacks.[9] It follows from our assumptions that the present value of the expected cost of a successful end-of-period attack, immediately after observing whether there was a beginning-of-period attack, is:

$$p^E \times OPC + A(p^E) + Q(p^E) \tag{1}$$

Note that $A(p^E)$ is an ex-ante cost that is determined once the probability of an end-of-period attack is set. To determine the optimal investment in risk management related to hacking, management trades off the expected cost of being hacked with the cost of risk management plus the cost of compensating stakeholders for the risk of cyberattacks. Optimally, the firm invests in risk management up to the point where the probability of being hacked is such that (using a prime to denote a derivative):

$$Q' + A = -OPC \tag{2}$$

For concreteness, it is useful to use a simple functional form for $Q(p)$. For now, we are concerned with the risk of an end-of-period attack, so that the relevant probability is p^E. We set $Q(p^E) = k / p^E$ where k is a constant with $0 < k < OPC + A$, which implies that the firm chooses to invest in risk management so that the optimal value of p^E is $p^{E*} = \left(\frac{k}{OPC+A}\right)^{1/2}$ since the firm does not incur a reputation loss from an end-of-period attack. It follows that the probability of being hacked is negatively related to the out-of-pocket costs and the marginal cost of imposing greater cyber risk on stakeholders. Figure 1 shows how the probability p^E of an end-of-period attack is determined given the cost of investing in risk management.

[9] It is reasonable to assume that the risk of cyberattack is largely uncorrelated with the other risks of the firm. Making the objective function convex in the net present value of the cost of cyberattacks would not change our conclusions.

Having determined the probability of an end-of-period attack, we can now turn to the implications of a beginning-of-period attack. With our assumptions, the optimal probability of an end-of-period cyberattack, p^{E*}, does not change with an attack at the beginning of the period as nothing changes in equation (1) if there is an attack at the beginning of the period. Consequently, a beginning-of-period attack does not affect the present value of the cost of an end-of-period cyberattack. Importantly, the terms on which stakeholders are willing to transact with the firm depend on p^{E*} and not p^{B*}, which is the optimal probability of a beginning-of-period attack. Therefore, there is no reputation loss from the beginning of period cyberattack. The firm loss from a beginning-of-period cyberattack is the unexpected out-of-pocket costs, $(1-p^{B*}) \times OPC$ because the market expects the costs of the beginning-of-period attack to be $p^{B*} \times OPC$.

With our analysis, the value of the firm is lower with cyber risk because of the present value of the sum of out-of-pocket costs from attacks, risk management investments to mitigate future attacks, and the compensation stakeholders require for their risk exposure to cyberattacks. A key assumption of the analysis is that neither $A(p^E)$ nor $Q(p^E)$ depend on whether there is a beginning-of-period attack. This assumption requires the absence of hysteresis: the loss distribution of a future attack does not depend on whether an attack has taken place. It also requires that the attack does not make the firm financially weak. If the firm becomes financially weak because of the attack, stakeholders will require better terms to deal with it and $A(p^E)$ will depend on whether an attack has taken place. An all-equity firm can always put itself back in the financial position it was in before the attack by raising equity for an amount equal to $(1-p^{B*}) \times OPC$. If it had an optimal amount of equity before the attack and raising equity is costless, the firm will raise that amount to get back to the optimum. Consequently, for the all-equity firm, there will be no reputation cost associated with the attack unless frictions to raising equity are high. We call a firm that can put itself in the same financial position it was in before the attack afterwards a firm that is not financially constrained. With our assumptions, such a firm would want to raise equity.

Consider now the case where the firm is leveraged. In this case, the loss of $(1-p^{B*}) \times OPC$ reduces the value of the debt if the debt is risky. As a result, if the firm raises equity, it has to consider the possibility

that equity financing benefits debtholders at the expense of shareholders (Myers, 1977). Therefore, it may not be optimal for the firm to raise equity in this case (Admati et al., 2018). Thus, for a leveraged firm, keeping all other assumptions the same, the firm is not the same after the attack because it is more highly leveraged than before. Stakeholders will not want to keep dealing with the firm on the same terms. Hence, the demand curve for the firm's products might shift to the left so that, for a given price, the firm would sell less. It follows that the loss to the firm from the attack will exceed $(1\text{-}p^{B*}) \times OPC$, so that $RL > 0$. We call a firm in this situation a financially constrained firm in that its financial condition prevents it from taking actions that would maximize firm value instead of equity value.

2.2. Learning effects

We now explore the case where an attack at the beginning of the period conveys information about the variables that determine the probability and the cost of an attack. In other words, the attack provides the firm and its stakeholders with a signal about the loss distribution of cyber risk. Given that managers and stakeholders tend to have limited information about the loss distribution for emerging risks such as cyber risk, it is important to consider learning effects in analyzing the real effects of cyberattacks. The firm and its stakeholders use this signal to reassess the loss distribution of cyber risk after the beginning-of-period attack. The signal leads to a new estimate of the out-of-pocket costs of an end-of-period attack, OPC^{Post}, to a new estimate of the cost function of mitigating cyber risk, $Q^{Post}(p^E)$, and/or to a new cost function for the change in terms of stakeholders, $A^{Post} \times p^E$. The solution of the model for the optimal probability of an end-of-period attack with the new loss distribution is obtained in the same way as before. The optimal probability of an end-of-period attack is written p^{Post*} when the beginning-of-period attack is informative about the loss distribution of the end-of-period attack.

To obtain the loss in firm value caused by a beginning-of-period attack, we have to take into account the change in the present value of the end-of-period attack resulting from the fact that there is a

beginning-of-period attack.[10] In this case, the shareholder loss resulting from the beginning-of-period attack becomes:

$$(1- p^{B*}) \times OPC + [p^{Post*} \times (OPC^{Post} + A^{Post}) + Q^{Post}(p^{Post*}) - p^{E*} \times (OPC^{E} + A^{E}) - Q^{E}(p^{E*})] \quad (3)$$

As the firm and its stakeholders learn from the beginning-of-period attack, the loss from the beginning of period attack exceeds the unexpected out-of-pocket costs if information that they acquire is adverse. There are three distinct sources of the greater wealth loss if the beginning-of-period attack conveys adverse information to the firm and its stakeholders. First, the firm and its stakeholders could find out because of the attack that the out-of-pocket costs of an end-of-period attack are higher than expected. Second, the cost of achieving a probability of an attack, *p*, may have been underestimated. In this case, it would be costlier for the firm to achieve the optimal attack probability determined before the information revealed by the beginning-of-period attack, so that firm value falls. The firm's response to the greater risk of an attack for a given amount of investment in risk management will be to invest more in risk management but also to accept a higher probability of an attack. The greater probability of an attack will increase both the compensation stakeholders demand for their risk exposure to an attack and the expected out-of-pocket costs of an attack. Third, stakeholders might have underestimated the costs they have to bear from a cyberattack. If they underestimated the costs, firm value will fall for a given probability of an attack, as stakeholders will ask for greater compensation to bear the risk of an attack.

Note that it is possible that an attack could have favorable information about the loss distribution of the end-of-period attack, in which case the shareholder wealth loss from a beginning-of-period attack would be decreased. In this case, the stock-price reaction to the announcement of the beginning-of-period attack could be even positive if out-of-pocket costs are low enough. To see this, take the extreme case,

[10] Note that an attack could reveal that the out-of-pocket costs of the beginning-of-period attack are higher than expected. We ignore this possibility in equation (3) for simplicity.

where the probability of an attack becomes very small. In this case, the firm would make a gain since it no longer has to compensate its stakeholders as much for the risk of a cyberattack and it no longer bears the risk of incurring out-of-pocket costs at the end of the period.

A successful beginning-of-period attack can have a reputation cost in our model for one of two reasons assuming that the attack only affects investors' assessment of the loss distribution of the end-of-period attack. First, if information learned from the beginning-of-period attack reflects an increase in the optimal probability of an attack (i.e., $p^{Post}* > p^{E}*$), stakeholders would charge more for the risk they bear (i.e., $p^{Post}* \times A > p^{E}* \times A$). Second, if information stakeholders learned makes them revise upward their assessment of the cost of an attack (i.e., $OPC^{Post} > OPC^{E}$, $A^{Post} > A^{E}$, or $Q^{Post}(p) > Q^{E}(p)$), so that they think the attack is costlier than they thought. In either case, firm value would fall more than unexpected out-of-pocket costs. In these two cases, the firm loss resulting from the change in its dealings with stakeholders will have two components. First, the firm will have to bear some costs to improve terms for its stakeholders. Second, stakeholders will be less willing to transact with the firm because it will never be optimal for the firm to offset completely the impact of the beginning-of-period attack. Consequently, a way to check that there is a reputation cost arising from a change in the firm's transactions with stakeholders is to investigate whether stakeholders change the terms on which they deal with the firm and whether stakeholders cut back on their dealings with the firm. The implication of this argument is that customers as firm stakeholders will find it less attractive to purchase products from the company than before. Hence, the reputation loss should be accompanied by lower sales than if the cyberattack had not happened. A firm might learn from a breach that it underestimated the benefits from investment in risk management. In particular, the firm might have underestimated the positive impact on sales of more investment in risk management. In such a situation, it is actually possible that sales would be higher after the breach because the firm would take steps to decrease the probability of a breach. A firm might also make other investments to decrease the terms on which it deals with stakeholders after a successful attack. It is notable that recent papers find that firms invest more in corporate social responsibility in the years

following a breach (Akey, Lewellen, and Liskovich, 2018; Lending, Minnick, and Schorno, 2018), which corresponds to an attempt to improve the terms on which they deal with stakeholders.

A beginning-of-period attack can also provide information to stakeholders about management or about the firm in general. If that information is adverse, the value of the equity will fall by more than the out-of-pocket costs of the beginning-of-period attack, so that there will be a reputation loss. For instance, they could learn that the firm's risk management processes are not as good as they thought. Stakeholders could also learn that management is not as competent as they thought. These updates are represented by a shift of the risk management cost curve, $Q(p^E)$, to the north-east in Figure 1, and result in a higher optimal probability of the end-of-period attack and larger costs of risk management, all else being equal. In this case, the reassessment of the risk management processes would affect how stakeholders deal with the firm generally, as they would perceive the firm to be riskier not just with respect to cyber risk but with respect to other risks as well.

We assume that management and stakeholders are rational when they learn about the risk of successful cyberattacks. However, the behavioral literature shows that individuals can ignore or underestimate risks (Kahneman and Tversky, 1972). Recent work in finance further shows that some low risk events can be neglected (e.g., Gennaioli, Shleifer, and Vishny, 2015). Other work shows that individuals can overreact to "fearsome risks," so that they think, after an occurrence of such risks, that these risks have a higher probability of occurrence than they actually do (Sunstein and Zeckhauser, 2011). When such risks manifest themselves, a reassessment of their loss distributions takes place. As a result, when an attack occurs, it leads customers and/or managers to reassess the importance of these risks. It is then possible for stakeholders (including shareholders) and/or managers to overreact to an attack in the sense that they might conclude that the probability of an attack is much higher than it actually is due to the availability heuristic (Tversky and Kahneman, 1973). Even when managers or stakeholders overreact, our model still applies if they use the loss distribution for the reassessment of cyber risk. If management believes that stakeholders will overreact to an attack, this means that the costs of an attack are higher.

Consider a firm that had an optimal level of overall risk before the attack. If the firm and its stakeholders learn that the cyber risk is greater than previously thought and the risk is above the optimal level after the attack, then the firm will seek to reduce risk. Assume that, for any type of risk, the cost of mitigating that risk is increasing and convex in the amount of the risk as we assume for cyber risk. With that assumption, it is optimal for the firm to seek to reduce risk across all types of risk exposures following a cyberattack. This is because it will be less costly for the firm to reduce any risk by a small enough amount than to reduce cyber risk by the same amount after it has already reduced it by some larger amount. The firm will also choose to reduce risk-taking incentives of management as it has become optimal for the firm to reduce its risk exposure.

2.3. Contagion effects

When the attack conveys information to the firm and its stakeholders, we would also expect it to convey information to the market about the value of competing firms. If the attack signals that management is not as competent as expected or that the firm is highly exposed to cyber risk related to firm-specific factors, the attack would be good news for competing firms. In contrast, the signal could be about the industry-wide risk and costs of cyberattacks in general. For instance, if the cost to the firm charged by stakeholders who are exposed to the risk increases because of the attack, stakeholders of industry competitors could also conclude that the cost of the risk of being exposed to an attack is higher than they thought. In this case, the value of competitors would fall. Since competitors would not bear the out-of-pocket costs, the competitors would lose less than the target. Importantly, in light of the behavioral literature, an attack on a firm within an industry can increase the awareness of the risk for stakeholders and firms throughout the industry.

2.4. Hypotheses

Our model leads to the following hypotheses regarding predictions about the shareholder wealth loss caused by cyberattacks:

Hypothesis 1 (no learning). In the case of full information and rational expectations, assuming that the loss distribution is unchanged by the attack and the firm is an all-equity firm, the attack results in a value loss of the firm's equity corresponding to the unexpected out-of-pocket costs and there is no reputation loss. If the firm is sufficiently financially constrained that the loss due to the attack makes the firm riskier for its stakeholders, the stakeholders will demand better terms from the firm, which is costly to the firm and is equivalent to a reputation loss.

Hypothesis 2 (learning). If the firm and its stakeholders learn from the successful attack, and the information is unfavorable, the wealth loss caused by the attack is higher than in the no learning case. If the attack reveals that cyber risk is higher than previously believed, the firm is perceived to be riskier and thus will seek to decrease its overall risk. As part of an attempt to decrease the risk, the firm will seek to increase its investment in risk management and will reduce the risk-taking incentives of management. In this case, the attack can cause a reputation loss even for an all-equity firm as its stakeholders demand better terms to transact with it. Though the firm will try to mitigate risk more to attenuate the reputation loss, the product demand from customers will be lower than before unless the firm manages to eliminate all the reputation loss immediately, so that the evidence of lower sales growth suggests that some of the shareholder wealth loss is attributed to a reputation loss. It is possible that the firm would learn from the breach that a lower probability of a breach is optimal, in which case post-breach sales might be higher.

Hypothesis 3 (contagion). If the attack reveals adverse information that is specific to the target, industry competitors are expected to benefit from the attack. However, if the attack reveals information about industry-wide cyber risk, such information is expected to reduce the value of the industry competitors.

3. Sample

To construct our sample of cyberattacks, we first start with all data breach incidents (6,328 incidents) covered in the PRC database over the period of 2005 to 2017.[11] We use the PRC database since firms are required to disclose data breaches to affected persons in a timely manner under the State Security Breach Notification Laws. In Online Appendix A, we discuss these State Security Breach Notification Laws and other regulations that govern firms' disclosure requirements for data breaches. We include only incidents in which a firm lost personal information by hacking or malware-electronic entry by an outside party (1,580 incidents). Our model applies to external attacks as well as to internal breaches. In untabulated tests, we construct a sample of 220 internal breaches using the same approach as the one we use for external breaches and find that these breaches exhibit considerable heterogeneity. Cyberattacks are also different from internal breaches in terms of the extent of the damage. Cyberattacks explain all recent large

[11] We obtain the data from the PRC's website, http://www.privacyrights.org/data-breach, which are downloaded on July 10, 2015 for the 2005-2014 sample period and on April 14, 2018 for the later sample period. Established to protect individuals' privacy, PRC, a nonprofit consumer and advocacy organization, located in San Diego, California, collects information about breach events from government agencies and verifiable news sources, and publishes the chronology of reported breach events involving loss of personally identifiable information that can be used to identify an individual in context (e.g., social security numbers, bank account information, emails, driver license numbers, and medical information) in the U.S. starting from 2005. The PRC classifies the attacks with the loss of personally identifiable information into breaches that result in financial information loss (e.g., loss of social security numbers and financial information such as credit card information) and others that result in no financial information loss (i.e., loss of driver license numbers and medical information). However, the PRC does not provide such a classification in recent years. Thus, we obtain the information after 2014 by manually searching event descriptions in the PRC database and news articles from *Factiva*. Although the PRC database also includes certain cyberattack incidents that do not involve the loss of personal information, we exclude these incidents from our sample to minimize the self-selection bias because they are not subject to cyberattack notification laws and firms may not have an obligation to disclose them. See also https://www.privacyrights.org/data-breach-FAQ for a detailed description of the data provided by PRC.

data breaches[12] and, thus, the consequences of these large-scale breaches, such as costs incurred from loss of operations and business disruption, tend to be less predictable than those of internal breaches in which the source of breaches are relatively easier to identify. We report announcement returns for a sample of 220 internal breaches later.

Next, we manually match organization names reported in the PRC database with firm names listed in Compustat and the Center for Research in Securities Prices (CRSP). When attacked firms are unlisted subsidiaries of listed firms, we consider cyberattacks as having occurred in their listed parent firms. If we cannot match organization names recorded in the PRC database with firm names in Compustat and CRSP, we search Capital IQ corporate profiles and other sources including company websites and *Factiva* to ensure the accuracy of their names for proper matching. We restrict the sample to attacked firms with financial and stock return data available in Compustat and CRSP, respectively. We require the sample firms to be listed on the New York Stock Exchange, the American Stock Exchange, or Nasdaq. These procedures yield a final sample of 307 cyberattacks for 224 unique firms, of which 163 are attacks on parents firms and 144 are attacks on subsidiaries.[13] Of 224 attacked firms, 51 firms (22.8%) experience

[12] Lists of the top data breaches do not appear to include internal breaches. See, for instance, "The 18 biggest data breaches of the 21st century," at https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.

[13] As discussed in Online Appendix A, the PRC database does not cover all cyberattack incidents of publicly listed firms in the U.S. due to the following two reasons. First, although most states have legislated state cyberattack notification laws by 2009, which require firms operating in the state to notify affected residents about cyberattack incidents, three states (i.e., Alabama, New Mexico, and South Dakota) had no such laws for the whole sample period. Second, even for incidents that are subject to state cyberattack notification laws, many states do not have legislation that requires the state government to collect data on cyberattack incidents and disclose the relevant information. Thus, it is possible that our sample underestimates the true extent of cyberattacks that affect publicly listed firms in the U.S. To check the representativeness of our sample, we independently search *Factiva* to locate news articles reporting cyberattack incidents in 2012 alone and compare the incidents reported by news media with

multiple cyberattacks during our sample period. In our sample, 73.9% of the reported cyberattacks involve financial information loss and the remaining 26.1% involve no financial information loss.

