Software Diffusion and Cyber Risk*

Giorgio Ottonello† Antonino Emanuele Rizzo‡

August 12, 2026

Abstract

The growth in size and concentration of the software industry is an important driver of cyber risk in the economy. Software products contain vulnerabilities that spread to customer firms and expose them to cyberattacks. We test this mechanism using a novel database that connects vulnerability discoveries and subsequent cyberattacks to software companies and their customers. Guided by a simple theoretical framework, we first show empirically that exposure to software vulnerabilities significantly increases a firm's likelihood of experiencing cyberattacks and elevates standard measures of firm risk. We then examine the aggregate implications, demonstrating that the recent rise in cyber risk is closely tied in the data to the expanding scale and concentration of the software industry.

JEL-Classification: G24, G32
Keywords: cyber risk, software vulnerabilities, software companies, firm risk, digital supply chain

*A previous version of this paper was titled *Do Software Companies Spread Cyber Risk?*. We thank for useful comments Vladimir Asriyan, Robert Battalio, Zhi Da, Nuri Ershain, Marcin Kacperczyk, Vasso Ioannidu, Alan Kwan, Michael Lee, Marco Macchiavelli, Xu Qiping, Victoria Vanasco, Silvio Vismara, Christian Wagner, Michael Weber as well as seminar participants at the University of Notre Dame, Southern Methodist University, University of Illinois Urbana-Champaign, Nova SBE, Universitat Pompeu Fabra, WU Vienna, ESCP Turin, Zayed University, SIPA-FRBNY Cyber Risk Workshop and conference participants at SGF 2024, CREDIT 2024, MadBarWorkShop 2024, CUHK-RAPS-RCFS 2024, 2025 State-of-the-Field Conference on Cyber Risk to Financial Stability, 2nd Financial Fraud, Misconduct and Market Manipulation Conference 2025 and the 2025 Third Party Service Provider Risks Workshop. Any remaining errors are our own.

†WU Vienna, Email: giorgio.ottonello@wu.ac.at
‡ESADE Business School, Email:emanuele.rizzo@esade.edu

1 Introduction

Software companies are essential in today's economy. According to Software.org (2021), they provided 15.8 million jobs in 2020 and contributed $933 billion in direct value-added GDP in the U.S. alone. This reflects a structural economic shift over the past few decades, characterized by an increase in the size of the software industry (Gómez-Cram and Lawrence, 2025) and a rise in its concentration (Crouzet and Eberly, 2019).

Our paper investigates how the growth and concentration of software companies contribute to novel and understudied sources of risk for firms and for the economy. We conjecture that the structural change in the software industry contributes to increasing cybersecurity risk. Our hypothesis centers on two key properties of software programs, the primary products of software companies. First, multiple firms can use them simultaneously as inputs in production, thereby enabling their broad diffusion in the economy. This property is called *non-rivalry in use* and is typical of intangible capital (Crouzet et al., 2022). Second, software programs are frequently susceptible to software vulnerabilities (SVs), which are flaws that hackers can exploit to launch cyberattacks on organizations utilizing the vulnerable software. As software companies grow and their market concentration rises, a larger number of firms become exposed to the same SVs, thereby increasing the likelihood and impact of cyberattacks.

To formally assess our conjecture, we build on the literature studying the microfoundations of aggregate shocks (e.g., Gabaix (2011)) and we develop a simple theoretical framework that illustrates the impact of SVs on individual firms and the economy. In this framework, firms use software and are exposed to cyberattacks. The probability of a cyberattack increases with exposure to SVs. Importantly, we model SVs as a software-specific latent factor, implying that exposure is shared by all firms using the same software. As a result, a vulnerability affecting widely used software poses risks for a larger share of the economy. The shared nature of SVs also influences their stock market implications. Specifically, exposure to SVs affects stock returns through the occurrence of cyberattacks, and because this exposure is shared, it has implications for the comovement of stock returns.

The model yields empirical predictions that we test in two steps. First, we study whether

the emergence of a SV leads to an increase in firm-level risk. Second, we investigate whether a larger and more concentrated software sector amplifies the aggregate consequences of SVs at the economy level. We find that the answer to both questions is positive.

Key to our analysis is a novel database that links each software vulnerability discovered between 2006 and 2024 to the software company producing the vulnerable product. Thanks to information we add on the supply chain of software companies, we identify the set of firms exposed to SVs. Specifically, a company is exposed to a SV if, at the moment of its disclosure, it is a customer of the software company whose product is vulnerable. We complement this data with a large, manually compiled list of cybersecurity attacks, which offers an important advantage over what is currently available in the literature. To the best of our knowledge, we are the first to link a significant portion of cyberattacks to specific vulnerabilities in software products.

Our theoretical framework starts from the assumption that exposure to a SV raises the number of cyberattacks a company suffers. Our first set of empirical analyses provides support for this assumption. In our baseline specification, we document that firms exposed to an additional SV are three times more likely to suffer a cyberattack in the following quarter. As we observe the root cause of each attack, we are able to reinforce the interpretation of the baseline effects as driven by SVs. When we focus on cyberattacks that we can trace back to a specific SV, the effect intensifies, as firms become five times more likely to experience a cyberattack. By contrast, and reassuringly, SVs have no predictive power for attacks arising from other causes, such as phishing campaigns. This null result speaks against any alternative explanation based on unobserved factors that correlate with both vulnerability-originated and non-vulnerability-originated attacks.

Next, we investigate the relationship between SVs and firm risk. If companies using vulnerable software are more exposed to cyberattacks, we should observe an impact of SVs on standard metrics of risk. To assess this testable implication of our theoretical framework, we regress one-quarter-ahead change in firm risk on an indicator for vulnerability exposure. We use several proxies for risk, including stock return volatility, 95% Value at Risk (VaR), 95% Expected Shortfall (ES), and second-order lower partial moment (LPSD). While the first measure captures overall volatility, the other proxies are designed to capture tail risk. The latter is particularly relevant for

our application, as cyberattacks are typically extreme, low-frequency events.

We find that being exposed to a SV increases firm risk, and especially left-tail risk. The magnitude of the increase ranges between 0.07 and 0.09 standard deviations. In addition, we show that firms exposed to SVs experience an increase in their expected stock returns between 10 and 60 days after the SV has been publicly announced. This result suggests that the rise in firm risk is associated with an increase in companies' discount rates.

Additional tests support the interpretation that results on cyberattacks and firm risk are driven by SVs rather than by other, unobserved factors. First, we perform a falsification test that exploits the severity scores assigned to SVs by the National Vulnerability Database (NVD). The severity score, which evaluates the level of threat that the vulnerability poses to a company, allows us to distinguish between major and minor vulnerabilities. We show that only major vulnerabilities impact the likelihood of cyberattacks and firm risk. Minor vulnerabilities have no detectable impact, and yet they correlate with several potential unobserved factors. Second, using the block permutation method from Chetty, Looney, and Kroft (2009), we randomize the timing of vulnerabilities and demonstrate that it is crucial in determining the effect on the frequency of cyberattacks and the firm risk variables. Jointly, these tests speak against the possibility that our findings are influenced by unobservable characteristics that might drive the matching between firms and software suppliers and, ultimately, influence outcome variables.