Table 1 presents a chronological distribution of the 307 cyberattacks by industry (SIC two-digit codes) and year. We find a generally increasing trend in the number of cyberattacks occurring over time: only four attacks occurred in 2005, in contrast to 46 in 2017. We also find that industries in which cyberattacks occur most frequently are service industries (31.27%), followed by finance (23.45%), manufacturing (17.59%) and wholesale trade and retail trade industries (15.96%), which suggests that firms that deal with a large number of customers are more likely to experience a cyberattack.

4. Likelihood of experiencing cyberattacks

To examine firm and industry characteristics that drive cyberattack incidents, we first compare the characteristics of firms that were successfully attacked, which we call targets, with those of firms that were not attacked successfully, which we call non-targets. As we focus only on cyberattacks that involve the loss of personal information subject to cyberattack notification laws, the sample used in this analysis represents the population of successful attacks where targets follow existing disclosure requirements as we understand them. When a firm experiences multiple cyberattacks in a given fiscal year, we treat all these multiple attacks as a single attack in that year, so the sample size reduces to 259 from 307. Table 2 presents summary statistics for 259 firm-year observations with cyberattack incidents and 54,717 firm-

---

those collected by the PRC database in 2012. We use the following keywords to locate the articles on cyberattack events in *Factiva*: "hacking," "hacked," "malware," "spyware," "cyber attack," and cyberattack." We restrict news sources to major wires including Dow Jones Newswires, Major News and Business Sources, Press Release Wires, Reuters Newswires, and The Wall Street Journal-All sources. We find that 18 incidents are covered in news media, of which 17 are included in the PRC database. The remaining one does not involve any loss of personal information and thus is not covered in the PRC database. Thus, it appears that the PRC database covers most of major cyberattack incidents.

year observations without cyberattack incidents covered in Compustat. It follows that the unconditional probability of a cyberattack in a given year for a firm in our sample is 0.47%. We winsorize all continuous variables at the 1st and 99th percentiles to mitigate the impact of outliers on our analysis.

Focusing on firm-level characteristics, we find that compared to firms experiencing no cyberattack, those experiencing cyberattacks are larger and older, and have a larger presence among *Fortune* 500 companies. These findings indicate that targets in our sample are more visible firms than non-target firms. Targets are also more profitable (higher ROA) and less risky (lower stock return volatility), have higher future growth opportunities (higher Tobin's *q*), higher leverage, and higher asset intangibility, and invest less in capital expenditures and R&D activities. Importantly, few targets are financially constrained. We report results using the index of Whited and Wu (2006), but results are similar with other indices. Using BoardEx board committee-level data, we also find that the proportion of firms having a risk committee on the board is higher for targets than for non-targets.[14] We consider a board having a risk committee if the name of its committee includes "risk" (e.g., Enterprise Risk Management Committee, Risk Management Committee, Audit and Risk Committee, and Risk Oversight Committee). Turning to industry-specific characteristics, we find that cyberattacks are more prevalent among firms operating in industries in which product market competition is less intense (measured by Herfindahl index and product uniqueness).

We turn next to a more direct examination of the likelihood of firms being targets. We use the data panel from Table 2 as the sample. Table 2 reports results of estimates of probit regressions in which the dependent variable is an indicator that takes the value one if a firm experiences a cyberattack in a given year, and zero otherwise.[15] We include several firm- and industry-level characteristics reported in Table 2

[14] When we exclude firms in finance industries (SIC 6000-6999) from the sample, we find the difference in the proportion of firms having a risk committee on the board between targets and non-targets (0.024 compared to 0.022) is insignificant. Thus, the difference in the existence of a risk committee between these two groups of firms reported in Table 2 is largely driven by firms in finance industries.

[15] We do not use hazard models in estimating the regressions in Table 3 due to the possibility of doubly censored data (i.e., the existence of multiple events for the same firm) in the analysis. Our sample may also not satisfy the

as explanatory variables that are measured one year before the attack (except Tobin's *q* that is measured two years before the attack since it is highly correlated with past stock performance). Using the lagged value of Tobin's *q* helps address the correlation issue since Tobin's *q* is directly affected by returns. In Regression (1), we include only firm-level characteristics as determinants. We also control for year and industry fixed effects (measured by two-digit SIC codes). We find that firms with higher visibility (measured by firm size, *Fortune* 500 membership, and institutional block ownership), higher valuations as measured by Tobin's *q*, higher ROA, higher asset tangibility, and fewer financial constraints are more likely to be targets of a cyberattack. In Regression (2), we add to Regression (1) an indicator for whether the firm has a risk committee (*Risk committee*), measured using the board committee information on BoardEx as discussed above. We control for the number of board committees in the regression. We see that firms with a risk committee are less likely to be targets. The sample is smaller as we require firms to have data available through BoardEx. With this smaller sample, we also find that younger and less leveraged firms are more likely to be targets. Though we do not report the results, we also estimate the regressions by adding corporate governance characteristics such as CEO-chair duality, the proportion of outside directors on the board, and board size to examine whether the quality of corporate governance can predict the likelihood of cyberattack incidents. We find that none of these variables is significant. This result seems to be specific to cyber risk since Chernobai, Jorion, and Yu (2011) show that good corporate governance plays an important role in reducing operational risk at U.S. financial institutions.

In Regression (3), we add industry variables that capture industry competition (Industry Herfindahl index and an indicator for unique industry) and future growth opportunities (industry Tobin's *q*). We find that cyberattacks are more likely in industries that face less intense product market competition (i.e.,

---

assumption of non-informative censoring that the mechanisms giving rise to censoring of the sample should not be related to the probability of an event occurring (Lagakos, 1979). For example, in our study, censored firms are unlikely to have the same probability of experiencing a subsequent event as firms that experience no cyberattacks.

industries with a higher Herfindahl index and more unique products) and industries with higher growth opportunities.

In Regression (4), we replace industry characteristics in Regression (3) with five industry indicators defined using the first two-digit SIC codes and omit the manufacturing industry as a reference group to examine whether cyberattacks are more likely in certain industries controlling for firm characteristics.[16] We find that among the major industries, cyberattacks are more likely in service industries, wholesale trade and retail trade industries, and transportation and communications industries. The coefficient on finance industries, however, is not significant. Hence, controlling for firm characteristics, it is not just the fact that a firm deals with large numbers of customers that makes an attack more likely.

Overall, the results in this section suggest that cyberattacks are more likely to occur in firms that are more visible, with greater valuations, more intangible assets, without a board risk committee, and in less competitive industries. Successfully targeted firms seem to rely more on customer personal information in doing business.

5. Impact of cyberattacks on shareholder wealth

In this section, we investigate the impact of cyberattacks on shareholder wealth using an event study. To identify cyberattack announcement dates, we search news articles reported in *Factiva* for the 188 attacks we identify. We also search *Factiva* for major confounding corporate events (e.g., announcements of mergers and acquisitions, earnings, and security issuance) within one trading day before and after the announcement and exclude observations associated with such news. Of 188 incidents, we are able to find 165 uncontaminated events in which news articles report cyberattacks and data on stock returns are not missing in CRSP. We use the date when a news article reporting the cyberattack appears in *Factiva* for

[16] In this regression, we exclude firms operating in three industries (agriculture, forestry, and fisheries industries, mineral and construction industries, and electric, gas, and sanitary services industries) because the number of cyberattacks is too low for statistical inference.

the first time as the initial public announcement date. The abnormal stock returns are calculated using the market model, the Fama-French (1993) three-factor model, and the Fama-French-Carhart (Carhart, 1997) four-factor model, respectively. The market model parameters are estimated using 220 trading days of return data beginning 280 days before and ending 61 days before the breach announcement, using either the value-weighted or the equally weighted CRSP index return as a proxy for the market return. The three factors used in the Fama-French (1993) three-factor model are the CRSP value-weighted index, SMB (daily return difference between the returns on small and large size portfolios), and HML (daily return difference between the returns on high and low book-to-market-ratio portfolios). The four factors used in the Fama-French-Carhart (Carhart, 1997) four-factor model are the CRSP value-weighted index, SMB, HML, and UMD (daily return difference between the returns on high and low prior return portfolios). Daily abnormal stock returns are cumulated to obtain the cumulative abnormal return (CAR) from day t_1 before the breach announcement date to day t_2 after the breach announcement date.

Panel A of Table 4 reports the mean and median CARs for various event windows. The mean CAR (-1, 1), CAR (-2, 2), and CAR (-5, 5) computed using the market model and the CRSP value-weighted index return are -0.84%, -1.10%, and -1.10%, respectively, all of which are significant. The corresponding median CARs are -0.52%, -0.81%, and -1.36%, all of which are also significant. The results using the CRSP equally weighted index return and those using the Fama-French (1993) three-factor model and the Fama-French-Carhart (Carhart, 1997) four-factor model are similar. In untabulated tests, we estimate stock-price reactions to 220 internal data breaches that we identify during our sample period for comparison. We find that announcement returns for 220 internal data breaches are generally insignificant. Specifically, we find that the mean for internal breaches computed using the market model and the CRSP value-weighted index return are -0.34%, -0.29%, 0.02%, respectively, of which only the CAR (-1, 1) is significant at the 5% level. The corresponding median CARs are small at -0.132%, 0.051%, and -0.078%, all of which are insignificant. When we use the CRSP equally weighted index return as the market portfolio return, none of the mean and median CARs are significant.

In Panel B of Table 4, we examine whether the stock-price reaction differs when personal financial information is stolen. We see that there is a highly significant difference in the stock-price reaction between cyberattacks involving financial information loss and the other cyberattacks. The average CAR (-1, 1) is -1.09% when there is financial information loss and an insignificant -0.23% when there is no such loss. Similarly, the corresponding average CARs (-2, 2) for cyberattacks with and without financial information loss are -1.46% and -0.20%, respectively. The difference is significant at the 10% level. Tests for the significance of median CARs using a non-parametric Wilcoxon signed-rank test show a similar pattern.

In untabulated tests, to examine whether the market reaction to cyberattacks worsens over time, we also divide our sample into two sub-periods, the early sub-period from 2005 to June 2011 and the late sub-period from July 2011 to 2017, and examine whether abnormal returns differ between these two sub-periods. We find that the mean (median) CAR (-1, 1) for the early sub-period is -1.37% (-0.81%) and the corresponding CAR (-1, 1) for the late sub-period is -0.65% (-0.46%), both of which are significant. The difference in mean (median) CARs (-1, 1) between the two sub-periods is insignificant.

In Panel C, we investigate the determinants of the shareholder wealth impact of cyberattacks using ordinary least squares (OLS) regressions in which the dependent variable is CAR (-1, 1). All regressions use year and industry fixed effects (two-digit SIC codes) except for Regressions (3) and (4). We use as explanatory variables firm size, log (firm age), ROA, leverage, sales growth, Tobin's *q*, and institutional block ownership. We also include an indicator that takes the value one if a firm's Whited and Wu's (2006) index (WW index) is above the top tercile in a given year, and zero otherwise (*Financial constraint*), an indicator that takes the value one if a cyberattack involves financial information loss, and zero otherwise (*Financial information loss*), and an indicator that takes the value one if a firm experiences another cyberattack incident within one year of the previous cyberattack, and zero otherwise (*Repeated cyberattacks within one year*).

In Regression (1), we include only *Financial information loss* in addition to year and industry fixed effects.[17] We find that the coefficient on *Financial information loss* is negative and significant at the 1% level. The coefficient of -0.018 suggests that cyberattacks that involve the loss of financial information lead to a 1.8 percentage points lower CAR (-1, 1) than those without such information loss. With a mean market value of about $58.93 billion for our sample firms, the coefficient estimate of -0.018 suggests that, all else being equal, cyberattacks with financial information loss result in an average value loss of more than $1.06 billion for the attacked firms than those that do not result in financial information loss.

In Regression (2), we add *Repeated cyberattacks within one year* and firm characteristics as additional explanatory variables. The coefficient on *Repeated cyberattacks within one year* is -0.025 and significant at the 10% level. The coefficient on *Financial information loss* is unchanged. It follows that repeated attacks within one year involving financial information loss yield a stock-price reaction worse by 4.3 percentage points than a first-time attack involving no information loss. Thus, firms experiencing repeated cyberattacks have a more significant negative valuation effect than those experiencing a single cyberattack. We also find that the market reaction is more negative when target firms are older and have higher leverage. The coefficient on the indicator variable for financially constrained firms is insignificant.

In Regression (3), we add industry characteristics and find that the stock price reaction is not affected by the degree of competition in an industry or by the uniqueness of industry products. However, firms in industries with better growth opportunities are more adversely affected by a cyberattack.

In Regression (4), as in Regression (4) of Table 3, we replace industry characteristics used in Regression (3) with five industry indicators identified according to the first two-digit SIC codes and omit

[17] Although the PRC provides the information about the number of records breached, we do not use such information in our analyses. First, about a half of the observations used in our event study analysis have missing values on the number of records breached. Second, reporting on the number of records breached is not standardized and varies by incident.

the manufacturing industries. We do not find that the impact of attacks is worse for any particular industry.

In Regression (5), we examine whether board oversight of firm risk affects the impact of cyberattacks on announcement returns. We view board oversight of firm risk as an indicator of higher investment in risk management. To capture board oversight of firm risk, we search a firm's 10-K and Def14A SEC filings.[18] Specifically, we define *Board attention to risk management* as an indicator that takes the value one if a specific board committee (e.g., Enterprise-Wide Risk Management Committee, Risk Committee, Audit and Risk committee, and Audit Committee that is responsible for risk oversight) or the board as a whole explicitly monitors firm-wide risks and risk management, and zero otherwise. We find that firms without board oversight of risk management experience a worse stock-price reaction by four percentage points than those with board oversight of risk management. In our model, such a result suggests that firms and stakeholders learn more from an attack when the target does not have board oversight of risk management.

In Regression (6), we examine whether the existence of a data breach notification law, which would influence managers' incentives to disclose the attack, affects the market reaction to a cyberattack announcement. For example, managers of targets not subject to state-level mandatory disclosure

[18] In Table 3, we use BoardEx to define *Risk committee* for a large sample of firm-year observations covered in Compustat. Since BoardEx provides only the names of board committees, we identify the existence of a risk committee on the board by checking whether the name of a board committee includes "risk." However, we find that some board committees whose names do not include "risk" still play an important role in firms' risk oversight. For example, eBay Inc. notes in its 2016 proxy statement that "While the board is ultimately responsible for risk oversight at eBay, the board has delegated to the Audit Committee the primary responsibility for the oversight of risks facing our businesses." Thus, using BoardEx data and focusing on board committee names alone does not allow us to accurately capture firms' risk oversight at the board level in the case of firms such as eBay. To overcome this limitation of using BoardEx in identifying board oversight of firm risk, we manually collect the data on firm's risk oversight by carefully reading 10-K and Def14A SEC filings for the relatively small sample used in Table 4.

requirements are likely to have greater incentives to withhold the bad news, which may cause more negative announcement returns than those for incidents without information withholding. To test this conjecture, we add *State law*, an indicator that takes value one if a firm is headquartered in a state in which a data breach notification law is effective in a given year, and zero otherwise, and find that its coefficient is negative and insignificant. However, it should be noted that, as discussed in Online Appendix A, a firm is required to disclose a breach based on the residency of the affected person, not based on the location of the breach. Given that a firm's affected persons (for instance, customers) do not necessarily reside in its headquarters state, this result should be interpreted with caution.

Next, we directly examine whether a firm's delay of discovery and reporting about its cyberattack affects its announcement return. To address this issue, we manually collect the information about the breach date and the date on which the data breach was discovered by the target or a third party by searching *Factiva*, breach reports disclosed by the state Attorney General's Offices, and cyber security expert blogs such as Krebs on Security. Using these dates, together with the announcement date obtained from *Factiva*, we then construct two variables: 1) *Delay of discovery*, which measures the number of days from the occurrence of the breach to the discovery of the breach by the firm and 2) *Delay of reporting*, which measures the number of days from a firm's discovery of the breach to the first media reporting. We use *Delay of discovery* to capture the extent to which the firm finds it difficult to fully discover a security breach caused by a cyberattack and *Delay of reporting* to capture the firm's reporting delay of its incident.[19]

[19] Online Appendix B presents summary statistics for these two variables: *Delay of discovery* and *Delay of reporting*. Because of limited information available in public sources and the difficulty to judge the exact timing of each event, the sample used in Online Appendix B is very small. We find that the average (median) number of days from the occurrence to discovery is 47.2 (14.5) for a sample of 40 firms with the information available. We also find that the average number of days from the discovery to the first media reporting is 16.2 for a sample of 67 firms with the information available. The Appendix also reports that the average number of days from a firm's discovery of the

In Regression (7), we examine how a firm's difficulty in discovering the breach affects its announcement return by adding the natural logarithm of *Delay of discovery*. Given that the sample size used in the regression is very small, we replace two-digit SIC codes used to control for industry fixed effects with Fama-French five industry codes. We find the market reaction is more negative when target firms spent more time to uncover the breach. This could reflect the fact that breaches that take more time to be fully discovered may be more far-reaching. Excluding year fixed effects from the regression does not change the result. In Regression (8), we examine how a firm's delay in reporting an attack affects its abnormal return by including the natural logarithm of *Delay of reporting*. We find that the coefficient on this variable is negative but not statistically significant.[20]

6. Do out-of-pocket costs explain shareholder wealth losses?

In this section, we examine whether the shareholder wealth loss is explained by out-of-pocket costs or whether there are other contributing components such as reputation costs. We first estimate out-of-pocket costs and shareholder wealth losses and then compare these two components to obtain the excess loss.

6.1. Estimate of out-of-pocket costs

Attacked firms incur several types of out-of-pocket costs caused by the attack in the post-attack period: investigation and remediation costs, legal penalties, and regulatory penalties (fines and penalties

---

breach to its reporting to the state regulator (a firm's SEC 8-K filing) is 27.9 (19.3) days for a sample of 35 (12) firms with the information available.

[20] For a subsample of 67 firms for which discovery dates are available, in untabulated tests, we compute the average market-adjusted buy-and-hold stock return (HPR) from the discovery date to one day before the media reporting date and find that it (0.002) is not significant, suggesting no information leakage prior to the attack announcements.

from regulators). We identify events in the post-attack period by searching Lexis-Nexis, West Law, an online legal research service, Factiva, 10-K filings, proxy statements, and annual reports of firms that publicly disclosure their cyberattack. We keep track of post-attack events by searching these sources up to three years after a firm's public disclosure of its first attack.[21] Panel A of Table 5 presents the breakdown of these out-of-pocket costs associated with 21 cyberattacks that have a negative CAR (-1, 1) when disclosed or with subsequent post-attack event announcement dates and also have information about out-of-pocket costs that we are able to obtain from various sources. An important caveat about our investigation of out-of-pocket costs is that we can only measure the costs that are voluntarily disclosed by firms or estimated by third parties. In particular, it is likely that firms do not disclose these costs if they are not material.

The first row presents investigation and remediation costs and other costs for eight cyberattacks. Investigation and remediation costs include expenses to hire experts to investigate the incident and to upgrade the IT system. Other costs include money stolen from bank accounts as well as costs that combine several items including remediation costs and costs that are difficult to disentangle. The mean investigation and remediation (other) cost is $89.25 million ($19.30 million) and the total investigation and remediation (other) cost is $535.50 million ($38.60 million).

In the second row, we report legal expenses including settlement costs for class-action lawsuits or other litigations, and other legal costs (e.g., attorney's fees) for ten attacked firms. We find that the average legal expenses ($61.33 million) tend to be smaller than the average costs for investigating the incidents and revamping the IT system although the total amount of legal expenses ($613.31 million) is larger than the total investigation and remediation costs. These results suggest that legal expenses are not likely to be the main source of costs resulting from cyberattacks.

[21] For 10K filings, we use the following keywords to locate information on a firm's losses associated with the cyberattack: "breach," "hack," "data," "security," "information," "intrusion," "remediation," "privacy," "legal proceedings," "penalties," "fines," "settlement," and "litigation."

In the third row, we report fines and penalties levied by regulators for two attacked firms. The mean cost is only $1.02 million, suggesting that regulatory costs borne by the attacked firm are extremely small.

The fourth row reports total out-of-pocket costs for 14 cyberattacks in which information about the total out-of-pocket costs is available but no detailed breakdown is available. The sum of total out-of-pocket costs is $1.25 billion with the mean and median total out-of-pocket costs of $89.07 million and $17 million, respectively. The last row reports total out-of-pocket costs for 21 cyberattacks in which either the information about their detailed breakdown is available or the information about the total out-of-pocket costs is available but their detailed breakdown is unavailable. When details of individual out-of-pocket costs are available, we sum up these individual costs to compute total costs. We choose the larger amount as total costs when the summation of individual costs is different from total costs reported in the fourth row. We find the total out-of-pocket cost of $1.72 billion with the mean and median total out-of-pocket costs of $82.01 million and $16 million, respectively.

6.2. Estimate of total shareholder wealth loss

To estimate the total shareholder wealth loss from a cyberattack, we classify post-attack events into four categories: 1) investigation by law enforcement agencies and regulatory bodies such as the Federal Bureau of Investigation (FBI), State Attorneys General, Federal Trade Commission (FTC), National Security Agency, and Securities and Exchange Commission (SEC), 2) repeated cyberattacks within three years of the first cyberattack,[22] 3) filings of class-action lawsuits and other litigations, and 4)

[22] As we keep track of post-attack events of a cyberattack up to three years, a cyberattack that occurs after three years is classified as a first-time cyberattack.

litigation settlements.[23] There are 91 public disclosures of the first-time attack made by 85 unique firms within three years.

Panel B of Table 5 shows the classification of post-attack events into these four categories. There are 56 post-attack events experienced by 28 firms: eight investigations by regulatory bodies, 18 repeated cyberattacks, 18 filings of class-action lawsuits and other litigations, and 12 litigation settlements. For 91 first-time attacks within three years, the mean (median) CARs from one day before to one day after the attack announcement date (CAR (-1, 1)) is a significant -0.72% (-0.70%). Although the mean and median CARs (-1, 1) around the announcements of investigations by regulatory bodies, repeated attacks, and litigation settlements in the post-attack period are all insignificant, the corresponding mean and median CARs (-1, 1) around the filings of class-action lawsuits and other litigations are -3.50% and -1.06%, respectively, of which the median CAR (-1, 1) is significant at the 10% level.[24]

In Panel C of Table 5, we report aggregate CARs (-1, 1) and total dollar market value losses associated with public disclosures of first-time cyberattacks within three years and post-attack events discussed above. Following the approach of Karpoff, Lee, and Martin (2008), we consider only first-time cyberattacks within three years that have a negative CAR (-1, 1) around the cyberattack announcement date or cyberattacks that are followed by at least one post-attack event with a negative CAR (-1, 1) around its announcement date. We then sum up CAR (-1, 1) for all announcements for the public disclosure of the first-time cyberattack within three years and four types of post-attack events. For each event, we compute a firm's total dollar market value loss by multiplying its CAR (-1, 1) around

[23] Unlike events that involve enforcement actions (e.g., financial misrepresentation), there are no typical sequences of enforcement process or events for firms experiencing cyberattacks. Of 91 first-time cyberattacks within three years, 59 (64.84%) do not experience any post-attack events.

[24] To check whether the significant median abnormal returns around the filing of class-action lawsuits and other legal actions against attacked firms are due to contaminated events, we search major events reported in *Factiva* within one day before and one day after the filing date and find no such contaminated events.

each event by its market value of equity 10 days before the event announcement date. We then sum up the dollar loss of all events.

In the first row of Panel C, we focus on a subsample of 21 cyberattacks for which either the first-time attack announcement or at least one post-attack event announcement has a negative CAR (-1, 1) and information about out-of-pocket costs is available. We find that the mean and median CARs (-1, 1) are -6.83% and -3.44%, respectively, the mean and median dollar losses are $1.15 billion and $0.26 billion, respectively, and the total dollar loss is $24.99 billion. In the second row, we use only a subsample of 20 cyberattacks for which either the first-time attack announcement or at least one post-attack event announcement has a negative CAR (-1, 1) and the firm experiences class-action lawsuits or other litigations in the post-attack period. We find that the mean and median CARs (-1, 1) are -8.04% and -4.13%, respectively, the mean and median dollar losses are $1.25 billion and $0.45 billion, respectively, and the total dollar loss is $24.16 billion. The last row shows the results for 75 cyberattacks that have a negative CAR (-1, 1) when the attack is disclosed or with subsequent post-attack event announcements. The aggregated mean and median CARs (-1, 1) for these cyberattacks are -3.61% and -1.70%, respectively, and the corresponding mean and median dollar losses are $1.39 billion and $0.26 billion, respectively. The total dollar market value loss computed by aggregating losses from all events amounts to $104.07 billion.

6.3. Comparison of total shareholder wealth losses and out-of-pocket costs

We next combine out-of-pocket costs in the post-attack period reported in Panel A with total dollar market value losses reported in Panel C to assess the relative importance of out-of-pocket costs and excess losses in total shareholder wealth losses. Our model predicts that the excess loss is zero if the attack does not reveal new information about cyber risk or the firm in general. If the excess loss is positive, it represents an upper bound of the reputation loss that the shareholders suffer (Karpoff, Lee, and Martin, 2008). The results are reported in Panel D of Table 5. The first column reports the results for a sample of 21 cyberattacks that have a negative CAR (-1, 1) when disclosed or with subsequent

post-attack event announcements and also have information about out-of-pocket costs that we are able to obtain. If total out-of-pocket costs exceed the total dollar shareholder wealth loss, the excess loss is set to zero. The excess loss that is computed by subtracting total out-of-pocket costs from the total dollar market value loss represents 93.48% of the aggregate shareholder wealth loss for these cases. The second column reports 75 cyberattacks that have a negative CAR (-1, 1) when disclosed or with subsequent post-attack event announcements. For cyberattacks for which we are unable to obtain information about out-of-pocket costs in the post-attack period, we set these costs to zero and use the total dollar shareholder wealth loss as the excess loss. We find that the aggregate loss in shareholder wealth for 75 cyberattacks is $104.07 billion. Since the total out-of-pocket costs for 75 cyberattacks are $574.1 million (not reported), the total excess loss is $102.97 billion, accounting for almost 98.94% of the total shareholder wealth loss. Similarly, in untabulated tests, we find that the mean (median) excess loss accounts for 98.49% (91.65%) of the mean (median) total shareholder wealth loss. Although it is not directly comparable, for their study of firms' financial misrepresentations, Karpoff, Lee, and Martin (2008) find that the mean (median) reputation loss for their sample constitutes 66.56% (92.09%) of the total shareholder wealth loss. Thus, the upper bound of the reputation loss in cyberattacks appears to be larger on average than for the events considered by Karpoff, Lee, and Martin (2008).

Overall, these results suggest that out-of-pockets costs are a small part of the loss experienced by shareholders in a typical attack where the shareholder wealth loss exceeds the out-of-pocket cost, while the excess loss, which is an upper bound for the reputation loss, represents a substantial portion of the total shareholder loss. We now turn to an investigation of the determinants of this excess loss.

7. Determinants of the excess loss

In our model, the excess loss consists of the reputation loss and other costs associated with learning. To understand better the nature of this excess loss, we investigate in this section whether there is evidence of reputation and learning effects following cyberattacks.

7.1. Difference-in-differences tests

With our model, a beginning-of-period attack that worsens the loss distribution of cyber risk should be associated with a decrease in the firm's future performance to reflect rising costs borne by the firm due to worsening of the terms on which the firm transacts with stakeholders and increasing exposure to cyber risk. To evaluate whether an attack increases the expected cost of cyber risk for the firm and changes the terms on which stakeholders transact with the firm, we perform difference-in-differences tests using firm-year observations three years before and three years after the attack. Since our difference-in-differences tests require three years of financial and stock return data after the attacks, we do not include attacks that occur after 2014 in these analyses. We consider only attacks that result in financial information loss since the analysis in Section 5 shows that the negative impact of cyberattacks on firm value is concentrated in such events. For firms that experience multiple cyberattacks during our sample period, we include only the first attack.

For each treatment firm, we then identify a control firm that does not experience cyberattacks using propensity-score matching. The propensity score is calculated using the logit regression of *Cyberattack* (an indicator that takes the value one if a firm experiences a cyberattack in a given year, and zero otherwise) on firm size, stock performance, stock return volatility, leverage, and the existence of an institutional blockholder (indicator). We require both treated and matched firms to be in the same industry (measured by two-digit SIC codes) as cyberattacks are concentrated among certain industries as shown in the previous section. We also require treated and matched firms to be in the same fiscal year, so the control firm has an "artificial" cyberattack year even if it does not experience a cyberattack (Chan, Chen, and Chen, 2013). This approach allows us to perform difference-in-differences tests for the changes in performance, financial health, and corporate policies surrounding the cyberattack. We then match, without replacement, a target with a non-target control firm that has the closest propensity score with a caliper of 0.1 and a common support range of 0.1 to 0.9 (Caliendo and Kopeinig, 2008). It is possible that a matching firm experiences an internal data breach although it does not experience a cyberattack in a

given year. Using our database of 220 internal data breaches, we find five control firms experiencing an internal data breach. Excluding these firms and their matched treatment firms does not affect our results.

Panel A of Table 6 presents descriptive statistics for a sample of 226 propensity-score matched sample firms (113 firms with a cyberattack that results in financial information loss and their 113 matching firms).[25] We find no significant difference between targets and their matching non-targets, suggesting our matching approach identifies matching firms that are very similar to treatment firms.

We use the following difference-in-differences regression specification:

$$OP_{it} = \alpha + \beta Post_{it} \times Cyberattack_{it} + \gamma_t + \omega_i + \varepsilon_{it}, \quad (4)$$

where OP_{it} is operating performance for firm i at time t. We measure firm operating performance using four variables: sales growth, ROA, ROE, and cash flow/assets. In subsequent analyses, we replace *OP* with the variables that measure firm risk and corporate policies. $Post_{it}$ is an indicator that takes the value one for firm-years in the post-attack period (year t, year t+1, and year t+2), and zero for the pre-attack period (year t-1, year t-2, year t-3), where year t is the fiscal year in which a cyberattack occurs. $Cyberattack_{it}$ is an indicator that takes the value one if firm i at time t experiences a cyberattack, and zero if firm i at time t is a non-target control firm. Our key independent variable of interest is the interaction term between *Post* and *Cyberattack*. We include industry (Fama-French 48 industries)-year-cohort fixed effects (γ_t) since the effects of cyberattacks that occur in a specific industry in recent years may be different from those that occur in the industry in earlier years due to the changing nature of cyberattacks over time. We include firm fixed effects (ω_i) to account for unobserved heterogeneity across firms and to

[25] We find that nine (two) out of 113 (113) control (treatment) firms are delisted as a result of mergers or voluntary delisting within three years of cyberattacks. Delisting of two control firms are triggered by performance-related reasons (delisting codes 500, 505 to 588) (Shumway and Warther, 1999). Thus, survivorship bias is unlikely to be a concern for our matching sample.

allow the heterogeneity to vary across paired groups. Note that we do not control for time-varying firm-specific variables in the regression since these firm characteristics can be affected by cyberattacks and thus including them in the regression biases estimates of the interaction term between *Post* and *Cyberattack*.

In a separate regression, we also break down the interaction term between *Post* and *Cyberattack* into interaction terms for three subperiods in the post-attack period: $Year_t$, $Year_{t+1}$, and $Year_{t+2}$. In this regression, we include firm-specific variables as additional controls. The reason for including controls is that firm characteristics in years after the attack could affect operating performance in these years. Hence, the interpretation of the coefficient on the interaction term involving *Post* for year t+1, for instance, would be the impact of the attack at t+1 given how firm characteristics have evolved up to that year.[26] The number of firm-year observations differs across the regressions depending on the availability of variables computed using Compustat, CRSP, and ExecuComp data.

7.2. Impact on sales growth and operating performance

Panel B of Table 6 reports regression estimates using sales growth as a dependent variable. We find that an attack has a significantly negative impact on sales growth, which shows clear evidence of a reputation cost arising from weakening customer confidence in the attacked firm. We also expect declining firm performance in the post-attack period, but for the whole sample we find no significant impact of cyberattacks on ROA, ROE, and cash flow/assets. The lack of significance of ROA, ROE, and cash flow/assets for the full sample may be due to the fact that the impact of cyberattacks on operating

[26] In untabulated tests, we also divide the sample according to the sample median values of the Kaplan and Zingales' (1997) index, the Whited and Wu's (2006) index, and the S&P credit rating score, and whether the firm is a dividend payer in a given year and reestimate all the regressions in Tables VI through IX. We find no systematic evidence that firms' performance, financial health, or corporate policies in the post-attack periods are affected by the extent to which they are financially constrained.

performance varies across firms and industries. We show in Panels C, D, and E of Table 6 that this heterogeneity across firm types and industries indeed matters to explain the impact of cyberattacks on operating performance. In Panel C, we divide the sample into two subgroups according to median firm size (total assets). We find that large firms experience a significant decrease in sales growth, ROA, and cash flow after the attacks. The decrease in sales growth is of 3.4 percentage points (Regression (1)), which is large compared to the average sales growth of 8 percent the year before the attack for the sample of targets. We see in Panel D that ROA and cash flow deteriorate significantly for firms in durable goods industries, which produce more unique products and impose higher liquidation costs on customers than other industries (Titman, 1984). In Panel E, we find that sales growth falls by 5.4 percentage points following attacks for firms in retail industries. Hence, for subsamples of large firms, firms in durable goods manufacturing industries, and firms in retail industries, the negative impact of cyberattacks on operating performance is more pronounced.

7.3. Impact on firm financial health

Bondholders and firm creditors as stakeholders of attacked firms may also demand better terms from the firms for their greater risk exposure and declining firm performance. Table 7 provides evidence of a decrease in S&P credit ratings, which is consistent with that prediction. We convert alphabetical symbols of S&P domestic long-term issuer credit ratings from AAA+ to D into rating scale numbers (highest = 23, lowest =1) with higher numbers indicating better ratings. There are 503 firm-year observations (39.0%) with no credit rating available. We exclude these firms in estimating Regressions (1) and (2).[27] We find that the coefficient on the interaction term between *Post* and *Cyberattack* is negative and significant at the 10% level in Regression (1), suggesting that targets experience deteriorating credit ratings in the post-

[27] In untabulated tests, we assign a rating scale number of zero for firms with no credit rating available, include an indicator that takes the value one for these firms in Regressions (1) and (2), and then reestimate the regressions. We find that our results do not change.

attack period. The average three-year impact is -0.325, which corresponds to one third of a rating notch. Focusing on each post-attack year separately (i.e., years *t*, *t*+1, and *t*+2) in Regression (2), we find that the decrease in credit rating is persistent for each of three years after the attack.

With our model, we also expect stakeholders to demand better terms from the attacked firm partly due to their concerns about the firm's weakening financial position and its higher default risk after the attack. Consistent with this expectation, we find that the firm is financially weaker after an attack. In other words, the firm does not choose to raise equity to offset the impact of the attack. Specifically, in Regressions (3) and (4), we use the bankruptcy score (Shumway, 2001) as a measure of financial health and find that the coefficient on the interaction term between *Post* and *Cyberattack* is positive and significant at the 10% level in Regression (3) for the three-year average. The coefficient is also positive and significant for $Year_{t+1}$ in Regression (4), providing some evidence of an increase in bankruptcy probability. In Regressions (5) and (6), we assess the impact of cyberattacks on the ratio of net worth (stockholder equity) to total assets. A lower ratio of net worth to total assets means that the firm has less of a cushion to cope with adversity. We see a significant reduction in this ratio for targets after the attack.

7.4. Impact on risk management policies

Next, we examine how target firms change their risk management policies in the post-attack period. While attacked firms often announce an investment in revamping their IT security systems and other follow-up measures, little is known about whether and how a cyberattack affects a firm's overall risk management policies. If a firm has an optimal risk management policy before the cyberattack and does not learn anything from the attack, our model predicts that the firm's risk appetite and its risk management policy do not change. However, if the firm and its stakeholders learn that the firm is riskier, we expect it to invest more in risk management and to take fewer risks.

We measure a firm's commitment to risk management using three variables. First, we measure it at the board level using the same variable as that used in Table 4, *Board attention to risk management*. We also decompose this indicator into two different indicators to examine the extent to which a firm is

committed to overhauling its risk management policy. The first indicator is *Risk oversight with committee*, which is a variable that takes the value one if a board committee's explicit duty involves ERM/firm-wide risk management oversight, and zero otherwise. The second indicator is *Risk oversight without committee*, which is a variable that takes the value one if a firm does not have any specific board risk committee but the board as a whole oversees ERM/firm-wide risk management, and zero otherwise.