Results so far document the *average* effect of SVs on the probability of cyberattacks and on firm risk. However, for some firms the adverse consequences might be exacerbated. For example, companies that possess limited security resources or that handle vast amounts of sensitive data might be ex-ante more attractive to attackers. Following this conjecture, we first study the heterogeneous effects of SVs on firms with high and low ex-ante cybersecurity risk, proxied either by the past number of cyber attacks or a text-based cyber risk measure similar to Florackis et al. (2022). Consistently, we observe that all the effects of SVs we document in our baseline results are worsened for firms with higher ex-ante exposure to cyberattacks. Second, we repeat our baseline tests separately for companies with high versus low cybersecurity protection, proxied by the number of relationships with cybersecurity firms. Hiring a cybersecurity specialist is one

way for companies with limited internal resources to protect themselves against cyberattacks. Consistent with this intuition, we document that firms employing a cybersecurity firm at the moment a SV is discovered are shielded from its adverse consequences. The fact that in our data many firms do not hire a cybersecurity specialist suggests there might be frictions that prevent all firms from getting cybersecurity protection in equilibrium. Finally, we split the sample based on firms' software expertise. The latter is proxied by the length of relationships firms maintain with their software suppliers. We argue that firms with shorter relationships' length likely have less expertise in the software adopted, which could be a hurdle to timely identifying and reacting to the SV. Our results indicate that the SVs' impact on cyberattacks probability and firm risk is particularly pronounced for firms with shorter supply chain relationships.

The significant impact of SVs on cybersecurity and firm risk begs the question of how firm policies change in response to their emergence. Motivated by theoretical and empirical work that links increases in firm risk with decreases in firms' investment (see, e.g., Bloom, Bond, and Van Reenen (2007), Bloom (2009), Hassan et al. (2019)), we analyze firms' investment policies. In line with prior research, we find that exposure to a SV, and the associated rise in firm risk, depresses firms' capital investment rate and CapEx growth by 0.06 and 0.13 standard deviations, respectively. We also explore whether firms "actively" manage the rise in cybersecurity risk associated with SVs. In this respect, we find that in response to a new SV exposure firms i) are more likely to hire a cybersecurity specialist company; ii) tend to improve their data privacy and security procedures. These findings support the interpretation that our measure captures an increase in cybersecurity risk and show how firms may respond to this new type of threat.

Our empirical tests so far support the claim that SVs are a primary driver of cyber risk for corporations. Building on these insights, we study the aggregate implications of SVs as well as how the structure of the software industry determines their magnitude. In this respect, our theoretical framework yields two predictions. First, the emergence of software vulnerabilities leads to a larger aggregate number of cyberattacks when a greater share of firms relies on software. Second, SVs have a stronger positive impact on aggregate risk when the software sector is both larger and more concentrated. The intuition for the role of concentration is straightforward. For SVs to influence

aggregate market volatility, their effects must be non-diversifiable. This occurs when the software sector is concentrated, so that SVs in a single product affect a large share of the market at the same time.

The model's predictions find empirical support in the data. At the software company-level, using a panel of variables aggregated across each software vendor's customers, we document that a SV leads to a greater number of cyberattacks when it emerges in the product of a larger software company. When we examine firm risk measures averaged across a software company's customers, we find that a SV leads to a larger increase in firm risk when it affects the product of a company with a larger market share, but only in periods when the software sector itself is larger. Next, we test the corresponding predictions at the economy-level. An interaction term between the number of discovered SVs per software company and the sales-based size of the software sector is positively and significantly associated with the number of cyberattacks in the economy. We also find that the software sector concentration magnifies the impact of SVs on aggregate volatility, but only when the sector is large enough. Overall, these findings support the model predictions, namely that a larger and more concentrated software sector is linked to an increase in cyber risk in the economy.

Our paper relates to the literature that studies the diffusion of new technologies and its economic implications.[1] More specifically, we link to studies on the diffusion of digital technologies, which are mainly based on software, a first order driver of the growth of intangible capital over the last decades (Crouzet et al., 2022). Recent papers have focused on the effect of such trend on corporate valuations (Gómez-Cram and Lawrence, 2025) and investment (Crouzet and Eberly, 2023). We add to the literature by showing that the diffusion of digital technologies, and more broadly intangible capital, can be an important driver of novel types of risk.

We also contribute to the growing literature on cybersecurity and finance. Recent papers have produced measures of cybersecurity risk at the firm level (Jamilov, Rey, and Tahoun, 2025; Florackis et al., 2022). Others have instead focused on the effect of cyberattacks on firms (Crosignani,

[1]The literature is extremely vast. For real effects, see for example Autor, Levy, and Murnane (2003), Acemoglu and Restrepo (2020), Akerman, Gaarder, and Mogstad (2015), Bloom et al. (2021). For the impact on financial markets, see Pástor and Veronesi (2009), Kogan et al. (2017), Ward (2020).

Macchiavelli, and Silva, 2023), the financial system (Duffie and Younger, 2019; Eisenbach, Kovner, and Lee, 2022; Kotidis and Schreft, 2025; Eisenbach, Kovner, and Lee, 2023), or government institutions (Curti et al., 2023). Our paper differs from this line of work as we approach the question from a new angle: we study the role of a large and concentrated software industry in amplifying cyber risk. In that respect, our results shed light on the economic drivers (software industry structure) behind the documented fact that idiosyncratic firm-level cyber risk does not wash out in the aggregate (Jamilov, Rey, and Tahoun, 2025).

Finally, our evidence indicates that SVs propagate cyber risk through the digital supply chain network of the software company, even to customers that belong to different industries. In that respect, we also contribute to the literature that examines how supply chains can serve as a medium through which risks are transmitted in the economy (Hertzel et al. (2008), Barrot and Sauvagnat (2016), Carvalho et al. (2021)). We add to this literature by introducing another important dimension of risk that propagates though supplier-customer links: cyber risk.

2 Institutional Background on Software Vulnerabilities

This section provides relevant institutional background on SVs and the role that software companies play in this context. First, we describe the process that leads to the public disclosure of SVs. Second, we show why SVs pose significant risk even after being publicly disclosed and despite security patches are made available. This discussion informs our analysis, in which investigate the effects of SVs after they are disclosed to the public.

2.1 Timing of Public Disclosure of SVs

A SV is a flaw in a software program, application, or operating system, which can be used with security impact. SVs pose a high risk to users of the affected software because cybercriminals exploit these vulnerabilities to compromise systems, gaining unauthorized access, stealing data, or disrupting services.

There are three groups of agents that can discover SVs. The first one are the software companies

themselves, who test their products to spot vulnerabilities before an attack is launched. The second group are independent security researchers, who cooperate with vendors and scan their software searching for flaws. Finally, a malicious hacker may be the first to discover the vulnerability. This is the worst case scenario, since there is no way to guard against the exploit before an attack happens. After a vulnerability is discovered, several considerations influence the decision of when to make it public. On the one hand, software companies may prefer to maintain knowledge of SVs private. Disclosing a SV can cause damages to reputation and brand image, not to mention the potential legal liabilities if a vulnerability results in data breaches or other forms of harm to users. Disclosure of a SV can also give attackers the very information they need to exploit a security hole in a system and cause harm. On the other hand, there are significant benefits in a timely disclosure of SVs. Public disclosure of software flaws enables informed consumer choice, and may push vendors to develop fast solutions for the vulnerabilities and build more secure products. Moreover, public disclosure may have its merits even absent a patch, as it is useful to inform other researchers, security experts, and the broader community about the vulnerability. Cybersecurity professionals and enterprises whose systems are at risk may try to find other ways to mitigate or eliminate the threat.