Table 8 reports results of OLS regressions. In Regressions (1) and (2), we use *Board attention to risk management* as the dependent variable and find that targets' boards are more likely to increase their attention to firm-wide risk management after the attack than non-targets by a significant 19 percentage points following attacks. In Regressions (3) and (4) and Regressions (5) and (6), we use *Risk oversight with committee* and *Risk oversight without committee*, respectively, to measure a different level of a firm's commitment to risk management policies in the post-attack period. We find that our results in Regressions (1) and (2) mainly come from *Risk oversight with committee*.[28]

In columns (7) and (8), we use a more restrictive definition of board attention to risk: *Existence of committee with risk name*, which is an indicator that takes the value one if the name of a firm's board committee includes "risk" and its explicit duty involves oversight of firm-wide risk and risk management, and zero otherwise. We find that the results are similar to those in Regressions (3) and (4) that use *Risk oversight with committee* as the measure of board attention to risk.[29]

[28] We repeat our analysis in Table 8 after excluding firms in financial industries (SIC 6000-6999). We find that excluding financial firms does not change our results.

[29] In Online Appendix C, we examine the effect of cyberattacks on a firm's commitment to other approaches to risk management including the presence of the Chief Information Officer (CIO) and the proportion of outside directors with prior CIO experience to the total number of directors on the board. We find that attacked firms are more likely to hire CIOs and actively look for board members with CIO experience in the post-attack period. We also investigate whether a firm's decision to invest in risk management policies in the post-attack period is affected by their customer clientele. We find that an increase in cybersecurity investment in the post-attack period measured by the presence of the CIO and the proportion of outside directors with CEO experience is concentrated among firms that

Overall, we find that victims of a cyberattack are more likely to increase board oversight of firm risk, suggesting that, after an attack, the board reassesses the firm's risk exposure and its costs.

7.5. Compensation policies

A cyberattack could result in a drop in CEO compensation if the attacked firm's board believes that its CEO handled the risk management poorly or did a poor job in handling the aftermath of the attack. Alternatively, it is also possible that the firm has to find a new CEO and hence the pay of the CEO increases as the skills expected from the new CEO may be scarce in the CEO labor market. We find that CEO turnover following an attack is rare, which is consistent with evidence in Larcker, Reiss, and Tayan (2017). Specifically, we find only seven turnover instances following the breach. On average, the compensation of the incoming CEO is not meaningfully different from the compensation of the departing CEO.

If the attack leads to a reassessment of the firm's risk exposures and risk appetite, we would also expect the board to change the CEO's risk-taking incentives. Specifically, if the board finds the firm to be riskier than it thought or concludes that the firm's risk appetite was too high, it would want to reduce the CEO's risk-taking incentives by adjusting the composition of equity-based compensation. A decrease in option grants reduces the sensitivity of CEO wealth to stock volatility (i.e., CEO vega) but it also reduces the sensitivity of CEO pay-performance sensitivity (i.e., CEO delta). Consequently, we would expect non-option share compensation to increase to preserve the CEO's incentives to increase firm value if the CEO receives fewer option grants. To test these predictions, we obtain information on CEO compensation for targets from ExecuComp. There are 88 firm-year observations in which CEO compensation data are

---

sell more unique or specialized products (measured as the ratio of a firm's selling expenses to sales (Titman and Wessels, 1988). The findings suggest that firms' post-attack investment in risk management policies is greater for firms that sell more unique products and thus cater to customers with higher demands for data security.

available. We then use the same propensity score matching approach used earlier to create 88 matching non-target firm-year observations covered in ExecuComp.

Table 9 reports the results for the effect of cyberattacks on CEO pay components. In addition to controlling for firm characteristics used in the previous regressions, we also control for stock performance and various CEO characteristics such as CEO-chair duality, CEO age, and CEO tenure. In Regressions (1) and (2), we use log (1 + CEO total pay) as the dependent variable. We find that CEO total pay does not significantly change in the post-attack period. We then decompose CEO total pay into fixed salary, bonus, and equity-based compensation (options plus restricted stocks) and use the ratio of each of these component payments to CEO total pay as the dependent variables in the next ten regressions. We find that the coefficients on the interaction term between *Post* and *Cyberattack*, $Year_t$, $Year_{t+1}$, and $Year_{t+2}$ are insignificant when we use the ratio of salary to CEO total pay as the dependent variable (Regressions (3) and (4)), while they are all negative and significant at the 1% level when we use the ratio of bonus to total pay as the dependent variable (Regressions (5) and (6)). The coefficient estimate of -0.050 for the interaction term between *Post* and *Cyberattack* in Regression (5) suggests that for the three years after the cyberattack, the ratio of bonus to total pay for CEOs of targets falls by 5 percentage points. When we use the ratio of equity-based compensation to total pay as the dependent variable, the coefficients on the interaction term between *Post* and *Cyberattack*, $Year_t$, $Year_{t+1}$, and $Year_{t+2}$ are insignificant, suggesting that boards do not change the proportion of CEOs' equity-based compensation after a cyberattack (Regressions (7) and (8)).

As a further test of the effect of cyberattacks on equity-based compensation, we estimate Regressions (7) and (8) separately for restricted stock grants (Regressions (9) and (10)) and option awards (Regressions (11) and (12)). Prior studies show that stock options and restricted stocks do not share common features in influencing managers' risk-taking incentives. For example, Guay (1999), and Coles, Daniel, and Naveen (2006) show that stock options are used to encourage managers to take value-increasing risky projects and are effective at countering managerial risk aversion. On the other hand, although restricted stocks, another form of equity-based pay, can provide managers with incentives to

increase stock prices, they lack the convexity of options and hence their value does not increase with the firm's volatility in the same way as options (e.g., Smith and Stulz, 1985; Bryan, Hwang, and Lilien, 2000; Bakke et al., 2016). Since restricted stocks expose risk-averse managers to the downside risk of the stocks, they are likely to make these managers more cautious.

We find that the proportion of restricted stock grants to CEO total pay increases significantly in the post-attack period, while the proportion of option awards to CEO total pay decreases significantly during the same period. For example, during the three years after the cyberattack, the proportion of restricted stock grants for targets on average increases by a significant 10.4 percentage point, while that of option grants declines by a significant 6.6 percentage point. Given that the level of post-attack CEO total pay is similar for targets and non-targets, these results suggest that target firms' boards adjust the components of equity-based compensation in the years after cyberattacks by replacing stock options with restricted stock. The increased usage of restricted stock in place of stock options would decrease the CEO's incentives to take high-risk projects. In untabulated tests, we find that these changes in the post-attack compensation policy indeed lead to a significant decrease in CEO vega for target firms after the attacks.[30]

Overall, Table 9 shows that, after the attack, the board decreases the CEO's risk-taking incentives, which is consistent with *Hypothesis 2* that if the attack reveals that the firm's cyber risk is higher than previously believed, it will seek to decrease its overall risk based on its learning.

7.6. Contributing factors to the total loss

Thus far, we show that cyberattacks are followed by changes in firm performance and policies, supporting *Hypothesis 2* that the firm and its stakeholders learn from the cyberattack. When stakeholders

[30] In untabulated tests, we examine the likelihood of post-attack CEO changes. We identify CEO changes each year from ExecuComp. We find that the coefficients on the interaction term between *Post* and *Cyberattack*, $Year_t$, $Year_{t+1}$, and $Year_{t+2}$ are insignificant, suggesting that the likelihood of CEO turnover is not significantly higher in targets than in non-targets after the attack.

learn that the firm has become riskier than they thought it was, they change the terms on which they deal with the corporation. Hence, we would expect the excess loss to be related to the changes that take place after the attack. In Table 10, we report regression results showing that this is the case. We use the ratio of the excess loss to the total dollar market value loss as the dependent variable and investigate whether this ratio is higher for larger firms, for retail firms, for firms experiencing more of a sales growth drop, and for firms that invest in risk management. *Big firm* is an indicator that takes the value one if the median firm size in the post-attack period (i.e., year t, year t+1, and year t+2, where year t is the fiscal year in which a cyberattack occurs) is above the sample median, and zero otherwise. *Big drop in sales growth* is an indicator that takes the value one if the change in sales growth from year t to the median sales growth in the post period is below the sample median, and zero otherwise.

In Regression (1), we find the coefficient on *Big firm* is positive and significant, while that on *Retail industry* is negative and significant. The coefficient on *Big drop in sales growth* is insignificant. In Regression (2), we include the interaction term between *Retail industry* and *Big drop in sales growth* and find that its coefficient is positive and significant, while the coefficient on *Retail industry* remains significantly negative, suggesting that the reputation loss is greater when attacked firms operating in retail industries experience a larger drop in sales in the post-attack period. In Regression (3), we include the interaction term between *Big firm* and *Big drop in sales growth*. The coefficient on the interaction term is positive and significant, indicating that larger firms experiencing a sharp decline in sales growth suffer a greater excess loss, so that the upper bound of the reputation loss is higher. In Regression (4), we add an indicator that takes the value one if a firm has a board committee that includes "risk" in the name in the pre-attack period, and zero otherwise (*Existence of committee with risk name*) and find that its coefficient is negative and significant at the 1% level. This finding suggests that the excess loss is relatively less for firms that invest more in risk management in the pre-attack period. Such a result seems puzzling in that, in our model, firms that invest less in risk management are those that expect a breach to be less costly. However, the result is consistent with our model if firms that invest less in risk management learn more adverse information from the breach. For instance, these firms could have been too optimistic about the

costs of a breach, so that with the benefit of hindsight, they learn that they invested suboptimally in risk management.The χ^2 goodness of fit test indicates that the models explain a significant portion of the cross-section variation.

8. Impact on Industry Competitors

Hypothesis 3 in Section 2 predicts that if an attack has adverse information that is idiosyncratic about the firm, competitors should benefit from it. Alternatively, if the information learned about the attack is related to more general industry-wide cyber risk, we expect competitors to be affected adversely. In this section, we test these predictions by examining how cyberattacks affect industry peer firms' market values.

Panel A of Table 11 shows the CARs for value-weighted and equally weighted portfolio returns of industry peer firms. We define peer firms as all other firms that share the same four-digit SIC codes as the attacked firms.[31] We find that the mean value-weighted portfolio CAR (-1, 1), CAR (-2, 2), and CAR (-5, 5) are -0.37%, -0.62%, and -0.92%, respectively, all of which are significant at the 1% level. The corresponding median CARs are also negative and significant. The results for equally weighted portfolio CAR (-1, 1), CAR (-2, 2), and CAR (-5, 5) are also similar. Overall, the univariate results reported in Panel A suggest that cyberattacks, on average, negatively affect industry peer firms' market values, so that attacks reveal adverse information about industry-wide cyber risk in general.

In Panel B, we use as the dependent variable the value-weighted peer firm portfolio CAR (-1, 1). We use as explanatory variables *Attacked firm CAR (-1, 1)* and characteristics of cyberattacks (i.e., *Financial information loss (indicator)* and *Repeated cyberattacks within one year (indicator*)). We also

[31] We require that peer firms do not experience a cyberattack in a given fiscal year. We further exclude peer firms if they experience major confounding corporate events (e.g., announcements of mergers and acquisitions, earnings, dividends, and management guidance) within one trading day before and after the cyberattack announcement. These procedures yield a final sample of 6,094 peer firms.

include the correlation between value-weighted peer firm portfolio returns and attacked-firm returns for the year preceding the cyberattack announcement (*Return correlation*), the natural logarithm of the average stock price of the peer firm portfolio (*log (average price)*), and other firm characteristics measured in the fiscal year immediately before the cyberattack announcement used in Panel C of Table 4. In Regression (1), we find that the coefficient on *Attacked firm CAR (-1, 1)* is 0.141, which is significant at the 1% level. This coefficient suggests that the CAR (-1, 1) for the portfolio of an attacked firm's industry peer firms decreases by 0.51% as the CAR (-1, 1) for the attacked firm decreases by one standard deviation (3.62%). Given that the mean value-weighted peer firm portfolio CAR (-1, 1) is -0.37%, this number is economically large and significant. In Regressions (2) and (3), we include industry characteristics of attacked firms as additional explanatory variables. In Regression (2), we find that the coefficient on the interaction term between *Financial information loss* and *Finance industry* is negative and significant at 10% level, indicating that peer firms suffer more when the cyberattack occurs in the financial industry and their incidents are associated with financial information loss. In Regression (3), we find that the coefficient on the interaction term between *Repeated cyberattack within one year* and *High competition*, which takes the value one if a firm operates in the industry whose Herfindahl index is below the sample median, and zero otherwise, is positive and significant at the 5% level. Thus, peer firms suffer less when attacked firms experience a repeated attack and the industry is highly competitive.

In Online Appendix D, we investigate how the effect of an attack differs across firms within an industry. We find that although cyberattacks, on average, negatively affect individual industry peer firms' market values, some peer firms such as well-performing firms, high-growth firms, firms with more outside directors, and firms that are located proximately to the attacked firm are hurt less by the attack and may even benefit from it.

It is clear from our evidence that, overall, attacks are contagious to firms in the same industry and that the loss experienced by industry peers is economically and statistically significant. These results suggest that an attack conveys important adverse information about industry-specific cyber risk. Part of this

adverse impact may be that some stakeholders in industry peer firms conclude that cyber risk is higher than they previously believed and expect better terms to deal with the firms.

9. Summary and Conclusion

In this paper, we develop and test a model where a firm has an optimal exposure to cyber risk. We believe that this model applies in other situations where stakeholders are exposed to a risk born by a firm. An important feature of our model is that a risk-neutral firm benefits from risk management if its stakeholders care about the risk they bear because of their interactions with the firm. The compensation required by stakeholders to bear the risk of an attack means that it is optimal for the firm to invest more in risk management to reduce the risk of an attack. With rational, fully informed agents and with no hysteresis, a successful cyberattack consistent with agents' pre-attack information should have no impact on a financially unconstrained target's reputation and post-attack policies. However, if the attack provides a valuable signal to the firm and its stakeholders about the cost of attacks and the likelihood of future attacks, we expect the new information to affect firm value. When the firm and its stakeholders learn that a cyberattack has greater costs or likelihood than previously believed, firm value will fall to reflect these increased costs and likelihood. Part of these costs are so-called reputation costs due to stakeholders wanting better terms to deal with the firm going forward as they will take more risk in their interactions with the firm.

We find that attacks that do not involve the loss of personal financial information do not cause a significant shareholder wealth loss. In contrast, attacks where personal financial information is lost involve a significant shareholder wealth loss. For the attacks for which out-of-pocket losses can be computed and shareholders experienced a significant wealth loss, total out-of-pocket costs account for only $1.7 billion of a total shareholders wealth loss of $24.99 billion. Thus, although it is possible that we underestimate out-of-pocket costs, most of the shareholder wealth loss is attributable to other factors, such as the new information about the likelihood and the costs of cyberattacks for the target, and the impact of this new information on the risks borne by stakeholders. We find evidence of such reputation costs as

sales growth and credit ratings drop for attacked firms. Importantly, we further find that the shareholder wealth loss is related to these reputation costs: firms whose sales growth drops more experience a higher shareholder wealth loss in excess of out-of-pocket costs.

In the absence of new information from a cyberattack, the firm's risk management policies and risk appetite should stay the same. In contrast, we find that attacked firms invest more in risk management and decrease their risk appetite by reducing risk-taking incentives of management.

Lastly, if the impact of an attack reveals only idiosyncratic information about the target, we would expect industry competitors to benefit from the attack. In contrast, we find that shareholders of these competitors experience a shareholder wealth loss as well. Such a result is consistent with the view that the new information revealed by the attack increases the expected costs of attacks for competitors as well.

Appendix

This appendix provides detailed descriptions of all the variables used in the tables.

Variable	Description	Source
Asset intangibility	1– total property, plant and equipment (*ppent*) / total assets (*at*)	Compustat
Bankruptcy score	e^X / (1+ e^X) where X = −13.303 − 1.982 × net income (*ni*) / assets (*at*) + 3.593 × liabilities (*lt*) / assets (*at*) − 0.467 × log (price close (*prcc_f*) × common shares outstanding (*csho*) / market value of securities used (*usdval*) − 1.809 × abnormal returns + 5.791 × standard deviation of returns (Shumway, 2001)	Compustat, CRSP
Board attention to risk management (indicator)	One if a firm's specific board committee or a board as a whole oversees firm-wide risk and risk management, and zero otherwise	10-K and Def 14a SEC filings
Bonus / CEO total pay	Ratio of bonus awarded to CEO total compensation (*tdc1*)	ExecuComp
CAPX / assets	Capital expenditures (*capx*) / total assets (*at*)	Compustat
Cash flow / assets	[Income before extraordinary items (*ib*) + depreciation and amortization (*dp*)] / total assets (*at*)	Compustat
CEO-chair duality (indicator)	One if the CEO is also the chair of the board, and zero otherwise	BoardEx
Cyberattack (indicator)	One if a firm experiences hacking or malware-electronic entry by an outside party, malware, and spyware, and zero otherwise	PRC
Delay of discovery	Number of days from the occurrence of the breach to the discovery of the breach by the firm	*Factiva* and other sources
Delay of reporting	Number of days from a firm's discovery of the breach to the first media reporting	*Factiva* and other sources
Durable goods industries (indicator)	One for industries with SIC codes of 3400 and above but less than 4000, and zero otherwise (Titman and Wessels, 1988)	Compustat
Equity-based compensation / CEO total pay	Ratio of the total dollar amount of options and restricted stocks awarded to the CEO during a fiscal year divided by CEO total pay (*tdc1*) in the same fiscal year	ExecuComp
Existence of committee with risk name (indicator)	One if the name of a firm's board committee includes "risk" and its explicit duty involves firm-wide risk and risk management oversight, and zero otherwise	10-K and Def 14a SEC filings
Financial constraint (indicator)	One if a firm's WW index (Whited and Wu, 2006) is in the top tercile of the sample in a given year, and zero otherwise.	Compustat
Financial industry (indicator)	One for industries with SIC codes of 6000 and above and less than 7000, and zero otherwise	Compustat
Financial information loss (indicator)	One if a firm experiences a cyberattack involving the loss of social security numbers or credit card/bank account information in a given fiscal year, and zero otherwise	PRC
Firm size	Natural logarithm of total assets (*at*)	Compustat
Fortune 500 membership (indicator)	One if a firm is included in the list of *Fortune* 500 companies in a given year, and zero otherwise	Compustat
Industry Herfindahl Index	Index computed as the sum of squared market shares of firms' sales at the two-digit SIC industry level	Compustat
Industry Tobin's *q*	Median Tobin's *q* of all firms in the same two-digit SIC code industries in a given year	Compustat
Institutional block ownership	Number of shares held by institutional shareholders that own more than 5% of a firm's equity scaled by the total number of shares outstanding	Thompson13F
Log (1 + CEO total pay)	Natural logarithm of (1 + CEO total compensation (*tdc1*))	ExecuComp
Log (average price)	Natural logarithm of the average stock price of the peer firm portfolio	CRSP
Log (firm age)	Natural logarithm of max (years in CRSP, years in Compustat)	Compustat, CRSP