How to best regulate the public disclosure of SVs is still an open question and one that generates a vigorous public policy discussions in the security field. What matters for the purpose of this paper, however, is that a SV can be disclosed even if a patch does not exist. The CISA policy, for example, is to "disclose vulnerabilities as early as 45 days after the initial attempt to contact the vendor is made regardless of the availability of a patch or update.[2] In this respect, a particularly harmful type of SVs is so-called zero-day vulnerability. This is an application flaw for which there is no solution provided by software companies and the vulnerability is being actively exploited by malicious actors.

[2]CISA vulnerability disclosure process.

2.2 Are SVs Harmful after Disclosure?

A vulnerability can remain dangerous for the users of an application years after its discovery, regardless of the disclosure of the SV or the existence of a patch (e.g., August, Niculescu, and Shin (2014), August et al. (2022)). The US Department of Homeland Security estimates that approximately 80 percent of successful security breaches involve SVs for which a patch exists but has not been implemented (Microsoft report). The key issue is that few companies are able to properly patch all vulnerabilities to which they are exposed. For example Tenable, a cybersecurity company, reports that only 10% of organizations address all their open vulnerabilities within a year of first assessment (Tenable report). There are at least three reasons why companies remain vulnerable despite patches are available.

First, the sheer number of security patches a company should be aware of and apply is monumental. On average, a company uses around 110 applications, a figure that has been growing since 2015 (Bettercloud report). Hence, IT specialists must monitor on average 110 applications for the updates and, when necessary, patch them. This issue is exacerbated by the fact that many organizations do not have full and complete inventories of all applications and software they are using. Moreover, the process of patching a single vulnerability is time consuming, as companies need to navigate the various processes involved in the patch and test it to ensure it does not interfere with the company's operations.[3] Second, and related, many companies lack the staff and the expertise to properly address all vulnerabilities. Today's extremely complex IT systems impose a heavy burden on company's IT specialists, who need to understand the vast network dependencies of each application to apply a patch effectively. Finally, there are instances where patching is simply not possible. For example, a legacy software that a company requires for day to day operations may no longer be supported by the manufacturers, either because they discontinued the product or the producer is no longer in business. Another common issue is that patching often requires systems to be stopped and then rebooted during the installation, meaning that the system's services are going to experience downtime period. Downtime costs are often very high for companies. For some of them, even a small amount of downtime is not an option (e.g., healthcare

[3]On average it takes 12 days for a company IT teams to coordinate for applying a patch across all company's devices (Ponemon Institute report).

sector).

To sum up, software vulnerabilities pose a serious threat to companies, and one that is hard to contain. While we only observe SVs in the data after disclosure, there are valid reasons to believe that any impact they may have on companies can still manifest after disclosure.

3 Theoretical Framework

To guide our empirical analysis, in this section we develop a simple theoretical framework to study how SVs affect individual firms and the broader economy. The framework builds on the literature studying the microfoundations of aggregate shocks, especially Gabaix (2011), as well as on the literature exploring the financial markets' implications of extreme events, in particular Kruttli, Tran, and Watugala (2025). At the firm level, the key insight of the model is that exposure to software vulnerabilities increases firm risk. At the aggregate level, the framework delivers two main predictions. The first states that the expected number of cyberattacks increases with the number of discovered SVs and the relative sales-based size of the software sector. The second prediction illustrates that, besides the number of discovered SVs and the relative size of the software industry, increases in aggregate risk are linked to a third factor: the sales-based Herfindahl–Hirschman Index of the software sector. Therefore, industry concentration amplifies aggregate volatility but does not affect the total number of attacks. The role of concentration is intuitive: as more firms depend on the same software product, the undiversifiable component of vulnerability-induced risk increases, amplifying aggregate stock market volatility.

3.1 Model Setup and Firm-level Implications

Consider an economy with N firms, with a number $T_{S,t} \leq N$ of them using a single unit of software at time t. The total number of firms using software s at time t is indicated by $Z_{s,t}$, with $\sum_s Z_{s,t} = T_{S,t}$. For simplicity, we assume that each software company has one software product, allowing us to denote a software company and its software product with s. The entire software sector is instead denoted by S.

Firms are exposed to cyberattacks. A central assumption of the model, which we test empirically in Section 5.1.1, is that exposure to SVs increases the likelihood that firms experience cyberattacks. The assumption has a sound economic foundation, as outlined in Section 2: ceteris paribus, a vulnerable software product is easier to hack than one without vulnerabilities. Formally, we characterize the number of cyberattacks hitting customer firm c in period $t+1$ as follows:

$$CA_{c,t+1} = a_c + \gamma_c I_{s(c),t} SV_{s(c),t} \tag{1}$$

where a_c is a scalar term representing the unconditional average number of cyberattacks affecting firm c; γ_c represents firm c exposure to software vulnerabilities, and it captures firm-level characteristics such as the quality of internal cybersecurity procedures, or whether the firm has hired a cybersecurity specialist firm; $I_{s(c),t}$ is an indicator equal to one if firm c uses software product s at time t; $SV_{s(c),t}$ is a random variable that counts the number of vulnerabilities hitting firm c at time t through software s. To capture the notion that SVs hit firms because of the software they use, we model $SV_{s(c),t}$ as a shared random effect, or a software-specific latent factor.[4] Each customer firm c using a software at time t is linked to a specific software product s. Firms either do not use a software, or they use the same software at each time t.[5] Each software product has an associated Poisson-distributed random effect, $SV_s \sim \mathcal{P}(\Lambda)$. Λ represents the expected number of vulnerabilities emerging in each software product. The random effect is shared by all firms using the same software, but the random effects originating from two different software products are independent of each others.

The occurrence of cyberattacks can be interpreted as a firm-level idiosyncratic shock which affects a firms' valuation. Borrowing from Kruttli, Tran, and Watugala (2025), we model the one-period return of customer firm c at $t+1$ as:

$$R_{c,t+1} = \mu_c + b_c F_{t+1} + \delta_c CA_{c,t+1} \tag{2}$$

where μ_c is a drift term; F_{t+1} is a common factor, with mean μ_F and variance σ_F^2; δ_c describes

[4] See i.e., Duffie et al. (2009) for a similar approach to model correlated defaults.

[5] The main conclusions of the model do not change if we let firms choose a different software in each period t.

the market impact of a cyberattack on the return of firm c; $CA_{c,t+1}$, the number of cyberattacks hitting firm c is assumed independent of factor returns F_{t+1}.

Under these assumptions, and given the cyberattack process in (1), the variance of stock c's return is:

$$Var(R_{c,t+1}) = b_c^2\sigma_F^2 + \delta_c^2\gamma_c^2 I_{s(c),t}\Lambda \tag{3}$$

Equation (3) delivers a firm-level testable implication: the risk of a stock increases as the expected number of vulnerabilities affecting customer firm c through its usage of software s increases.

3.2 Aggregate Implications

In expectation, the aggregate number of cyberattacks per firm in the economy ($\frac{CA_{t+1}}{N} = \frac{1}{N}[\sum_{c=1}^{N} CA_{c,t+1}]$) is given by:

$$E\left(\frac{CA_{t+1}}{N}\right) = \frac{1}{N}\left[\sum_{c=1}^{N} a_c + \sum_{c=1}^{N} \gamma_c I_{s(c),t} E(SV_{s(c),t})\right] \tag{4}$$

the second term within brackets captures the contribution of software-related vulnerabilities: it is larger when software usage in the economy is higher, that is, when total software adoption $\sum_s Z_{s,t} = T_{S,t}$ is larger. Recall that $Z_{s,t}$ measures the sales of software product s as each firm uses a single unit of software. In the special case where the unconditional average number of cyberattacks is identical across firms ($a_c = a, \forall c = 1, .., N$), all firms have the same exposure to vulnerabilities ($\gamma_c = \gamma, \forall c = 1, .., N$), equation (4) simplifies to:

$$E\left(\frac{CA_{t+1}}{N}\right) = \frac{1}{N}\left[Na + \gamma\Lambda\sum_s Z_{s,t}\right] = a + \gamma\Lambda\frac{T_{S,t}}{N} \tag{5}$$

This equation delivers our first economy-level testable implication: The expected number of cyberattacks per firm at time $t+1$ is increasing in the share of firms using software ($\frac{T_{S,t}}{N}$) and in the expected number of vulnerabilities discovered (Λ).