Net worth	Stockholder equity (*seq*) / total assets (*at*)	Compustat
Number of board committees	Number of board committees in a given fiscal year	BoardEx
Option awards / CEO total pay	Total dollar amount of stock options awarded to the CEO during a fiscal year divided by CEO total pay (*tdc1*) in the same fiscal year	ExecuComp
R&D / assets	Max (0, R&D expenditures (*xrd*)) / total assets (*at*)	Compustat
Repeated cyberattacks within one year (indicator)	One if a firm experiences another cyberattack within one year of the previous cyberattack, and zero otherwise	PRC
Restricted stock grants / CEO total pay	Total dollar amount of restricted stocks awarded to the CEO during a fiscal year divided by CEO total pay (*tdc1*) in the same fiscal year	ExecuComp
Retail industry (indicator)	One for industries with SIC codes of 5,200 and above but less than 6,000, and zero otherwise	Compustat
Return correlation	The correlation between value-weighted peer firm portfolio returns and attacked-firm returns for the year preceding the cyberattack announcement	CRSP
Risk committee (indicator)	One if the name of a firm's board committee includes "risk," and zero otherwise	BoardEx
Risk oversight with committee (indicator)	One if a board committee's explicit duty involves firm-wide risk and risk management oversight, and zero otherwise	10-K and Def 14a SEC filings
Risk oversight without committee (indicator)	One if a firm does not have any specific board risk committee but the board as a whole oversees firm-wide risk and risk management, and zero otherwise	10-K and Def 14a SEC filings
ROA	Net income (*ni*) / total assets (*at*)	Compustat
S&P credit rating	Scale numbers of alphabetical symbols of S&P domestic long term issuer credit ratings (*splticrm*) ranging from AAA+ to D (highest=23, lowest=1)	Compustat
Salary / CEO total pay	Total dollar amount of salary paid to the CEO during a fiscal year divided by to CEO total compensation (*tdc1*) in the same fiscal year	ExecuComp
Sales growth	$Sales_t$ / $sales_{t-1}$	Compustat
State law (indicator)	One if a firm is headquartered in a state in which a data breach notification law is put in place in a given year, and zero otherwise	Perkins Coie law firm website
Stock performance	Buy-and-hold return for the year net of the CRSP value-weighted index return	CRSP
Stock return volatility	Standard deviation of a firm's daily stock returns during a fiscal year	CRSP
Tobin's *q*	[Total assets (*at*) – common/ordinary equity (*ceq*) + market value of equity (*prcc_f* × *csho*)] / total assets (*at*)	Compustat
Unique industry (indicator)	One if a firm's industry is in the top quartile of all the two-digit SIC industries annually sorted by industry-median product uniqueness, and zero otherwise. Product uniqueness is defined as selling expense scaled by sales	Compustat

References

Admati, A.R., Demarzo, P.M. Hellwig, M.F., Pfleiderer, P., 2018. The leverage ratchet effect. Journal of Finance 73, 145-198.

Akey, P., Lewellen, S., Liskovich, I., 2018. Hacking Corporate Reputations. Unpublished working paper, University of Toronto.

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

Bakke, T.E., Mahmudi, H., Fernando, C.S., Salas, J. M., 2016. The causal effect of option pay on corporate risk management. *Journal of Financial Economics* 120, 623-643.

Daniele, B., Tosun, O., 2018. Cyberattacks and stock market activity. Unpublished working paper, University of Warwick.

Stephen, B., Hwang, L., Lilien, S., 2000. CEO stock-based compensation: An empirical analysis of incentive intensity, relative mix, and economic determinants. *Journal of Business* 73, 661-693.

Caliendo, M., Kopeinig, S., 2008. Some practical guidance for the implementation of propensity score matching. *Journal of Economic Surveys* 22, 31-72.

Campbell, K., Gordon, L.A., Loeb, M.P., 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.

Carhart, M. M., 1997. On persistence in mutual fund performance. *Journal of Finance* 52, 57-82.

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, 70-104.

Chan, L.H., Chen, K.C.W., Chen, T.Y., 2013. The effects of firm-initiated clawback provisions on bank loan contracting. *Journal of Financial Economics* 110, 659-679.

Chernobai, A., Jorion, P., Yu, F., 2011. The determinants of operational risk in U.S. financial institutions. *Journal of Financial and Quantitative Analysis* 46, 1683-1725.

Coles, J.L., Daniel, N.D., Naveen, L., 2006. Managerial incentives and risk-taking. *Journal of Financial Economics* 79, 431-468.

Crouhy, M., Galai, D., Mark, R., 2014. *The Essentials of Risk Management*. McGraw-Hill Education.

Cummins, J.D., Lewis, C.M., Wei, R., 2006. The market value impact of operational loss events for US banks and insurers. *Journal of Banking and Finance* 30, 2605-2634.

Fama, E.F., French, K.R. 1993. Common risk factors in the returns on stocks and bonds. *Journal of Financial Economics* 33, 3-56.

Froot, K.A., Scharfstein, D.S., Stein, J.C. 1993. Risk management: Coordinating corporate investment and financing policies. *Journal of Finance* 48, 1629-1658.

Garg, A., Curtis, J., Halper, H., 2003a. The financial impact of IT security breaches: what do investors think?. *Information Systems Security* 12, 22-33.

Garg, A., Curtis, J., Halper, H., 2003b. Quantifying the financial impact of IT security breaches. *Information Management and Computer Security* 11, 74-83.

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

Gennaioli, N., Shleifer, A., Vishny, R., 2015. Neglected risks: The psychology of financial crises. *American Economic Review* 105, 310-314.

Guay, W.R., 1999. The sensitivity of CEO wealth to equity risk: an analysis of the magnitude and determinants. *Journal of Financial Economics* 53, 43-71.

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

Hovav, A., D'Arcy, J., 2003. The impact of denial of service attack announcements on the market value of firms. *Risk Management and Insurance Review* 6, 97-121.

Hovav, A., D'Arcy, J., 2004. The impact of virus attack announcements on the market value of firms. *Information Systems Security* 13, 32-40.

Johnson, M., Kang, M.J., Tolani, L., 2017. Stock price reaction to data breaches. *Journal of Finance Issues* 16, 1-13.

Kahneman, D., Tversky, A., 1972. Subjective probability: A judgment of representativeness. *Cognitive psychology* 3, 430-454.

Kaplan, S.N., Zingales, L., 1997. Do investment-cash flow sensitivities provide useful measures of financing constraints?. *Quarterly Journal of Economics* 112, 169-215.

Karpoff, J.M., 2012. Does reputation work to discipline corporate misconduct?. In: Pollock T.G., Barnett M.L. (Eds.), *Oxford Handbook of Corporate Reputation*, Oxford University Press, pp.361-382.

Karpoff, J.M., Lee, D.S., Martin, G.S., 2008. The cost to firms of cooking the books. *Journal of Financial and Quantitative Analysis* 43, 581-611.

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, 13-22.

Lagakos, S. W., 1979. General right censoring and its impact on the analysis of survival data. *Biometrics* 35, 139-156.

Lam, J., 2014. *Enterprise Risk Management: From Incentives to Controls* (2nd edition). Wiley.

Larcker, D.F., Reiss, P.C., Tayan, B, 2017, Critical update needed: Cybersecruity expertise in the boardroom, Unpublished working paper, Stanford University.

Lending, C., Minnick, K., Schorno, P.J., 2018. Corporate governance, social responsibility and data breaches. *Financial Review* 53, 413-455.

Makridis, C., Dean, B., 2018. Measuring the economic effects of data breaches on firm outcomes: Challenges and opportunities. Unpublished working paper, MIT.

Myers, S.C., 1977. Determinants of corporate borrowing. *Journal of Financial Economics* 5, 147-175.

Nordlund, J., 2019. The role of experience in the director labor market: Evidence from cybersecurity events, Unpublished working paper, Louisiana State University.

Sunstein, C.R., Zeckhauser, R., 2011. Overreaction to fearsome risks. *Environmental and Resource Economics 48*, pp.435-449.

Stulz, R.M., 2003. *Risk Management and Derivatives*. Cengage Learning.

Tyler, S., 2001. Forecasting bankruptcy more accurately: A simple hazard model. *Journal of Business* 74, 101-124.

Tyler, S., Warther, V.A. 1999. The delisting bias in CRSP's Nasdaq data and its implications for the size effect. *Journal of Finance* 54, 2361-2379.

Smith, C.W., Stulz, R.M., 1985. The determinants of firms' hedging policies. *Journal of Financial and Quantitative Analysis* 20, 391-405.

Titman, S., 1984. The effect of capital structure on a firm's liquidation decision. *Journal of Financial Economics* 13, 137–151.

Titman, S., Wessels, R., 1988. The determinants of capital structure choice. *Journal of Finance* 43, 1-19.

Tversky, A., Kahneman, D., 1973. Availability: A heuristic for judging frequency and probability. *Cognitive Psychology* 5, 207–232.

Whited, T.M., Wu, G., 2006. Financial constraints risk. *Review of Financial Studies* 19, 531-559.

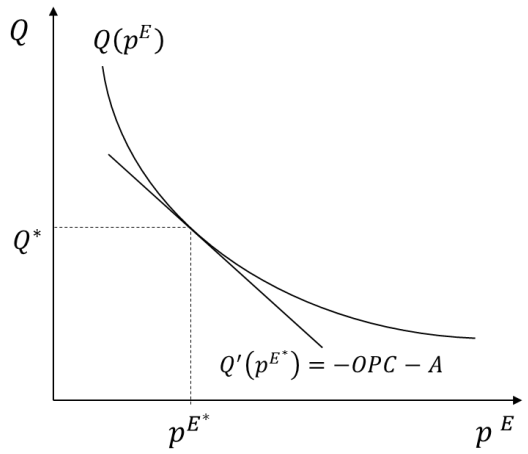

Figure 1. Optimal choice of investment in risk management and resulting probability of being hacked

In the Figure, $Q(p^E)$ is the cost of a risk management program that achieves a probability p^E of an end-of-period breach. *OPC* stands for the out-of-pocket costs of a breach. The costs of the terms on which stakeholders deal with the firm are given by A x p, so that these costs increase with the probability of a breach. The firm chooses an optimal probability of a breach, p^{E*}, by equating the marginal cost of risk management to the marginal expected cost of breach.

Table 1
Distribution of Cyberattacks by Year and Industry

The table presents the chronological distribution of 307 successful cyberattacks against 224 distinct firms covered in Compustat over the period 2005 to 2017 by calendar year and industry (SIC two-digit codes). The percentages of cyberattacks occurred in a given year for each industry are reported in parentheses. The percentage of cyberattacks occurred in the whole industry during the sample period are reported in brackets.

Calendar year	Agriculture, forestry, fisheries (01-09)	Mineral, construction (10-17)	Manufac-turing (20-39)	Transport, communi-cations (40-48)	Electric, gas, and sanitary services (49)	Wholesale trade and retail trade (50-59)	Finance (60-69)	Service industries (70-89)	Total
2005	0	0	2	0	0	1	1	0	4
	(0.00)	(0.00)	(3.70)	(0.00)	(0.00)	(2.04)	(1.39)	(0.00)	
2006	0	0	0	1	0	3	4	0	8
	(0.00)	(0.00)	(0.00)	(3.23)	(0.00)	(6.12)	(5.56)	(0.00)	
2007	0	0	1	1	0	1	10	4	17
	(0.00)	(0.00)	(1.85)	(3.23)	(0.00)	(2.04)	(13.89)	(4.17)	
2008	0	0	2	1	0	2	3	1	9
	(0.00)	(0.00)	(3.70)	(3.23)	(0.00)	(4.08)	(4.17)	(1.04)	
2009	0	0	0	1	0	1	7	3	12
	(0.00)	(0.00)	(0.00)	(3.23)	(0.00)	(2.04)	(9.72)	(3.13)	
2010	0	0	2	1	0	6	6	1	16
	(0.00)	(0.00)	(3.70)	(3.23)	(0.00)	(12.24)	(8.33)	(1.04)	
2011	0	0	5	3	0	2	3	3	16
	(0.00)	(0.00)	(9.26)	(9.68)	(0.00)	(4.08)	(4.17)	(3.13)	
2012	0	2	6	2	0	3	5	12	30
	(0.00)	(67.00)	(18.18)	(6.45)	(0.00)	(6.12)	(6.94)	(12.50)	
2013	0	0	7	2	0	3	9	23	44
	(0.00)	(0.00)	(12.96)	(6.45)	(0.00)	(6.12)	(12.50)	(23.96)	
2014	1	0	8	3	1	7	2	10	32
	(100.00)	(0.00)	(14.81)	(9.68)	(100.00)	(14.29)	(2.78)	(10.42)	
2015	0	0	6	5	0	6	2	9	28
	(0.00)	(0.00)	(11.11)	(16.13)	(0.00)	(12.24)	(2.78)	(9.38)	
2016	0	0	5	6	0	6	10	18	45
	(0.00)	(0.00)	(9.26)	(19.35)	(0.00)	(12.24)	(13.89)	(18.75)	
2017	0	1	10	5	0	8	10	12	46
	(0.00)	(33.00)	(18.52)	(16.13)	(0.00)	(16.33)	(13.89)	(12.50)	
Total	1	3	54	31	1	49	72	96	307
	(100.00)	(100.00)	(100.00)	(100.00)	(100.00)	(100.00)	(100.00)	(100.00)	
	[0.33]	[0.98]	[17.59]	[10.10]	[0.33]	[15.96]	[23.45]	[31.27]	[100.00]

Table 2
Summary Statistics

The table shows summary statistics for a sample of 259 firm-year observations that experience a cyberattack in the following fiscal year (206 distinct firms) and the remaining 54,717 firm-year observations (7,835 distinct firms) that do not experience a cyberattack covered in Compustat over the period 2005 to 2017. The appendix provides detailed descriptions of the construction of the variables. ***, **, and * denote that *t*-tests (Wilcoxon *z*-tests) for mean (median) differences in firm and industry characteristics between attacked and non-attacked firms are significance at the 1%, 5%, and 10% levels, respectively.

	Firm-years followed by cyberattack (N = 259): A		Firm-years without cyberattack (N = 54,717): B		Test of difference (A - B)	
Variable	Mean	Median	Mean	Median	Mean	Median
Total assets ($ billion)	43.177	10.314	8.162	0.777	35.015***	9.537***
Firm age	27.471	21.000	20.751	15.000	6.720***	6.000***
Tobin's *q*	2.112	1.607	1.852	1.374	0.260***	0.233***
ROA	0.058	0.050	-0.017	0.023	0.075***	0.027***
Stock performance	0.003	-0.024	0.008	-0.039	-0.005	0.015
Sales growth	1.083	1.056	1.146	1.070	-0.063**	-0.014
Leverage	0.242	0.210	0.213	0.163	0.029**	0.047***
Stock return volatility	0.086	0.072	0.120	0.101	-0.034***	-0.029***
Financial constraint (indicator)	0.046	0.000	0.318	0.000	-0.272***	0.000***
R&D / assets	0.019	0.000	0.042	0.000	-0.023***	0.000***
CAPX / assets	0.035	0.025	0.044	0.024	-0.009**	0.001
Asset intangibility	0.831	0.890	0.772	0.876	0.059***	0.014**
Institutional block ownership (%)	10.656	5.300	12.672	6.980	-2.016**	-1.680**
Fortune 500 membership (indicator)	0.521	1.000	0.108	0.000	0.413***	1.000***
Risk committee (indicator)	0.082	0.000	0.054	0.000	0.028*	0.000*
Number of board committees	4.064	4.000	3.577	3.000	0.487***	1.000***
Industry Herfindahl index	0.074	0.040	0.059	0.037	0.015***	0.003***
Unique industry (indicator)	0.958	1.000	0.881	1.000	0.077***	0.000***
Industry Tobin's *q*	1.542	1.492	1.544	1.462	-0.002	0.030

Table 3
Likelihood of Becoming Cyberattack Targets

The table presents estimates of probit regressions in which the dependent variable is an indicator that takes the value one if a firm experiences a cyberattack in a given year, and zero otherwise. The sample consists of 54,003 firm-year observations covered in Compustat over the period 2005 to 2017. All explanatory variables are measured one year before the attack except for Tobin's *q* that is measured two years before the attack. The appendix provides detailed descriptions of the construction of the variables. *P*-values reported in parentheses are based on standard errors adjusted for heteroskedasticity and clustering at the firm level. ***, **, and * denote significance at the 1%, 5%, and 10% levels, respectively.