The expected total number of cyberattacks per firm in the economy can also be decomposed

into the portion attributable to each software company as follows:

$$E\left(\frac{CA_{s,t+1}}{N}\right) = \sum_{c:s(c)=s}\left(\frac{CA_{c,t+1}}{N}\right) = \frac{1}{N}\sum_{c:s(c)=s}\left[a_c + \gamma_c I_{s,t} E(SV_{s,t})\right] \tag{6}$$

under the same simplifying assumptions above ($a_c = a$, $\gamma_c = \gamma$), this expression simplifies to:

$$E\left(\frac{CA_{s,t+1}}{N}\right) = \frac{Z_{s,t}}{N}\left(a + \gamma\Lambda\right) \tag{7}$$

The software company-level decomposition thus generates an additional testable implication: the expected number of attacks affecting customers of vendor s increases linearly with the vendor's market share ($\frac{Z_{s,t}}{N}$).

Based on Equation 2, the return on the market portfolio is:

$$R_{M,t+1} = \sum_{c=1}^{N} w_c R_{c,t+1} = \sum_{c=1}^{N} w_c(\mu_c + b_c F_{t+1} + \delta_c CA_{c,t+1}) \tag{8}$$

where w_c denotes the weight of firm c in the market portfolio. Under the assumption that the common factor F_{t+1} is independent of cyberattack realizations, the variance of the market return can be written as:

$$Var(R_{M,t+1}) = Var(\sum_{c=1}^{N} w_c R_{c,t+1}) = \sum_{c=1}^{N}\sum_{d=1}^{N} w_c w_d b_c b_d \sigma_F^2 + \sum_{c=1}^{N}\sum_{d=1}^{N} w_c w_d \delta_c \delta_d Cov(CA_{c,t+1}, CA_{d,t+1}) \tag{9}$$

where the last term captures the contribution of cyber risk to comovement in stock returns. From the cyberattack process in (1), and given the assumption of the shared-random-effect structure that vulnerabilities are independent across software products but shared among firms using the same product, we obtain:

$$\mathrm{Cov}(CA_{c,t+1},\, CA_{d,t+1}) = \begin{cases} 0, & \text{if } s(c) \neq s(d), \\ \gamma_c\, \gamma_d\, \Lambda, & \text{if } s(c) = s(d). \end{cases}$$

Thus, in the extreme case in which no two firms use the same software product, the cyber-

driven covariance term vanishes and the variance of the market portfolio collapses to the factor-risk component.

To build intuition, we again impose three simplifying assumptions: all firms have the same size, $w_c = 1/N, \forall c = 1, .., N$; all firms have the same exposure to vulnerabilities ($\gamma_c = \gamma$); and cyberattacks affect firms' stock prices equally, ($\delta_c = \delta$). With these assumptions the variance of the market portfolio simplifies to:

$$Var(R_{M,t+1}) = \frac{1}{N^2} \sum_{c=1}^{N} \sum_{d=1}^{N} b_c b_d \sigma_F^2 + \frac{\delta^2 \gamma^2 \Lambda}{N^2} \sum_{s} Z_{s,t}^2 \tag{10}$$

where $Z_{s,t}$ denotes the number of firms using software product s at time t. Writing $\sum_s Z_{s,t} = T_{S,t}$, and defining the Herfindahl–Hirschman Index of the software sector as $HHI_{S,t} = \sum_s (Z_{s,t}/T_{S,t})^2$, we obtain:

$$Var(R_{M,t+1}) = \frac{1}{N^2} \sum_{c=1}^{N} \sum_{d=1}^{N} b_c b_d \sigma_F^2 + \delta^2 \gamma^2 \Lambda HHI_{S,t} \left(\frac{T_{S,t}}{N} \right)^2 \tag{11}$$

the testable implication that emerges from (11) is that, for a given expected number of vulnerabilities, the contribution of cyber risk to aggregate market volatility increases with both the size of the software sector ($\frac{T_{S,t}}{N}$) and its concentration ($HHI_{S,t}$).

As before, we can decompose the variance of the market return into the contributions associated with each software vendor. Let $R_{s,t+1}$ denote the return among the customers of software company s. Then, since cyberattack shocks are independent across software products, we have: $Var(R_{M,t+1}) = \sum_s Var(R_{s,t+1})$.

For a given software vendor s, the variance of the returns of its customer firms is given by:

$$Var(R_{s,t+1}) = \frac{1}{N^2} \sum_{c:s(c)=s} \sum_{d:s(d)=s} b_c b_d \sigma_F^2 + \frac{\delta^2 \gamma^2 \Lambda}{N^2} Z_{s,t}^2 \tag{12}$$

where the last term uses again the fact that any two firms using software s share the same vulnerability shock. Factoring out software–sector size and concentration in the last term, we can

rewrite (12) as:

$$Var(R_{s,t+1}) = \frac{1}{N^2}\sum_{c\in s}\sum_{d\in s} b_c b_d \sigma_F^2 + \delta^2\gamma^2\Lambda\left(\frac{Z_{s,t}}{T_{S,t}}\right)^2\left(\frac{T_{S,t}}{N}\right)^2 \tag{13}$$

Thus, the final testable implication of our framework is that the risk borne by the customers of software vendor s increases with: the expected number of vulnerabilities affecting the software; the market share of company s ($\frac{Z_{s,t}}{T_{S,t}}$); and the overall size of the software sector ($\frac{T_{S,t}}{N}$).

We test the empirical implications of the theoretical framework at the firm level (Section 5.1), the software vendor level (Section 6.1), and the aggregate (economy) level (Section 6.2) in the empirical analyses presented in the remainder of the paper.

4 Data and Variable Construction

4.1 Data

We obtain accounting data and stock prices of U.S. firms for the period 2006-2024 from the CRSP-Compustat merged dataset. We gather data on supply chains from the FactSet Revere Supply Chain Relationship database.[6] We use information on customer-supplier links to identify firms using products affected by software vulnerabilities, as detailed in the next section. Our final sample of U.S. firms comes from the intersection of CRSP-Compustat merged and FactSet Revere Supply Chain Relationship.

We collect the list of known SVs from the National Vulnerability Database (NIST).[7] NIST dataset provides information on the date in which the SV was first published; the Common Vulnerabilities and Exposures (CVE) identifier; an assessment of the vulnerability risk, through the Common Vulnerability Scoring System Version 3.0 (CVSS v3.0); and finally, the identity of the

[6]FactSet Revere collects customer and supplier relationship information from primary public sources, such as SEC 10-K annual filings, investor presentations, and press releases. Its multiple sources imply that FactSet Revere is less affected by the limitation of datasets that rely on information from the Statement of Financial Accounting Standard (SFAS) No.131, which requires firms to disclose only the existence and sales to principal customers representing more than 10% of total firm revenues (see e.g., Adelino et al. (2023)).

[7]Available here. NIST updates its database at least once per day. During these updates NIST can add, correct, or enrich historical data even years after the initial entry. This means that historical data downloaded at two different points in time can be different. Our dataset has been compiled as of April 1^st, 2024.

vendor of the product affected by the vulnerability (i.e, the software company). The vulnerabilities in our sample affect at least once the software products of 55 different software companies which we can identify in Factset Revere.

We assemble a novel database on cyberattacks drawing from three data sources. The first is the Privacy Rights Clearinghouse (PRC) data. PRC is a nonprofit organization that collects information on data breaches and other cybersecurity incidents from publicly available, government-maintained data sources. PRC categorizes incidents into hacking attacks and data breaches originating from other causes. The second source is the VERIS Community Database (VCDB). VCDB provides a repository of widely collected public incidents and offers a classification of security incidents similar to that of PRC. These first two sources have been also used by other papers in the literature (e.g, Florackis et al. (2022)). We supplement this data with information retrieved from Hackmageddon, a website specializing in publishing cyberattack-related data and news.[8] Our final list includes 802 firm-cyberattack pairs.

We manually identify public US corporations in our list of cyberattacks. For each cyberattack affecting a public US firm, we manually search for information about the root cause of the attack. Whenever we can link a cyberattack to a software vulnerability we label the attack as vulnerability-related. We are able to trace back cyberattacks to vulnerabilities for 133 events. In other cases, we classify the attack as due to other causes.[9]

Our sample includes both software companies affected by SVs and companies whose products are not affected. We construct the sample of unaffected software companies in two steps. First, we identify the list of unique 4-digit SIC codes where the 55 software companies affected by vulnerabilities operate.[10] Second, we retrieve the set of firms in the CRSP-Compustat database that operate within one of the SIC 4-digit industries in the resulting list. After excluding companies

[8]More details on PRC data are https://privacyrights.org/. Info on VCDB data is https://github.com/vz-risk/VCDB. For Hackmageddon, see https://www.hackmageddon.com/.

[9]In our data we observe cyberattacks caused by: phishing, an attack that sends fake emails to steal sensitive information; malvertising, the use of online advertisements to spread malware, such as viruses or ransomware; credential stuffing or password spraying, the practice of exploiting stolen usernames and passwords across multiple services or accounts; SQL injection, an attack that uses malicious SQL code to access a company's database; or Domain Name System (DNS) hijacking, an attack in which users are redirected to malicious sites instead of the actual website they are trying to reach.

[10]The resulting list of SIC codes includes: 3570, 3571, 3572, 3576, 3577, 3620, 3651, 3661, 3663, 3674, 3825, 7370, 7371, 7372, 7373

that do not have customer information in Factset Revere, we obtain a software company-level panel that consists of 34,336 observations. On average, we observe 484 software companies each year and 1,421 unique software suppliers from 2006 through 2024. The number of software companies in our sample exceeds the total number of publicly listed software companies identified by Gómez-Cram and Lawrence (2025) from April 2003 through December 2022, which is 1,030. This discrepancy arises from the differing objectives behind the data collection in the two studies. Gómez-Cram and Lawrence (2025) focus on publicly traded companies where software is the primary source of revenue, aiming to measure the value of software with precision. In contrast, our sample includes any company involved in software production, regardless of whether it constitutes its primary revenue source, thereby encompassing any company whose products potentially contain software vulnerabilities.

4.2 Measuring Exposure to SVs

We retrieve the list of customers for each of the 1,421 software companies in our sample from Factset Revere. A customer firm enters our final sample if it has non-missing values of the variables used to estimate equation (14) in Section 5.1.1. In the resulting sample, we define a firm as exposed to a vulnerability if at the time of the SV discovery the firm is a customer of the software company producing the vulnerable software.

For some firms in our sample exposure to a SV happens within one year from the occurrence of a cyberattack that hit the firm. We exclude these cases from the set of firms exposed to SVs. There are two reasons for this exclusion. The first is that we want to rule out a simple reverse causality story: the vulnerability in a software is discovered and made public as a consequence of a successful hacking attack against the firm that used that software. Under this alternative scenario, it is the cyberattack that causes the vulnerability, and not the other way around. By excluding a vulnerability if it follows a cyberattack we make sure these incidents cannot explain our results. The second reason is that cyberattacks have a significant impact on victim firms, and this impact plausibly manifests in variables such as stock prices and firm risk. Therefore, in instances in which a vulnerability follows a cyberattack it is challenging to disentangle the effect

of the former from the impact of the latter. This is a potential concern for us, since our empirical question involves understanding whether exposure to SV, as opposed to actual incidents, has any effect on firm outcomes. Excluding cases in which a vulnerability follows a cyberattack directly addresses this concern. After applying this filter our sample includes 98,885 observations, 4,753 unique customer firms, and 1,811 treated firms. In Table 1, Panel A we present summary statistics for the main customer-level variables used in the paper.

In Table IA2 in the Internet Appendix we report statistics on SVs for each of the 55 software companies affected by SVs. The table reports, for each software company: the total number of vulnerabilities affecting its products; the total number of customers that in our data are linked to the company; and the share of customers served by the software companies. The average number of vulnerabilities by supplier is 30, with a minimum of 1 and a maximum of 584 for Microsoft. Suppliers in our list are linked on average to 161 customers, with a minimum of 2 for Bentley Systems and a maximum of 1058 for Microsoft.

In Table 2 we present the correlation between exposure to SVs and lagged firm-level covariates. The dependent variable is an indicator that takes the value 1 if a firm is exposed to a SV in one of the software products it uses. In the first three columns, we consider a list of standard firm-level characteristics: market capitalization, book-to-market ratio, profitability, leverage, and the cumulative stock return over the previous 12 months. We report the results for regression models without fixed effects, with firm fixed effects, firm and time fixed effects, and with firm and industry-time fixed effects. Interestingly, none of the firm-level controls exhibit a significant and consistent relationship with the emergence of a SV across all regression models. In Column (4), we include a variable that counts the number of cyberattacks against the company in the previous three years. This variable does not show a correlation with the likelihood of a vulnerability emerging, which is reassuring. Similar to excluding firms whose exposure to SVs follows cyberattacks, the absence of a significant relationship between the number of cyberattacks and exposure to SVs helps to rule out the possibility of reverse causality. Overall, the empirical evidence in Table 2 suggests that firm-level observables do not consistently predict SVs.

5 Empirical Findings: Firm-Level

Here we present the firm-level empirical findings of the paper. Section 5.1 includes the baseline results, which revolve around the effect of SVs on the probability of cyberattacks and on firm risk. Section 5.2 investigates the economic mechanism behind the main findings by analyzing the heterogeneous impact of SVs in the cross-section of firms, as well as how they react to SVs' exposure.