	Dependent variable = Cyberattack (indicator)			
	(1)	(2)	(3)	(4)
Firm size	0.203***	0.241***	0.165***	0.190***
	(0.000)	(0.000)	(0.000)	(0.000)
Log (firm age)	-0.039	-0.121**	-0.105**	-0.054
	(0.380)	(0.013)	(0.011)	(0.248)
Tobin's q_{t-1}	0.063***	0.043*	0.081***	0.070***
	(0.007)	(0.060)	(0.000)	(0.002)
ROA	0.843*	0.531	0.855*	0.900*
	(0.098)	(0.224)	(0.078)	(0.094)
Sales growth	-0.201*	-0.172	-0.195**	-0.198*
	(0.055)	(0.106)	(0.029)	(0.058)
Stock performance	-0.092	-0.099	-0.089	-0.100
	(0.316)	(0.313)	(0.308)	(0.280)
Leverage	-0.292	-0.397**	-0.089	-0.144
	(0.118)	(0.035)	(0.553)	(0.342)
Financially constraint (indicator)	-0.186*	-0.218*	-0.363***	-0.249**
	(0.086)	(0.059)	(0.003)	(0.027)
Stock return volatility	-0.148	0.146	-0.114	-0.050
	(0.810)	(0.819)	(0.844)	(0.935)
Institutional block ownership	0.004*	0.003	0.005**	0.004*
	(0.053)	(0.220)	(0.015)	(0.069)
R&D / assets	-0.058	-0.029	-0.562	-0.074
	(0.953)	(0.977)	(0.505)	(0.932)
CAPX / assets	0.678	1.482	1.061	0.604
	(0.495)	(0.120)	(0.203)	(0.506)
Asset intangibility	0.732***	0.710***	0.686***	0.622***
	(0.001)	(0.003)	(0.000)	(0.003)
Fortune 500 (indicator)	0.337***	0.245***	0.396***	0.344***
	(0.000)	(0.001)	(0.000)	(0.000)
Risk committee (indicator)		-0.412***		
		(0.002)		
Number of board committees		0.039		
		(0.131)		
Industry Herfindahl Index			0.879***	
			(0.000)	
Unique industry (indicator)			0.274**	
			(0.019)	
Industry Tobin's *q*			0.155**	
			(0.044)	
Wholesale trade and retail trade				0.490***
				(0.000)
Finance				-0.003
				(0.980)
Service industries				0.544***
				(0.000)
Transportation and communications				0.383***
				(0.002)
Year fixed effects	Y	Y	Y	Y
Industry fixed effects	Y	Y	N	N
Observations	45,906	40,442	54,003	48,369
Pseudo R^2	0.230	0.247	0.189	0.205

Table 4
Cumulative Abnormal Returns (CARs) for Attacked Firms around Cyberattack Announcement Dates

This table presents the mean and median cumulative abnormal returns (CARs) for firms around cyberattack announcement dates (Panel A), the comparison of mean and median CARs between firms experiencing cyberattacks that result in financial information loss and those firms experiencing cyberattacks that result in no financial information loss (Panel B), and estimates of ordinary least squares (OLS) regressions in which the dependent variable is the CAR from one day before to one day after the cyberattack announcement date (Panel C). The sample consists of 165 announcements (125 distinct firms) of cyberattacks over the period 2005 to 2017. The abnormal stock returns are calculated using the market model, Fama-French (1993) three-factor model, and the Fama-French-Carhart (Carhart, 1997) four-factor model, respectively. The market model parameters are estimated using 220 trading days of return data beginning 280 days before and ending 61 days before the breach announcements, using the CRSP value-weighted (equally weighted) return as a proxy for the market return. The daily abnormal stock returns are cumulated to obtain the CAR from day t_1 before the attack announcement date to day t_2 after the attack announcement date. The three factors used in Fama-French (1993) three-factor model are CRSP value-weighted index, SMB (daily return difference between the returns on small and large size portfolios), and HML (daily return difference between the returns on high and low book-to-market-ratio portfolios). The four factors used in the Fama-French-Carhart (Carhart, 1997) four-factor model are CRSP value-weighted index, SMB, HML, and UMD (daily return difference between the returns on high and low prior return portfolios). In Regressions (1)-(6) of Panel C, we include industry fixed effects using two-digit standard industry classification (SIC) codes. In Regressions (7) and (8) of Panel C, we replace two-digit SIC codes by Fama-French five industry codes. The appendix provides detailed descriptions of the construction of the variables. In Panels A and B, the numbers in parentheses are *p*-values for *t*-tests and *z*-values for Wilcoxon signed-rank tests that the mean CAR and the median CAR are equal to zero, respectively. In Panel B, the numbers in brackets in the last two columns are *p*-values of the *t*-test for equality of mean CARs and *z*-values of the Wilcoxon *z*-test for equality of median CARs, respectively. In Panel C, *p*-values reported in parentheses are based on standard errors adjusted for heteroskedasticity and clustering at the firm level. ***, **, and * denote significance at the 1%, 5%, and 10% levels, respectively.

Panel A. Univariate analysis

	Market model				Three and four factor models			
	Value-weighted		Equally weighted		Fama-French three-factor model		Fama-French-Carhart four-factor model	
CARs (%)	Mean	Median	Mean	Median	Mean	Median	Mean	Median
CAR (-1, 1)	-0.844***	-0.521***	-0.794***	-0.571***	-0.768***	-0.521***	-0.750**	-0.441***
	(0.003)	(-3.658)	(0.006)	(-3.279)	(0.008)	(-3.190)	(0.010)	(-3.123)
CAR (-2, 2)	-1.101***	-0.810***	-1.001***	-0.768***	-1.035***	-0.546***	-1.055***	-0.511***
	(0.000)	(-3.660)	(0.002)	(-2.956)	(0.002)	(-3.138)	(0.001)	(-3.100)
CAR (-5, 5)	-1.099**	-1.355***	-1.240**	-1.330***	-1.066**	-1.198**	-1.115**	-0.990***
	(0.034)	(-2.594)	(0.022)	(-2.646)	(0.034)	(-2.524)	(0.027)	(-2.674)

Panel B. Comparison of CARs between cyberattacks with and without financial information loss

	Financial information loss (N=118): a		No financial information loss (N=47): b		Test of difference (a – b):	
CARs (%)	Mean	Median	Mean	Median	*t*-test	Wilcoxon *z*-test
CAR (-1, 1)	-1.087***	-0.529***	-0.234	-0.311	-0.853	-0.218
	(0.003)	(-3.871)	(0.526)	(-0.646)	[0.170]	[1.383]
CAR (-2, 2)	-1.458***	-1.136***	-0.204	-0.296	-1.254*	-0.840**
	(0.000)	(-3.987)	(0.615)	(-0.381)	[0.069]	[2.072]
CAR (-5, 5)	-1.585**	-1.484***	0.119	-0.808	-1.704	-0.676
	(0.020)	(-2.861)	(0.840)	(-0.138)	[0.134]	[1.589]

Panel C: OLS regressions of CARs (-1, 1)

	CAR (-1, +1)							
Independent variable	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
Financial information loss (indicator)	-0.018**	-0.018**	-0.014**	-0.012*	-0.017*	-0.017*	-0.047**	-0.027
	(0.018)	(0.038)	(0.035)	(0.077)	(0.063)	(0.055)	(0.045)	(0.161)
Repeated cyberattacks within one year (indicator)		-0.025*	-0.018	-0.018	-0.024	-0.025	-0.021	-0.037*
		(0.071)	(0.113)	(0.131)	(0.161)	(0.143)	(0.398)	(0.088)
Board attention to risk management (indicator)					0.040*			
					(0.083)			
State law (indicator)						-0.016		
						(0.302)		
Delay of discovery							-0.007*	
							(0.088)	
Delay of reporting								0.001

								(0.855)
Industry Herfindahl Index			0.030					
			(0.363)					
Unique industry (indicator)			0.003					
			(0.832)					
Industry Tobin's *q*			-0.015**					
			(0.041)					
Transportation / communications industry (indicator)				-0.002				
				(0.821)				
Wholesale / retail trade industry (indicator)				0.011				
				(0.225)				
Finance industry (indicator)				-0.001				
				(0.905)				
Service industry (indicator)				-0.005				
				(0.619)				
Firm size		0.002	0.002	0.002	0.001	0.002	0.008	0.008*
		(0.570)	(0.477)	(0.311)	(0.840)	(0.623)	(0.228)	(0.053)
Log (firm age)		-0.013*	-0.012**	-0.014**	-0.014*	-0.013	-0.036***	-0.031***
		(0.052)	(0.023)	(0.013)	(0.067)	(0.101)	(0.005)	(0.005)
ROA		0.003	0.036	0.041	0.028	0.018	0.068	0.072
		(0.965)	(0.439)	(0.409)	(0.689)	(0.813)	(0.286)	(0.305)
Leverage		-0.027*	-0.015	-0.014	-0.034**	-0.030**	-0.055	-0.026
		(0.053)	(0.118)	(0.161)	(0.024)	(0.045)	(0.162)	(0.309)
Financial constraint (indicator)		-0.000	-0.001	-0.003	-0.000	0.001	-0.008	-0.009
		(0.966)	(0.898)	(0.749)	(0.984)	(0.912)	(0.736)	(0.646)
Sales growth		-0.025	-0.012	-0.017	-0.026	-0.021	-0.068	-0.048
		(0.260)	(0.448)	(0.350)	(0.330)	(0.425)	(0.234)	(0.247)
Tobin's *q*		0.000	0.000	-0.001	-0.001	-0.000	0.005	-0.001
		(0.941)	(0.970)	(0.527)	(0.803)	(0.878)	(0.369)	(0.839)
Institutional block ownership		-0.000	-0.000	-0.000	-0.000	-0.000	-0.000	0.000
		(0.328)	(0.298)	(0.566)	(0.856)	(0.630)	(0.675)	(0.848)
Year fixed effects	Y	Y	Y	Y	Y	Y	Y	Y
Industry fixed effects	Y	Y	N	N	Y	Y	Y	Y
Observations	165	165	165	162	149	151	40	67
Adj. R^2	-0.095	-0.039	0.053	0.028	-0.027	-0.057	0.257	0.232

Table 5
Total Dollar Market Value Losses, Out-of-Pocket Costs, and Excess Losses

Panel A presents cyberattack-related out-of-pocket costs for 21 cyberattacks that have a negative CAR (-1, 1) when disclosed or with subsequent post-attack event announcement dates and also have information about cyberattack-related costs available. *Investigation and remediation costs* include expenses to hire experts to investigate the incidents and to upgrade the IT system. *Other costs* include money stolen from bank accounts, costs that combine several items including remediation costs and costs that are difficult to disentangle. *Legal penalties* include settlement costs for class-action lawsuits or other litigations, and other legal costs (e.g., attorney's fees). *Regulatory penalties* include fines and penalties levied by regulators. Panel B presents the cumulative abnormal returns (CARs) from one day before to one day after the cyberattack announcement date for 91 first-time cyberattacks within three years and those from one day before to one day after the post-attack event announcement date for 56 firms over the period 2005 to 2014. Post-attack events are grouped by announcement type. We obtain information about post-attack events from various sources including Lexis-Nexis, West Law, an online legal research service, Factiva, 10-K filings, proxy statements, and annual reports of the attacked firm. Panel C presents total dollar market value losses associated first-time cyberattacks within three years that are followed by at least one post-attack event. The first row includes a subsample of 21 cyberattacks that have a negative CAR (-1, 1) when disclosed or with subsequent post-attack event announcements and also have information about cyberattack-related costs available. The second row includes a subsample of 20 cyberattacks that have a negative CAR (-1, 1) when disclosed or with subsequent post-attack event announcements and result in class-action lawsuits and other litigations in the post-attack period. The third row includes 75 cyberattacks having a negative CAR (-1, 1) when disclosed or with subsequent post-attack event announcements. For each event, we compute a firm's total dollar market value loss by multiplying its CAR (-1, 1) around each event including the cyberattack announcement by its market value of equity 10 days before the event announcement date. We then sum up the dollar loss of all events to compute total dollar market value losses. Panel D combines the total dollar market value loss reported in Panel C and a breakdown of cyberattack-related out-of-pocket costs reported in Panel A to compute excess losses. The first column includes a subsample of 21 cyberattacks that have a negative CAR (-1, 1) when disclosed or with subsequent post-attack event announcements and also have information about cyberattack-related costs available. The second column includes 75 cyberattacks having a negative CAR (-1, 1) when disclosed or with subsequent post-attack event announcements. If total cyberattack out-of-pocket costs exceed total dollar market value loss, the excess loss is set to zero. For cyberattacks in which we are able to obtain the information about costs associated with post-attack events, the excess loss is computed by subtracting total out-of-pocket costs from the total dollar market value loss. For cyberattacks in which we are unable to obtain the information about cyberattack out-of-pocket costs, we set these costs as zero and use the total dollar market loss as the excess loss. The market model parameters are estimated using 220 trading days of return data beginning 280 days before and ending 61 days before the event announcements, using the CRSP value-weighted return as a proxy for the market portfolio return. ***, **, and * denote significance at the 1%, 5%, and 10% levels, respectively, for *t*-tests and Wilcoxon signed-rank tests that the mean and median values are equal to zero.

Panel A. Cyberattack-related out-of-pocket costs: Using firms with information on out-of-pocket costs available

Cost	No. of Cyberattacks	Total costs ($ millions)	Mean	Median
1. Investigation and remediation costs: a	6	535.50	89.25	37.00
Other costs: b	2	38.60	19.30	19.30
2. Legal penalties (legal settlements and other legal costs): c	10	613.31	61.33	17.68
3. Regulatory penalties (fines and penalties from regulators): d	2	2.04	1.02	1.02
4. Total out-of-pocket cost for firms in which its information is available but its breakdown is unavailable: e	14	1,247.01	89.07	17.00
5. Total out-of-pocket costs [Max (sum of (a, b, c, and d), e)]	21	1,722.16	82.01	16.00

Panel B. CARs (-1, 1) around public disclosures of first-time cyberattacks within three years and those around cyberattack-related events in the post-attack period

Event type	Number of events for each category	Number of events with a negative CAR (-1, 1) (%)	Mean CAR (-1, 1)	Median CAR (-1, 1)
1. Public disclosures of first-time cyberattacks within three years	91	58 (63.74%)	-0.717*	-0.695***
Post-attack events:				
2. Investigation by regulatory bodies	8	4 (50.00%)	0.071	-0.019
3. Repeated attacks within three years	18	10 (55.56%)	-0.944	-0.252
4. Filings of class-action suits and other legal litigations	18	12 (66.67%)	-3.503	-1.064*
5. Litigation settlements	12	8 (66.67%)	-0.277	-0.275

Panel C. Aggregate CARs (-1, 1) and total dollar market value losses associated with public disclosures of first-time cyberattacks within three years and post-attack events

CARs and dollar loss	Mean	Median	Aggregate losses: $ million
1. A subsample of 21 cyberattacks that have a negative CAR (-1, 1) when disclosed or with subsequent post-attack event announcements and also have information on cyberattack-related out-of-pocket cost available			
Aggregate CAR (-1, 1): %	-6.828**	-3.436***	
Dollar loss: $ million	1,150.44	259.08	24,990.56
2. A subsample of 20 cyberattacks that have a negative CAR (-1, 1) when disclosed or with subsequent post-attack event announcements and result in class-action lawsuits and other litigations			
Aggregate CAR (-1, 1): %	-8.036***	-4.132***	
Dollar loss: $ million	1,249.53	451.38	24,159.21
3. Full sample of 75 cyberattacks that have a negative CAR (-1, 1) when disclosed or with subsequent post-attack event announcements			
Aggregate CAR (-1, 1): %	-3.607***	-1.702***	
Dollar loss: $ million	1,393.89	259.08	104,069.59

Panel D. Excess loss

Dollar loss: $ millions	A subsample of 21 cyberattacks that have a negative CAR (-1, 1) when disclosed or with subsequent post-attack event announcements and also have information about out-of-pocket available	A full sample of 75 cyberattacks that have a negative CAR (-1, 1) when disclosed or with subsequent post-attack event announcements
Aggregate dollar market value loss (mean loss, median loss)	$24,159.21 ($1,150.44, $259.08)	$104,069.59 ($1,393.89, $259.08)
Out-of-pocket cost and reputation loss (% of aggregate dollar market value loss, mean loss, median loss)		
1. Investigation and remediation costs	$535.50 (2.22%, $25.50, $0.00)	$535.50 (0.51%, $7.14, $0.00)
2. Other costs	$38.60 (0.16%, $1.84, $0.00)	$38.60 (0.04%, $0.52, $0.00)
3. Legal penalties	$613.31 (2.54%, $29.21, $0.00)	$613.31 (0.59%, $8.18, $0.00)
4. Regulatory penalties	$2.04 (0.01%, $0.10, $0.00)	$2.04 (0.00%, $0.03, $0.00)
Excess loss	$22,584.31 (93.48%, $1,075.44, $237.46)	$102,966.20 (98.94%, $1,372.88, $237.46)

Table 6
Effects of Cyberattacks on Firms' Operating Performance

This table presents descriptive statistics for treated firms that experience a cyberattack involving financial information loss over the period 2005 to 2015 and control firms that do not experience a cyberattack over the same period (Panel A) and estimates of ordinary least squares (OLS) regressions in which the dependent variables are firm performance (Panels B-E). The propensity score is calculated using the logit regression of *Cyberattack* (an indicator that takes the value one if a firm experiences a cyberattack involving financial information loss, and zero otherwise) on firm size, stock performance, stock return volatility, leverage, and institutional blockholder (indicator). We require both treated and matching firms to be in the same industry (the same two-digit standard industrial classification (SIC) codes) and in the same fiscal year. The sample consists of 1,291 firm-year observations (113 treated firms that experience a cyberattack involving financial information loss and 113 control firms that do not experience a cyberattack). *Post* is an indicator that takes the value one for post-attack period (year *t*, year *t*+1, and year *t*+2), and zero for pre-attack period (year *t*-1 and year *t*-2, and year *t*-3), where year *t* is the fiscal year in which a cyberattack occurs. The appendix provides detailed descriptions of the construction of the variables. *P*-values reported in parentheses are based on standard errors adjusted for heteroskedasticity and clustered at the firm level. ***, **, and * denote significance at the 1%, 5%, and 10% levels, respectively.

Panel A. Descriptive statistics for propensity-score matched sample firms

	Treatment firms with a cyberattack (N=113): a		Control firms without a cyberattack (N=113): b		Test of difference (a –b): *p*-value	
Variable	Mean	Median	Mean	Median	*t*-test	Wilcoxon *z*-test
Firm size	9.340	9.371	9.304	9.136	0.90	0.98
Stock performance	−0.042	−0.035	−0.002	−0.016	0.29	0.45
Stock return volatility	0.088	0.074	0.087	0.073	0.94	0.67
Leverage	0.216	0.163	0.221	0.179	0.85	0.76
Institutional blockholder (indicator)	0.537	0.670	0.574	0.698	0.42	0.49

Panel B. Effects of cyberattacks on firm performance

	Sales growth		ROA		ROE		Cash flow / assets	
Independent variable	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
Post (indicator) × Cyberattack (indicator)	-0.032*		-0.006		-0.021		-0.003	
	(0.067)		(0.180)		(0.188)		(0.512)	
Year $_t$		-0.021		-0.005		-0.019		-0.003
		(0.223)		(0.326)		(0.378)		(0.527)
Year $_{t+1}$		-0.014		-0.003		-0.016		0.001
		(0.640)		(0.631)		(0.500)		(0.860)
Year $_{t+2}$		-0.015		-0.003		-0.013		0.003
		(0.645)		(0.687)		(0.640)		(0.738)
Firm size		-0.065		-0.020**		-0.036		-0.027**
		(0.201)		(0.048)		(0.399)		(0.029)
Leverage		0.076		0.021		0.096		0.048
		(0.484)		(0.544)		(0.242)		(0.150)
Tobin's *q*		0.064***		0.021***		0.012*		0.023***
		(0.000)		(0.000)		(0.083)		(0.000)
Stock return volatility		0.135		-0.030		0.015		-0.017
		(0.467)		(0.396)		(0.906)		(0.652)
Institutional block ownership		0.048		-0.008		-0.026		0.005
		(0.755)		(0.688)		(0.822)		(0.820)
Firm fixed effects	Y	Y	Y	Y	Y	Y	Y	Y
Industry-year cohort fixed effects	Y	Y	Y	Y	Y	Y	Y	Y
Observations	1,290	1,262	1,291	1,263	1,290	1,263	1,247	1,220
Adj. R^2	0.057	0.062	0.609	0.637	0.302	0.295	0.691	0.719

Panel C. Effects of cyberattacks on firm performance: subsample analyses according to firm size (total assets)

	Large firm	Small firm	Large firm	Small firm	Large firm	Small firm	Large firm	Small firm
	Sales growth		ROA		ROE		Cash flow / assets	
Independent variable	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
Post (indicator) × Cyberattack (indicator)	-0.034*	-0.034	-0.009*	-0.006	-0.028	-0.025	-0.007*	-0.001
	(0.100)	(0.235)	(0.051)	(0.486)	(0.174)	(0.289)	(0.070)	(0.901)
Control variables	N	N	N	N	N	N	N	N
Firm fixed effects	Y	Y	Y	Y	Y	Y	Y	Y
Industry-year cohort fixed effects	Y	Y	Y	Y	Y	Y	Y	Y
Observations	643	647	644	647	644	646	615	632
Adj. R^2	0.069	0.074	0.734	0.534	0.408	0.151	0.810	0.608

Panel D. Effects of cyberattacks on firm performance: subsample analyses according to durable goods manufacturing industries and other industries

	Durable goods industries	Other industries	Durable goods industries	Other industries	Durable goods industries	Other industries	Durable goods industries	Other industries
	Sales growth		ROA		ROE		Cash flow / assets	
Independent variable	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
Post (indicator) × Cyberattack (indicator)	-0.040	-0.031	-0.040**	-0.002	-0.137	-0.006	-0.035**	0.001
	(0.311)	(0.105)	(0.029)	(0.683)	(0.100)	(0.686)	(0.050)	(0.844)
Control variables	N	N	N	N	N	N	N	N
Firm fixed effects	Y	Y	Y	Y	Y	Y	Y	Y
Industry-year cohort fixed effects	Y	Y	Y	Y	Y	Y	Y	Y
Observations	144	1,146	144	1,147	144	1,146	144	1,103
Adj. R^2	0.079	0.055	0.641	0.609	0.250	0.324	0.666	0.697

Panel E. Effects of cyberattacks on firm performance: subsample analyses according to retail industries and other industries

	Retail industries	Other industries	Retail industries	Other industries	Retail industries	Other industries	Retail industries	Other industries
	Sales growth		ROA		ROE		Cash flow / assets	
Independent variable	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
Post (indicator) × Cyberattack (indicator)	-0.054**	-0.027	-0.011	-0.005	-0.002	-0.025	-0.004	-0.003
	(0.046)	(0.173)	(0.359)	(0.293)	(0.951)	(0.161)	(0.647)	(0.591)
Control variables	N	N	N	N	N	N	N	N
Firm fixed effects	Y	Y	Y	Y	Y	Y	Y	Y
Industry-year cohort fixed effects	Y	Y	Y	Y	Y	Y	Y	Y
Observations	193	1,097	193	1,098	193	1,097	193	1,054
Adj. R^2	0.131	0.047	0.707	0.581	0.380	0.285	0.708	0.678

Table 7
Effects of Cyberattacks on Firms' Financial Health

The table presents estimates of ordinary least squares (OLS) regressions in which the dependent variables are the measures of a firm's financial health. The sample consists of 1,291 firm-year observations (113 treated firms that experience a cyberattack involving financial information loss over the period 2005 to 2015 and 113 control firms that do not experience a cyberattack over the same period). The propensity score is calculated using the logit regression of *Cyberattack* (an indicator that takes the value one if a firm experiences a cyberattack involving financial information loss, and zero otherwise) on firm size, stock performance, stock return volatility, leverage, and institutional blockholder (indicator). We require both treated and matching firms to be in the same industry (the same two-digit standard industrial classification (SIC) codes) and in the same fiscal year. *Post* is an indicator that takes the value one for post-attack period (year *t*, year *t*+1, and year *t*+2), and zero for pre-attack period (year *t*-1 and year *t*-2, and year *t*-3), where year *t* is the fiscal year in which a cyberattack occurs. The appendix provides detailed descriptions of the construction of the variables. *P*-values reported in parentheses are based on standard errors adjusted for heteroskedasticity and clustering at the firm level. ***, **, and * denote significance at the 1%, 5%, and 10% levels, respectively.

	S&P credit rating		Bankruptcy score		Net worth	
Independent variable	(1)	(2)	(3)	(4)	(5)	(6)
Post (indicator) × Cyberattack (indicator)	-0.325*		0.010*		-0.038***	
	(0.085)		(0.082)		(0.000)	
Year $_t$		-0.314***		0.003		-0.022***
		(0.010)		(0.694)		(0.006)
Year $_{t+1}$		-0.519***		0.016*		-0.031***
		(0.009)		(0.063)		(0.005)
Year $_{t+2}$		-0.751***		0.006		-0.038***
		(0.007)		(0.331)		(0.006)
Control variables (ROA and those used in Panel B of Table 6)	N	Y	N	Y	N	Y
Firm fixed effects	Y	Y	Y	Y	Y	Y
Industry-year cohort fixed effects	Y	Y	Y	Y	Y	Y
Observations	788	776	1,287	1,260	1,291	1,263
Adj. R^2	0.922	0.941	0.587	0.613	0.926	0.937

Table 8
Effects of Cyberattacks on Firms' Risk Management Policy

The table presents estimates of ordinary least squares (OLS) regressions in which the dependent variables are indicators for board attention to risk, which are measured using the information obtained from its 10-K and Def14A SEC filings. The sample consists of 1,126 firm-year observations (113 treated firms that experience a cyberattack involving financial information loss over the period 2005 to 2015 and 113 control firms that do not experience a cyberattack over the same period). The propensity score is calculated using the logit regression of *Cyberattack* (an indicator that takes the value one if a firm experiences a cyberattack involving financial information loss, and zero otherwise) on firm size, stock performance, stock return volatility, leverage, and institutional blockholder (indicator). We require both treated and matching firms to be in the same industry (the same two-digit standard industrial classification (SIC) codes) and in the same fiscal year. In columns (1) and (2), *Board attention to risk management* is an indicator that takes the value one if a firm's specific board committee (e.g., Enterprise-Wide Risk Management Committee, Risk Committee, Audit and Risk committee, and Audit Committee that is responsible for risk oversight) or a board as a whole oversees firm-wide risk management, and zero otherwise. In columns (3) and (4), *Risk oversight with committee* is an indicator that takes the value one if a board committee's explicit duty involves firm-wide risk and risk management oversight, and zero otherwise. In columns (5) and (6), *Risk oversight without committee* is an indicator that takes the value one if a firm does not have any specific board risk committee but the board as a whole oversees firm-wide risk and risk management, and zero otherwise. In columns (7) and (8), *Existence of committee with risk name* is an indicator that takes the value one if the name of a firm's board committee includes "risk" and its explicit duty involves firm-wide risk and risk management oversight, and zero otherwise. *Post* takes the value one for post-attack period (year *t*, year *t*+1, and year *t*+2), and zero for pre-attack period (year *t*-1 and year *t*-2, and year *t*-3), where year *t* is the fiscal year in which a cyberattack occurs. The appendix provides detailed descriptions of the construction of the variables. *P*-values reported in parentheses are based on standard errors adjusted for heteroskedasticity and clustered at the firm level. ***, **, and * denote significance at the 1%, 5%, and 10% levels, respectively.

	Board attention to risk management (indicator)		Risk oversight with committee (indicator)		Risk oversight without committee (indicator)		Existence of committee with risk name (indicator)	
Independent variable	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
Post (indicator) × Cyber-attack (indicator)	0.190*** (0.000)		0.166*** (0.000)		0.023 (0.415)		0.136*** (0.000)	
Year $_t$		0.163*** (0.000)		0.139*** (0.000)		0.028 (0.362)		0.094*** (0.002)
Year $_{t+1}$		0.172*** (0.000)		0.159*** (0.000)		0.019 (0.551)		0.131*** (0.000)
Year $_{t+2}$		0.292*** (0.000)		0.258*** (0.000)		0.040 (0.280)		0.179*** (0.000)
Control variables (ROA and those used in Panel B of Table 6)	N	Y	N	Y	N	Y	N	Y
Firm fixed effects	Y	Y	Y	Y	Y	Y	Y	Y
Year-cohort fixed effects	Y	Y	Y	Y	Y	Y	Y	Y
Observations	1,126	1,102	1,126	1,102	1,126	1,102	1,126	1,102
Adj. R^2	0.687	0.728	0.812	0.826	0.857	0.864	0.761	0.763

Table 9
Effects of Cyberattacks on CEO Pay Components

This table presents estimates of OLS regressions in which the dependent variables are log (1 + CEO total pay) in columns (1) and (2), the ratio of salary to CEO total pay in columns (3) and (4), the ratio of bonus to CEO total pay in columns (5) and (6), the ratio of equity-based compensation (restricted stock grants plus option awards) to CEO total pay in columns (7) and (8), the ratio of restricted stock grants to CEO total pay in columns (9) and (10), and the ratio of option awards to CEO total pay in columns (11) and (12). The sample consists of 1,005 CEO-firm-year observations with CEO compensation data available in *ExecuComp* from 2005 to 2015 (88 firm-year observations that experience a cyberattack involving financial information loss over the period 2005 to 2015 and 88 control firm-year observations that do not experience a cyberattack over the same period). The propensity score is calculated using the logit regression of *Cyberattack* (an indicator that takes the value one if a firm experiences a cyberattack involving financial information loss, and zero otherwise) on firm size, stock performance, return volatility, leverage, and institutional blockholder (indicator). We require both treated and matching firms to be in the same industry (the same two-digit standard industrial classification (SIC) codes) and in the same fiscal year. *Post* is an indicator that takes the value one for post-attack years (year *t*, year *t*+1, and year *t*+2), and zero for pre-attack years (year *t*-1 and year *t*-2, and year *t*-3), where year *t* is the fiscal year in which a cyberattack occurs. The appendix provides detailed descriptions of the construction of the variables. *P*-values reported in parentheses are based on standard errors adjusted for heteroskedasticity and clustered at the firm level. ***, **, and * denote significance at the 1%, 5%, and 10% levels, respectively.

	Log (1 + CEO total pay)		Salary / CEO total pay		Bonus / CEO total pay		Equity-based compensation / CEO total pay		Restricted stock grants / CEO total pay		Option awards / CEO total pay	
Independent variable	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)
Post (indicator) × Cyberattack (indicator)	-0.063		-0.008		-0.050***		0.037		0.104***		-0.066***	
	(0.550)		(0.611)		(0.000)		(0.132)		(0.000)		(0.001)	
Year $_t$		-0.099		-0.007		-0.043***		0.042		0.084***		-0.043**
		(0.462)		(0.764)		(0.008)		(0.168)		(0.004)		(0.031)
Year $_{t+1}$		-0.056		-0.012		-0.048***		0.032		0.103***		-0.072***
		(0.731)		(0.590)		(0.005)		(0.262)		(0.001)		(0.001)
Year $_{t+2}$		-0.114		-0.009		-0.046***		0.016		0.112***		-0.094***
		(0.325)		(0.651)		(0.002)		(0.567)		(0.001)		(0.000)
Stock performance		0.318**		-0.033		0.012		0.030		0.048*		-0.019
		(0.013)		(0.141)		(0.545)		(0.313)		(0.079)		(0.325)
CEO-chair duality (indicator)		0.120		-0.012		-0.004		-0.000		0.033		-0.036
		(0.378)		(0.655)		(0.866)		(0.990)		(0.342)		(0.170)
CEO age		0.000		-0.000		0.002		0.001		0.003		-0.003
		(0.975)		(0.986)		(0.335)		(0.865)		(0.324)		(0.319)
Log (CEO tenure)		-0.081		0.020		0.006		-0.060***		-0.047**		-0.012
		(0.393)		(0.223)		(0.630)		(0.008)		(0.030)		(0.387)
Control variables (ROA and those used in Panel B of Table 6)		Y		Y		Y		Y		Y		Y
Firm fixed effects	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Industry-year cohort fixed effects	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Observations	1,005	985	1,005	985	1,005	985	1,005	985	1,005	985	1,005	985
Adj. R^2	0.567	0.594	0.565	0.587	0.409	0.432	0.459	0.492	0.519	0.547	0.594	0.616

Table 10
Determinants of the Excess Loss

The table presents estimates of tobit regressions in which the dependent variable is the ratio of the firm's total loss in excess of its out-of-pocket costs (excess loss) to the total dollar market value loss. The excess loss is computed by subtracting total cyberattack-related out-of-pocket costs from the total dollar market value loss from cyberattacks in which we are able to obtain information about out-of-pocket costs associated with post-attack events. For cyberattacks in which we are unable to obtain information about out-of-pocket costs in the post-attack period, we set these costs as zero and use the total dollar market loss as the excess loss. If total out-of-pocket costs exceed total dollar market value loss, the excess loss is set to zero. Total dollar market value loss is the summation of the dollar loss of all events. For each event, we compute a firm's total dollar market value loss by multiplying its CAR (-1, 1) around each event by its market value of equity 10 days before the event announcement date. The sample includes 75 cyberattacks that have a negative CAR (-1, 1) when disclosed or with subsequent post-attack event announcements. *Big firm* is an indicator that takes the value one if the median firm size in the post-attack period (i.e., year *t*, year *t*+1, and year *t*+2, where year *t* is the fiscal year in which a cyberattack occurs) is above the sample median, and zero otherwise. *Big drop in sales growth* is an indicator that takes the value one if the change in sales growth from year$_{t-1}$ to the median sales growth in the post-attack period (is below the sample median, and zero otherwise. *Existence of committee with risk name* is an indicator that takes the value one if a firm has a board committee with its name including "risk" in the pre-attack period and its explicit duty involves firm-wide risk and risk management, and zero otherwise. The market model parameters are estimated using 220 trading days of return data beginning 280 days before and ending 61 days before the event announcements, using the CRSP value-weighted return as a proxy for the market portfolio return. The appendix provides detailed descriptions of the construction of the variables. *P*-values reported in parentheses are based on standard errors adjusted for heteroskedasticity and clustering at the firm level. ***, **, and * denote significance at the 1%, 5%, and 10% levels, respectively.

	Ratio of excess loss to total dollar market value loss			
Independent variable	(1)	(2)	(3)	(4)
Big firm (indicator): a	0.191*	0.124	-0.159	0.189
	(0.097)	(0.324)	(0.247)	(0.130)
Retail industry (indicator): b	-0.523***	-0.698***		
	(0.001)	(0.001)		
Big drop in sales growth (indicator): c	-0.155	-0.248**	-0.328**	-0.074
	(0.138)	(0.037)	(0.038)	(0.543)
b × c		0.412*		
		(0.089)		
a × c			0.739***	
			(0.003)	
Existence of committee with risk name (indicator)				-0.406***
				(0.004)
Leverage	-0.371	-0.413	-0.178	-0.229
	(0.322)	(0.295)	(0.607)	(0.540)
Asset intangibility	-0.458	-0.502*	-0.152	-0.416
	(0.101)	(0.075)	(0.456)	(0.224)
Tobin's *q*	0.071	0.072	0.010	0.010
	(0.147)	(0.147)	(0.791)	(0.804)
Year fixed effects	Y	Y	Y	Y
Industry fixed effects	N	N	Y	Y
Observations	75	75	75	70
Pseudo R^2	0.389	0.412	0.455	0.402
Number of left-censored observations	1	1	1	1
Number of right-censored observations	54	54	54	50
Log likelihood	-22.91	-22.05	-20.46	-21.43
χ^2	29.23	30.94	34.12	28.79
Probability > χ^2	0.006	0.006	0.003	0.017

Table 11
Cumulative Abnormal Returns (CARs) for Portfolios of Industry Competitors around Cyberattack Announcement Dates

The table presents the mean and median cumulative abnormal returns (CARs) for 146 portfolio of individual industry peer firms of attacked firms over the period 2005 to 2017 (Panel A) and estimates of ordinary least squares (OLS) regressions in which the dependent variable is the CAR from one day before the attack announcement date to one day after the attack announcement date (CAR (-1, 1)) for the value-weighted portfolio of individual industry peer firms (Panel B). Industry peer firms are firms that have the same four-digit SIC code as the attacked firm. The market model parameters are estimated using 220 trading days of return data beginning 280 days before and ending 61 days before the attack announcements, using the CRSP value-weighted (equally weighted) return as a proxy for the market portfolio return. The daily abnormal stock returns are cumulated to obtain the CAR from day t_1 before the attack announcement date to day t_2 after the attack announcement date. The appendix provides detailed descriptions of the construction of the variables. In Panel A, the numbers in parentheses are *p*-values for *t*-tests and *z*-values for Wilcoxon signed-rank tests that the mean CAR and the median CAR are equal to zero. In Panel B, *p*-values reported in parentheses are based on standard errors adjusted for heteroskedasticity and clustered at the firm level. ***, **, and * denote significance at the 1%, 5%, and 10% levels, respectively.

Panel A. Univariate analysis

	Value-weighted portfolio		Equally weighted portfolio	
CARs (%)	Mean	Median	Mean	Median
CAR (-1, 1)	-0.372***	-0.174***	-0.347***	-0.121***
	(0.000)	(-2.990)	(0.005)	(-2.584)
CAR (-2, 2)	-0.622***	-0.307***	-0.555***	-0.196***
	(0.000)	(-3.533)	(0.002)	(-2.879)
CAR (-5, 5)	-0.920***	-0.428***	-0.988***	-0.272***
	(0.000)	(-3.226)	(0.001)	(-2.675)

Panel B. OLS regressions of CARs (-1, 1) for the value-weighted portfolio of individual industry peer firms

	CAR (-1, 1)		
Independent variable	(1)	(2)	(3)
Attacked firm CAR (-1, 1): a	0.141***	0.140***	0.139***
	(0.002)	(0.000)	(0.000)
Financial information loss (indicator): b	0.004	0.002	0.002
	(0.293)	(0.465)	(0.597)
Repeated cyberattack within one year (indicator): c	-0.000	-0.002	-0.008**
	(0.899)	(0.570)	(0.019)
Returns correlation	-0.013	-0.009	-0.010
	(0.465)	(0.411)	(0.380)
Log (average price)	-0.000	0.003	0.003*
	(0.897)	(0.114)	(0.084)
Finance industry (indicator): d		0.007	-0.004
		(0.175)	(0.356)
High competition (indicator): e		0.000	0.000
		(0.868)	(0.997)
Unique industry (indicator)		0.002	0.002
		(0.360)	(0.316)
Industry Tobin's *q*		0.002	0.001
		(0.365)	(0.604)
b × d		-0.012*	
		(0.056)	
c × e			0.011**
			(0.017)
Firm-level characteristics (those used in Panel C of Table 4)	Y	Y	Y
Year fixed effects	Y	Y	Y
Industry fixed effects	Y	N	N
Observations	146	146	146
Adj. R^2	0.136	0.118	0.117

Online Appendix

Risk management, firm reputation, and the impact of successful cyberattacks on target firms

July 2019

Appendix A
U.S. Security Breach Notification Laws and Regulations

This appendix summarizes laws and regulations that require publicly listed firms in the U.S. to notify affected individuals about data breaches and report the breaches to state governments and other regulatory agencies. We briefly describe the requirements and developments of these laws and regulations including the State Security Breach Notification Laws, the **SEC Cybersecurity** Disclosure **Guidance**, and the Privacy Rule to implement the requirement of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which could affect corporate disclosure decision and thus the coverage of incidents reported by the PRC database.