5.1 Main Results

5.1.1 Probability of Cybersecurity Incidents

In this section, we test the core assumption of our theoretical framework, as expressed in equation (1): exposure to SVs increases a corporation's cybersecurity risk. We perform this analysis using our sample of customer firms at the intersection of the Factset Revere and CRSP-Compustat merged datasets. We estimate the logit model:

$$P(\text{CyberAttack}_{c,t+1} = 1 \mid \text{SV}_{c,t}, X_{c,t}, \alpha_{i,t}) = L(\alpha_{i,t} + \beta \text{SV}_{c,t} + X'_{c,t}\gamma) \tag{14}$$

where c indexes customers, i industries based on the Fama-French 48-industry classification, and t quarters. In the first column of the table, we study the probability of experiencing a cyberattack of any type. This variable covers the full sample period from 2006 through 2024 and is sourced from all three datasets on cyberattacks described in the Data section. In the last three columns of the table, our goal is to decompose the probability of cyberattacks into the probability of cyberattacks related and unrelated to SVs. We obtain the necessary information to make this distinction from Hackmageddon, a website specializing in publishing cyberattack news. Since this website starts covering cyberattack news in 2010, in columns (2) through (4) we restrict the sample to the years from 2010 to 2024. In this reduced sample period, Column (2) again examines the probability of experiencing a cyberattack of any type. In Column (3) we focus on the subset of cyberattacks that we can directly link to a SV. Finally, in Column (4) we focus on cyberattacks that we can attribute to causes other than SVs. In all columns, the main independent variable is an indicator

that takes the value 1 if customer c is exposed to a SV coming from one of its software suppliers in quarter t. $X_{c,t}$ is a set of controls that includes market capitalization, book-to-market, ROA, previous 12-month return, and leverage. $\alpha_{i,t}$ indicates a full set of Fama–French 48-industry $\times$ time (year-quarter) fixed effects. Standard errors are clustered at the customer level. For ease of interpretation, we report the odds ratios.

Table 3, Panel A, reports the results. Column (1) shows that the coefficient on $SV_{c,t}$ is positive and highly significant. Columns (1) and (2) indicate that a firm exposed to a vulnerability through its suppliers is more than three times more likely to suffer a cyberattack of any type. When we focus on attacks that we can directly link to software vulnerabilities, the effect grows stronger: exposed firms are five times more likely to experience a SV-caused attack. In the last column, we turn to attacks unrelated to software vulnerabilities. Reassuringly, the last column shows a coefficient that is not statistically significant and of a much smaller magnitude.[11]

A necessary condition for a causal interpretation of our results is that the impact of SVs on cyber incidents follows the discovery of a vulnerability, rather than preceding it. We explore the dynamic effect of SVs on cyberattacks in Figure IA1, Panel A. To construct this figure, we run the following variation of equation (14):

$$P(\text{CyberAttack}_{c,t+n} = 1 \mid \text{SV}_{c,t}, X_{c,t}, \alpha_{i,t}) = L(\alpha_{i,t} + \beta \text{SV}_{c,t} + X'_{c,t}\gamma) \tag{15}$$

where we let n vary from two quarters before the discovery of a SV to three quarters after. The graph plots the resulting coefficients on $SV_{c,t}$ and the 95% confidence intervals. We observe no effect of a SV on cyberattacks in the two quarters before the event, while a SV remains a strong predictor of cyberattacks up to three quarters after its discovery. Overall, results in this section indicate that SVs are an important cause of cyberattacks.

[11] In Table IA3 we use OLS regressions to study the effect of SVs on the likelihood of cyberattacks and find qualitatively similar results.

5.1.2 Customer Risk

In this section, we study the impact of SVs on firm risk. This analysis follows directly from the firm-level prediction formalized in equation (3). We use several proxies for firm risk, all measured at the quarterly horizon. The first is the standard deviation of daily stock returns. The next three measures capture a firm's left-tail risk, that is, the probability of extreme negative events. We use: Value-at-risk (VaR), defined as (the absolute value of) the worst 5% daily return; Expected Shortfall, defined as (the absolute value of) the average of the worst 5% daily returns; and lower partial standard deviation (LPSD), defined as the standard deviation of negative daily stock returns.[12] We run:

$$log(Risk_{c,t+1}/Risk_{c,t-1}) = \alpha + \beta SV_{c,t} + \gamma X_{c,t} + \epsilon_{c,t+1} \tag{16}$$

where $log(Risk_{c,t+1}/Risk_{c,t-1})$ is the logarithm of the change between quarter $t-1$ and quarter $t+1$ in each of the four risk measures. For ease of interpretation we standardize the dependent variables. $X_{c,t}$ is a set of controls that includes market capitalization, book-to-market, ROA, previous 12-month return, leverage, and the number of cyberattacks experienced by firm c in the year preceding quarter t. α indicates firm and Fama–French 48-industry $\times$ time (year-quarter) fixed effects. Standard errors are clustered at the customer level.

The results are displayed in Table 4. The discovery of a SV in the software used by customer c in quarter t leads to an increase in firm risk, regardless of the variable used. The effect is economically meaningful and consistent: return volatility and value-at-risk rise by 0.09 standard deviations, while expected shortfall and the lower partial second moment increase by 0.07. The size of the effects is economically comparable to what documented in prior research for other types of risk. For example, the impact of political risk on firm stock volatility documented in Hassan et al. (2019), Table IV is in the same order of magnitude.

In panels B through E of Figure IA1, we study the dynamic effect of SVs on firm risk variables.

[12] More details on the construction of the variables can be found in the data appendix.

We do so by running the following variation of equation (16):

$$log(Risk_{c,t+n}/Risk_{c,t-1}) = \alpha + \beta SV_{c,t} + \gamma X_{c,t} + \epsilon_{c,t+1} \tag{17}$$

in which we let n in the dependent variable vary from two quarters before the discovery of a SV to three quarters after. The graphs in Figure IA1 plot the coefficients on $SV_{c,t}$ for different horizons of the dependent variable. Across all panels, there is no impact of a SV on firm risk before its discovery. We observe a strong impact on risk variables one quarter after the discovery of a SV. The effect is weaker at longer horizons but does not revert, indicating that exposure to SVs leads to a persistent increase in firm risk. Overall, the results in this section suggest that the increased probability of cyberattacks following the discovery of SVs translates into a rise in stock market-based measures of firm risk, observable at the quarterly horizon.

If SVs increase firm risk, they may also impact discount rates. In particular, if exposure to a SV increases discount rates, consistent with an increase in firm risk, we should be able to detect an increase in expected stock returns after the discovery of a SV. To investigate this possibility, in line with a similar analysis in Kruttli, Tran, and Watugala (2025), we perform an event study of stock returns around the discovery of a SV. In Table 5 we report estimates from the following model:

$$CAR_{c,t+n\to t+m} = \alpha_{i,t} + \beta SV_{c,t} + \gamma X_{c,t} + \epsilon_{c,t+n\to t+m} \tag{18}$$

For each discovery of a SV (i.e., an event), the sample includes the set of treated firms, which are firms exposed to the SV, and a set of control firms that are never exposed to any vulnerability during our sample period.[13] $SV_{c,t}$ is an indicator variable identifying the set of firms exposed to each vulnerability at the moment of its discovery. $\alpha_{i,t}$ indicates a full set of Fama–French 48-industry $\times$ time (year-quarter) fixed effects. $CAR_{c,t+n\to t+m}$ is the cumulative abnormal return of firm c computed starting at date $t+n$ and ending at date $t+m$, where t is the date of the SV discovery. We compute abnormal returns using the Fama-French 5-factor model. We also let n and m vary to consider different event windows that include from 10 days after the event up

[13] As a result, $SV_{c,t}$ is a fixed firm-level characteristic, and we cannot include firm fixed effects in the regression.

to two months after: $n = 10$ and $m = 20$, $n = 10$ and $m = 30$, $n = 10$ and $m = 40$, $n = 10$ and $m = 60$. Under the scenario in which SVs impact discount rates, we should obtain positive estimates of β when focusing on these event windows.