A.1 State Security Breach Notification Laws

State Security Breach Notification Laws require firms to inform affected state residents about compromise of their personal information. While details of the legislations vary across states, they typically contain several common elements such as entities that are subject to the regulations (e.g., individuals, businesses, and government entities); the definition of personal information (e.g., information that can be used on its own or with other information to identify a person); the definition of breaches (e.g., accessed and/or disclosed in an unauthorized fashion); requirements for notification (e.g., timing/method of notice and entities to be notified); and exemptions (e.g., encrypted personal information). One important note regarding State Security Breach Notification Laws is that disclosure is required based on the residency of the affected consumers, not the actual location of the data breach. The National Conference of State Legislature (NCSL) provides a list of security breach laws.[32]

Appendix Table A summarizes the effective date of the State Security Breach Notification Laws.[33] As of July 2018, all 50 states and Washington D.C., Guam, Puerto Rico, and Virgin Islands in the U.S. have legislated such a law. California legislated such a law in 2003, followed by nine states in 2005 and 18 more in 2006. By 2009, a total of 46 states and four U.S. territories had legislated a law.

[32] http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.
[33] https://www.perkinscoie.com/en/news-insights/security-breach-notification-chart.html.

Alabama and South Dakota were the last to adopt the laws in 2018. Thus, the number of states that require data breach notification has increased over our sample period, suggesting that more firms are subject to breach notification requirements.

A.2 SEC Cybersecurity Disclosure Guidance

In addition to the notification requirement by the State Security Breach Notification Laws, publicly traded firms in the U.S. are required to disclose "materially important" cybersecurity risks and cyber incidents according to the Securities and Exchange Commission (SEC) **Cybersecurity** Disclosure Guidance. However, the SEC 2011 rules have been criticized by lawyers and investors since the disclosure requirements are too general without detailed instruction about the coverage of information, and the definition of "materiality" is vague and thus is subject to alternative interpretations, which may result in underreporting of cybersecurity events by attacked firms.[34] On February 21, 2018, the SEC updated the 2011 guidance regarding disclosure requirements under the federal securities laws and related policies and procedures. To address the negative consequences associated with cybersecurity incidents in a more comprehensive manner, the new SEC guideline now requires the firms to disclose the board's role in overseeing cybersecurity risk management, and prohibits insiders from trading on material nonpublic information relating to cybersecurity risks and incidents.

A.3 HIPAA Privacy Rule

The HIPAA Privacy Rule enacted in 2003 has established national standards to protect privacy regarding certain health information and medical records of individuals that are held by "covered entities" (e.g., health care clearinghouses, employer-sponsored health plans, health insurers, and medical service providers that engage in certain transactions). The Privacy Rule requires covered entities and their business associates, who hold and transmit health information in electronic form, to protect the privacy of personal health information, and sets limits and conditions on the use and disclosure of such information without patient authorization. The rule also requires covered entities and their business associates to notify the Secretary of the U.S. Department of Health and Human Services (HHS) if they discover a breach of unsecured protected health information.[35]

[34] See, for instance, "Senators Ask Wall St. Watchdog to Review Cyber Breach Disclosure Rules," *Reuters* (September 26, 2017). https://www.reuters.com/article/us-usa-cyber-senate/senators-ask-wall-st-watchdog-to-review-cyber-brea ch-disclosure-rules-idUSKCN1C02WU.

[35] The submitted breaches affecting 500 or more individuals are publicly available at the following website: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf. Due to the large size of submitted breaches, the HHS has become a major information source of data breaches since the inception of its public disclosure.

Appendix Table A
Effective Dates of Data Breach Legislation Implemented at Each U.S. State and Territory

U.S. State and Territory	Effective date
Alabama	June 1, 2018
Alaska	July 1, 2009
Arizona	December 31, 2006
Arkansas	August 12, 2005
California	July 1, 2003
Colorado	September 1, 2006
Connecticut	January 1, 2006
Delaware	June 28, 2005
District of Columbia	July 1, 2007
Florida	July 1, 2014
Georgia	May 5, 2005
Guam	July 11, 2009
Hawaii	January 1, 2007
Idaho	January 1, 2006
Illinois	June 27, 2006
Indiana	July 1, 2006
Iowa	July 1, 2008
Kansas	January 1, 2007
Kentucky	July 15, 2014
Louisiana	January 1, 2006
Maine	January 31, 2006
Maryland	January 1, 2008
Massachusetts	October 31, 2007
Michigan	July 2, 2007
Minnesota	January 1, 2006
Mississippi	July 1, 2011
Missouri	August 28, 2009
Montana	March 1, 2006
Nebraska	July 14, 2006
Nevada	January 1, 2006
New Hampshire	January 1, 2007
New Jersey	January 1, 2006
New Mexico	January 16, 2017
New York	December 7, 2005
North Carolina	December 1, 2005
North Dakota	June 1, 2005
Ohio	February 17, 2006
Oklahoma	November 1, 2008
Oregon	October 1, 2007
Pennsylvania	June 20, 2006
Puerto Rico	January 5, 2006
Rhode Island	March 1, 2006
South Carolina	July 1, 2009
South Dakota	July 1, 2018
Tennessee	July 1, 2005
Texas	April 1, 2009
Utah	January 1, 2007
Vermont	August 12, 2012
Virgin Islands	October 17, 2005
Virginia	July 1, 2008
Washington	July 24, 2005
West Virginia	June 6, 2008
Wisconsin	March 31, 2006
Wyoming	July 1, 2007

Appendix B
Time Interval from the Occurrence of Cyberattacks to Their Disclosure

This appendix presents summary statistics for the number of days from the date a cyberattack occurred to the date in which the incident is discovered by a firm or a third party and the number of days from the date in which the incident is discovered by a firm or a third party to the date of media reporting (a firm's reporting to the state regulator, a firm's SEC 8-K filing). We manually collect the information on occurrence, discovery, and reporting dates by searching *Factiva*, breach reports disclosed by the state Attorney General's Offices, and cyber security expert blogs such as Krebs on Security (https://krebsonsecurity.com).

Time interval (days)	N	Mean	Median	Min.	Max.
From occurrence of the incidence to discovery	40	47.2	14.5	0	416
From discovery to media reporting	67	16.2	10.0	0	140
From discovery to reporting to the state regulator	35	27.9	18.0	1	135
From discovery to reporting to the SEC	12	19.3	9.0	0	70

Appendix C
Effects of Cyberattacks on the Presence of CIOs and Outside Directors with CIO Experience in the Post-Attack Period

In this appendix, we examine the effect of cyberattacks on the presence of the Chief Information Officer (CIO) and the proportion of outside directors with prior CIO experience to the total number of directors on the board. Attacked firms often announce the replacement of responsible executives such as the CIO to cope with the aftermath of the attack. For instance, Equifax announced the replacements of CIO and Chief Security Officer eight days after its initial public announcement of cybersecurity incident on September 7, 2017. The results reported in Appendix Table C. In column (1), we use an indicator for the presence of the CIO as the dependent variable. We find that the coefficient on the interaction term between *Post* and *Cyberattack* is positive and significant at the 1% level, suggesting that the likelihood of hiring the CIO increases for attacked firms in the post-attack period. The presence of the CIO is particularly evident in the first two years ($Year_{t+2}$) after the attack (column (2)). In columns (7) and (8), we use as the dependent variable the proportion of outside directors with CIO experience on the board and find that it increases significantly in the post-attack period, especially in $Year_{t+2}$, suggesting that attacked firms actively look for board members with IT expertise.

We next investigate whether a firm's decision to invest in risk management policies in the post-attack period is affected by its customer clientele. We divide the sample into firms operating in unique industries and those operating other industries according to industry-median product uniqueness (the ratio of a firm's selling expenses to sales (Titman and Wessels (1988)). We expect customers of firms that sell more unique or specialized products (e.g., Tiffany & Co.) to have greater concerns about data security and thus to demand more investment in cybersecurity. Consistent with this expectation, we find that an increase in cybersecurity investment in the post-attack period measured by the presence of the CIO is concentrated among firms operating in the unique industry (columns (3)-(6)). We also find some weak evidence that the proportion of outside directors with CIO experience increases in $Year_{t+2}$ only among firms operating in the unique industry (columns (9)-(12)). These results suggest that firms' post-attack investment in risk management policies is greater for firm that sell more unique products and thus cater to customers with higher demands for data security.

Appendix Table C
Effects of Cyberattacks on the Presence of CIOs and the Proportion of Outside Directors with CIO Experience on the Board

The table presents estimates of ordinary least squares (OLS) regressions in which the dependent variables are an indicator for the presence of a chief information officer (CIO) in a given year in columns (1)-(6) and the proportion of outside directors with CIO experience to the total number of directors on the board in columns (7)-(12). The sample consists of 1,160 firm-year observations (113 treated firms that experience a cyberattack involving financial information loss over the period 2005 to 2015 and 113 control firms that do not experience a cyberattack over the same period). The propensity score is calculated using the logit regression of *Cyberattack* (an indicator that takes the value of one if a firm experiences a cyberattack involving financial information loss, and zero otherwise) on firm size, stock performance, stock return volatility, leverage, and institutional blockholder (indicator). We require both treated and matching firms to be in the same industry (the same two-digit standard industrial classification (SIC) codes) and in the same fiscal year. *Post* is an indicator that takes the value of one for post-attack period (year *t*, year *t*+1, and year *t*+2), and zero for pre-attack period (year *t*-1 and year *t*-2, and year *t*-3), where year *t* is the fiscal year in which a cyberattack occurs. Columns (3)-(6) and (9)-(12), we divide the sample into two subgroups according to whether firms operate in the unique industry. *Unique industry* is an indicator that takes the value of one if a firm's industry median product uniqueness (selling expense / sales) is above the sample median, and zero otherwise. *P*-values reported in parentheses are based on standard errors adjusted for heteroskedasticity and clustering at the firm level. ***, **, and * denote significance at the 1%, 5%, and 10% levels, respectively.

	Presence of the CIO (indicator)						Proportion of outside directors with CIO experience					
	Full sample		Unique industry		Non-unique industry		Full sample		Unique industry		Non-unique industry	
Independent variable	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)
Post (indicator) ×	0.077***		0.091**		0.061		0.003*		0.003		0.004	
Cyberattack (indicator)	(0.010)		(0.013)		(0.216)		(0.081)		(0.274)		(0.140)	
Year $_t$		0.085*		0.068		0.102		0.000		-0.002		0.002
		(0.061)		(0.236)		(0.168)		(0.920)		(0.414)		(0.164)
Year $_{t+1}$		0.077*		0.103**		0.046		0.003		0.002		0.004
		(0.072)		(0.045)		(0.531)		(0.208)		(0.504)		(0.321)
Year $_{t+2}$		0.033		0.028		0.036		0.009**		0.012**		0.005
Control variables (ROA and those used in Panel B of Table VII)	N	Y	N	Y	N	Y	N	Y	N	Y	N	Y
Firm fixed effects	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Industry-year cohort fixed effects	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Observations	1,160	1,135	650	631	500	495	1,160	1,135	650	631	500	495
Adj. R^2	0.557	0.561	0.615	0.624	0.478	0.470	0.724	0.727	0.730	0.732	0.679	0.685

Appendix D
Effects of Cyberattacks on the Value of Individual Industry Peer Firms

In this appendix, we examine the effects of cyberattacks on the value of individual industry peer firms. Panel A of Appendix Table D shows the CARs for individual peer firms of an attacked firm. We find that the mean individual peer firm CAR (-1, 1) computed using the CRSP value-weighted index return as the market portfolio return is an insignificant -0.03%. However, the median individual peer firm CAR (-1, 1) is -0.18%, which is significant at the 1% level, suggesting that cyberattacks have a significant negative spillover effect on individual industry peer firms. Using the CRSP equally weighted index return as the market portfolio return leads to similar results.

Next, to examine whether spillover effects shown in Panel A differ across characteristics of peer firms, in Panel B of Appendix Table D, we estimate OLS regressions of CARs (-1, 1) for individual peer firms of attacked firms on peer firm characteristics and CARs (-1, 1) for attacked firms. We include as peer firm characteristics an indicator that takes the value one if a peer firm is headquartered within 60 miles of the attacked firm, and zero otherwise (*Within 60 miles of an attacked firm (indicator)*), the correlation between the individual industry peer firm's stock return and the attacked firm's stock return (*Attacked firm CAR (-1, 1)*) for the year preceding the cyberattack announcement (*Return correlation*), and other firm characteristics measured in fiscal year immediate before the cyberattack announcement used in Panel C of Table IV. In Regression (1), we find that the coefficient on the *Attacked firm CAR (-1, 1)* is positive and significant at the 5% level, suggesting that cyberattacks signal negative information about industry-wide problems in risk management and IT security systems. For peer firm characteristics, we find that the coefficient on *Within 60 miles of an attacked firm (indicator)* and *Return correlation* are negative but insignificant. However, the coefficients on *ROA* and *Sales growth* are positive and significant, suggesting that cyberattacks affect better-performing peer firms less adversely. The coefficients on Tobin's *q* is negative and significant at the 10% level, suggesting that peer firms with higher future growth opportunities suffer more from focal firms' cyberattacks. In Regression (2), we include an interaction term between *Attacked firm CAR (-1, 1)* and *Within 60 miles of an attacked firm (indicator)* as an additional explanatory variable. We find that while the coefficient on *Within 60 miles of an attacked firm (indicator)* remains negative and insignificant, its interaction with *Attacked firm CAR (-1, 1)* is negative and significant at the 5% level. These results indicate that geographically proximate peer firms benefits from cyberattcks on the other firms in the same industry, possibly due to the weakening industry position of an attacked firm in the local area. In Regression (3), we add *Risk committee (indicator)*, *Presence of CIO (indicator)*, and governance characteristics (i.e., board size, proportion of independent directors on the board, and CEO-chair duality (indicator)) as additional explanatory variables. We find that the coefficient on the proportion of outside directors on the board is

positive and significant, suggesting that well-governed peer firms suffer less from their rivals' cyberattacks. However, the coefficient on other variables are not significant.

Overall, these results suggest that although cyberattacks, on average, negatively affect industry peer firms' market values, some peer firms such as well-performing firms, high-growth firms, firms with more outside directors, and firms that are located proximately to the attacked firm are affected less adversely by cyberattacks in their industry.

Appendix Table D
Effects of Cyberattacks on the Value of Individual Industry Peer Firms

The table presents the mean and median cumulative abnormal returns (CARs) for 6,094 individual industry peer firms of an attacked firms (Panel A) and estimates of ordinary least squares (OLS) regressions in which the dependent variable is the CAR from one day before the attack announcement date to one day after the attack announcement date (CAR (-1, 1)) for individual industry peer firms. The sample consists of 5,775 individual industry peer firms that have the same four-digit SIC code as firms experiencing cyberattacks over the period 2005 to 2017. *Within 60-miles of an attacked firm* is an indicator that takes the value one if an industry peer firm is located within 60-miles of the attacked firm, and zero otherwise. *Returns correlation* is the correlation between the individual industry peer firm return and the attacked firm return for the year preceding the cyberattack announcement. The market model parameters are estimated using 220 trading days of return data beginning 280 days before and ending 61 days before the breach announcements, using the CRSP value-weighted return as a proxy for the market portfolio return. In Panel A, the numbers in parentheses are *p*-values for *t*-tests and *z*-values for Wilcoxon signed-rank tests that the mean CAR and the median CAR are equal to zero. In Panel B, *p*-values reported in parentheses are based on standard errors adjusted for heteroskedasticity and clustered at the event level. ***, **, and * denote significance at the 1%, 5%, and 10% levels, respectively.

Panel A. CARs for individual industry peer firms

	CRSP value-weighted index return		CRSP equally weighted index return	
CARs (%)	Mean	Median	Mean	Median
CAR (-1, 1)	-0.034	-0.177***	-0.071	-0.169***
	(0.522)	(-3.456)	(0.176)	(-3.867)
CAR (-2, 2)	0.062	-0.213**	-0.008	-0.261***
	(0.370)	(-2.538)	(0.907)	(-3.288)
CAR (-5, 5)	0.266	-0.237	-0.157	-0.295***
	(0.018)	(-1.477)	(0.163)	(-4.106)

Panel B. OLS regressions of CARs (-1, 1) for individual industry peer firms

	CAR (-1, 1)		
Independent variable	(1)	(2)	(3)
Attacked firm CAR (-1, 1): a	0.125**	0.138***	0.133***
	(0.017)	(0.006)	(0.009)
Within 60 miles of an attacked firm (indicator): b	-0.000	-0.002	-0.002
	(0.979)	(0.446)	(0.457)
a × b		-0.230**	-0.211**
		(0.023)	(0.030)
Returns correlation	-0.008	-0.007	-0.008
	(0.181)	(0.200)	(0.153)
Firm size	0.000	0.000	0.000
	(0.565)	(0.594)	(0.545)
Log (firm age)	-0.001	-0.001	-0.001
	(0.345)	(0.385)	(0.303)
ROA	0.011**	0.011**	0.010
	(0.031)	(0.027)	(0.101)
Leverage	0.000	0.000	0.000
	(0.927)	(0.931)	(0.939)
Financially constraint (indicator)	0.001	0.001	0.001
	(0.744)	(0.734)	(0.699)
Sales growth	0.005*	0.005*	0.005*
	(0.095)	(0.088)	(0.067)
Tobin's *q*	-0.001*	-0.001*	-0.001*
	(0.079)	(0.066)	(0.098)
Institutional block ownership	-0.000	-0.000	-0.000
	(0.934)	(0.917)	(0.880)
Risk committee (indicator)			-0.002
			(0.470)
Board size			-0.000
			(0.516)
Proportion of outside directors on the board			0.013**
			(0.041)
CEO-chair duality (indicator)			-0.000
			(0.817)
Year fixed effects	Y	Y	Y
Industry fixed effects	Y	Y	Y
Observations	5,775	5,775	5,601
Adj. R^2	0.024	0.025	0.026