The columns of Table 5 display positive and statistically significant point estimates of β. In the ten days of the window that uses $n = 10$ and $m = 20$, exposed firms experience returns 0.02 standard deviations larger than the unexposed firms, or a difference of 0.138 percentage points. The effect grows in statistical significance and economic magnitude as we enlarge the event window. When focusing on the window that ends two months after the SV discovery, we observe that exposed firms experience expected returns 0.04 standard deviations larger than the unexposed firms, or a difference of 0.714 percentage points. This pattern of expected returns is consistent with market participants pricing in the consequences of SVs, and strengthen our conclusion that SVs increase firm risk.

5.1.3 Falsification Tests and Robustness

Our interpretation of the results is that exposure to SVs causes an increase in the likelihood of a cyberattack and in firm risk. To pose a concern for a causal interpretation, any unobserved factor needs to account simultaneously for the evidence on cyberattack probability and firm risk, as well as the emergence of a SV in a product used by the firm. One such possibility goes as follows. Firms with low awareness of cybersecurity risks, or weak internal controls, may be more prone to cyberattacks and therefore exhibit higher risk. If these same firms also tend to choose software from producers with similarly weak controls, their software might contain more vulnerabilities. In that case, the true cause of the heightened cyberattack probability and firm risk would be the unobserved firm-level factors rather than the SVs, but the matching between firms and software producers would explain the coefficients we observe. In this section we provide several pieces of evidence that challenge this alternative interpretation.

We begin by noting that the absence of a significant coefficient in the last column of Table 3 already speaks against the existence of unobserved factors driving our results. A firm with poor internal cybersecurity controls would invite any type of attack, not exclusively attacks caused by

a SV. Therefore, under the alternative interpretation described above, we would expect also the last column of Table 3 to display a positive and significant coefficient. The absence of an effect stands in stark contrast to this.

In the first tests of this section we exploit information on the severity of a vulnerability. We decompose our main independent variable into an indicator variable that identifies Major Vulnerabilities and one that instead identifies Minor vulnerabilities. Major (Minor) vulnerabilities are defined as those vulnerabilities with a Common Vulnerability Scoring System (CVSS) above or equal (below) 7. A higher CVSS is assigned to a vulnerability that is more likely to be successfully exploited and that can cause a greater damage to the company. Such distinction is useful to address alternative explanations based on unobserved factors. The underlying rationale is that a vulnerability, regardless of its severity, could still be a signal of poor internal cybersecurity controls on the part of the software producer. Therefore, such a vulnerability could still affect firms with weak internal cybersecurity controls under the alternative explanation based on the matching between similar firms and software producers. As a result, if unobserved factors were behind our results, we should observe our baseline results even when focusing on minor vulnerabilities. In contrast to this, Tables IA4 and IA5 show that our baseline results only hold when we focus on major vulnerabilities. Restricting the analysis to minor vulnerabilities leads to no impact on the probability of cyberattacks or on measures of firm risk.

In the second test of this section, we adopt a different strategy and argue that, if unobserved factors were responsible for the customer-supplier matching and, ultimately, for our results, then the timing of a vulnerability discovery would not matter. The firm-supplier pair would have a higher number of cyber attacks regardless of the discovery of a vulnerability. To test for this, we adopt the block permutation procedure of Chetty, Looney, and Kroft (2009). In each iteration, the date of the SV variable is re-assigned to each firm by randomly selecting one of the dates in our sample period with replacement. Equation (14) and (16) are then estimated on the falsified data for each of the dependent variables in Tables 3 and 4.

Panel A in Figure IA2 reports the empirical cumulative distribution function (cdf) generated from running the regression model of Column (1) of Table 3, Panel A with 1,000 random iterations

of this procedure and capturing the placebo coefficient estimate. The vertical dotted line indicates the position of the actual coefficient of Column (1) of Table 3, Panel A. We also report the implied p-value when the actual coefficient is placed in the context of cdf. Our coefficient has a p-value of 0.000, indicating that the timing of the vulnerability is essential to determine the effect on the number of cyberattacks that we document. A similar conclusion can be drawn from the other plots (Panels B to F) of Figure IA2, which are generated from the regression models of Table 4: the timing of a vulnerability discovery is crucial to obtain our observed impact of SVs on firm risk. We conclude from the falsification tests that unobserved factors are unlikely to drive the link between SVs, future cyberattacks, and risk variables.

Finally, we address concerns of measurement error in our definition of supplier-customer links. While we believe that Factset Revere provides the best available information to identify software suppliers customers, it is still possible that the database misses existing supply chain links. If this problem exists in our data, the impact on our main results is arguably most severe for software suppliers affected by a large number of SVs, as they account for a large portion of the variation in our main independent variable. To address this concern, we construct alternative samples that exclude customers of the top three software suppliers by number of vulnerabilities: Microsoft, Adobe, Apple.[14] We then repeat the estimation of the regression models in Tables 3 and 4 using these alternative samples. Results, reported in Tables IA7 and IA8, shows that our main results are robust to excluding any of the top three suppliers in our data.

5.2 Insights on the Economic Mechanism

Having established the strong impact of SVs on firms' risk, we now investigate the economic mechanism behind our findings. We start by exploring which type of firms are most exposed to the harmful consequences of SVs. This exercise can provide insights on how to design cyber risk mitigation policies. Next, we investigate how firms change their policies in reaction to SVs exposure. This analysis allows us to shed light on the real effects of SVs and how firms try to protect themselves against cybersecurity risk.

[14] See Table IA2 for the list of software companies and the number of vulnerabilities in their products.

5.2.1 The Heterogeneous Impact of SVs

We explore which firms are more exposed to the adverse effects of SVs. In the notation of the theoretical framework of Section 3, the goal of this section is to single out firms with larger values of γ_c from equation (1). We do so by re-estimating equations (14) and (16) for different subsamples based on relevant firm characteristics. We split the sample based on proxies of ex-ante risk of hacking attacks, quality of cybersecurity and degree of expertise in the software used.

Our first split is inspired by recent literature, which suggests that some firms face higher risk of cyber incidents. For example, Florackis et al. (2022) show that such risk is observable, measurable, and reflected in firms' "Risk Factors" section in 10-K filings. A similar argument is made by Jamilov, Rey, and Tahoun (2025) using earning calls. Building on this fact, we posit that the effects of a SV should be greater for firms that already face higher risk of cyberattacks at the moment of the vulnerability discovery. To test this conjecture, we employ two proxies for ex-ante exposure to hacking incidents. The first, and arguably more direct, counts the number of cyberattacks a firm has suffered over the past 5 years. The second, inspired by Florackis et al. (2022), counts the number of times a firm uses sentences related to cybersecurity risk in its 10-K. Both variables are characterized by strong differences across industries. For example, the Fama-French 48 industries "Computers" and "Electronic Equipment" consistently display higher values of both variables. To avoid capturing a simple industry effect, we first subtract from each variable its mean within each Fama-French 48-industry and date pair, and then use the median of the demeaned variable to divide firms into subsamples.

Columns (1) through (4) of Table 6 show that both proxies yield similar results: the impact of a SV on the probability of cyberattacks and firm risk is greater for firms that already face higher cybersecurity risk when the SV emerges. In terms of economic magnitude, coefficients show that for firms with higher ex-ante risk of cyberattacks the impact of a SV emergence is between 1.5 and 3.1 times the impact for firms with lower ex-ante risk.

Second, we explore heterogeneity related to the extent to which firms are protected against the occurrence of a cyberattack. When a new vulnerability emerges, firms that have appropriate cybersecurity controls in place are likely better able to mitigate its adverse consequences. While

we do not observe a firm's internal security policies, our supply-chain relationships data offers a valid alternative. We classify a firm as having a stronger cybersecurity posture if the firm employs the services of a cybersecurity specialist. In columns (5) and (6) of Table 6 we reports the results for the two subsamples of firms with or without relationships with cybersecurity firms. Consistent with our conjecture, and with the value of a solid cybersecurity protection, we observe that the adverse effects of SVs only manifest in the sample of firms that do not have a relationship with a cybersecurity firm.

The final split is inspired by an important reason why companies fail to protect themselves against SVs. As outlined in Section 2, implementing the prescribed solution to address a vulnerability requires specialized knowledge of the software. The internal IT departments of some firms might not possess this knowledge, especially with today's complex IT infrastructure. Our final sorting variable aims to identify companies for which this issue is likely to be more severe by exploiting information in our supply-chain relationships data. Specifically, we conjecture that a firm that has a longer relationship with its suppliers is more likely to have developed specialized knowledge of its suppliers' software than a company that has shorter relationships. In our data, we separate firms with below or above median average supplier relationship length. In line with our intuition, columns (7) and (8) of Table 6 show that the effects of SVs are between 1.6 and 1.9 larger for firms in the first group, that is, firms characterized by lower software-specific expertise.

Taken together, our cross-sectional analysis provides two economic insights. First, the impact of SVs is particularly pronounced for companies that are ex-ante more exposed to hacking attacks. This result also reinforces the notion that SVs have an impact on firms because they increase cyber risk, rather than because of other unobserved factors. Second, the negative effect of SVs can be mitigated through appropriate monitoring (e.g., cybersecurity controls or specialized software knowledge). This evidence suggests that an important driver of our results are frictions preventing firms from properly assessing and acting on the increased cybersecurity risk.

5.2.2 Real Effects of SVs

Results so far show that firms exposed to SVs experience higher probability of hacking incidents and increases in their risk. Two natural questions that arise in light of this evidence are whether and how these firms modify their policies to react to a SV's emergence. Answering these questions can broaden our understanding of the real effects of SVs.

Both theoretical and empirical literature suggest that an increase in any kind of risk tends to decrease firm-level investments (see, e.g., Bloom, Bond, and Van Reenen (2007), Bloom (2009), Hassan et al. (2019)). In Column (1) and (2) of Table 7 we test this prediction. We reestimate equation (16) using as dependent variables: the capital investment rate $\mathrm{I}_{t+1}/\mathrm{K}_t$, measured quarterly and calculated recursively as detailed in Stein and Stone (2013); the growth in capital expenditures. In line with previous literature, the coefficient indicates that exposure to an additional SV decreases firm investments by 0.06 standard deviations; and CapEx growth by 0.13 standard deviations.

In the last two columns of Table 7 we focus on variables more directly related to cybersecurity concerns. With the first variable we aim to investigate whether firms hire cybersecurity specialists. This is a logical starting point given the evidence of section 5.2.1 showing that these specialized companies offer effective protection against cyberattacks. Thus, in Column (3) we use as dependent variable an indicator that takes value of 1 if in quarter $t+1$ customer firm c begins a new relationship with a cybersecurity firm. The coefficient on $SV_{c,t}$ indicates that exposure to a SV increase the likelihood of hiring a cybersecurity specialist by 0.22 standard deviations.

The costs to firms of a cyberattack are higher when the attack involves the theft of sensitive customer data. This is because the loss of sensitive data can damage the company's reputation and trigger costly lawsuits. Therefore, companies concerned with such costs could try to reduce the risk of incurring legal and reputational damages from a data security breach. To explore this possibility, in Column (4) we use as dependent variable MSCI Privacy & Data Security Score. Higher values of this score, which ranges from 1 to 10, identifies companies "*with comprehensive privacy policies and data security management systems*". The coefficient on $SV_{c,t}$ indicates that firms exposed to a SV improve their score by 0.52 standard deviations.

Overall, our results indicate that firms react to SVs by decreasing their investments, increasing their protection against attacks, and reducing the costs of a successful attack. The increase in protection is consistent with the evidence in Ademović, Ioannidou, and Mosk (2025), who find that, following a cyberattack, companies increase cybersecurity hiring and adoption of advanced technologies.

6 Software Industry Structure and Cyber Risk

In this section we study the aggregate impact of software vulnerabilities, and the role that size and concentration of the software industry play in determining its magnitude. As in the theoretical framework of Section 3, we focus on two levels of aggregation: across all customers of a software company and at the economy-level.

6.1 Software Company-Level Analysis

We start by studying whether the consequences of a SV for the customers of software suppliers align with the prediction of the theoretical framework developed in Section 3. According to equation (7), the emergence of a SV should be associated to a larger number of cyberattacks among the customers of a software company with a larger customer base. Equation (13) instead shows that the size of a vulnerability impact on risk variables depends on two factors: i) the software supplier's market share; and ii) the size of the software sector.

We bring these predictions to the data using a supplier-level panel data. We begin by studying the impact of vulnerabilities on the number of cyberattacks among the software companies customers. We start by estimating the model:

$$\frac{Cyberattacks_{s,t+1}}{N_{t+1}} = \alpha + \beta_1 SV_{s,t} + \beta_2 Size_{s,t} + \beta_3 SV_{s,t} \times Size_{s,t} + \gamma X_{s,t} + \epsilon_{s,t+1} \quad (19)$$

where the unit of observation is a supplier s in quarter t. The dependent variables are defined as the number of cybersecurity incidents of any type (column (1)), the number of cybersecurity incidents of any type occurred after 2010 (column (2)), related to vulnerabilities (column (3)), or

due to causes different from vulnerabilities (column (4)) that hit customers of software supplier s in quarter $t+1$, scaled by the total number of firms in our sample at time $t+1$. $SV_{s,t}$ is an indicator variable that takes a value of 1 when a product of supplier s is affected by a SV in quarter t. For a given supplier s, $Size_{s,t}$ is defined as supplier s's sales normalized by total sales across firms in CRSP/Compustat data in quarter t. $Size_{s,t}$ is the empirical analog of the ratio $\frac{Z_{s,t}}{N}$ in equation (7), and is intended to capture the size of the software company relative to all firms in the economy. The set of controls $X_{s,t}$ includes market capitalization, book-to-market, ROA, previous 12-month return, leverage, and the number of cybersecurity incidents that the software supplier s customers experienced over the previous year. α indicates different sets of fixed effects, including year-quarter and software company fixed effects. Standard errors are clustered at the supplier level.[15]

Table 8 presents the results. The coefficient of interest is β_3, the interaction term between $SV_{s,t}$ and $Size_{s,t}$. In Column (1), where we analyze the probability of cyberattacks of any type, β_3 is positive and significant. The magnitude indicates that a one standard deviation increase in $Size_{s,t}$ amplifies the effect of a vulnerability discovery on the probability that customers of supplier s are victim of cyberattacks by 0.07 standard deviations. This effect is entirely driven by cyberattacks originating from software vulnerabilities, as displayed in column (3). In contrast, the interaction term is not statistically significant when we examine attacks unrelated to vulnerabilities.

Next, we investigate the impact of vulnerabilities on customer risk. We do so by estimating a variant of equation (19) in two separate subsamples. The first subsample includes all dates when the size of the software sector is above its time-series median. The second subsample focuses on periods when the size of the software sector is below its time-series median. We compute the software sector's size as total sales of software companies in our data normalized by total sales of all firms in CRSP/Compustat data in quarter t. This is the empirical analog of the fraction $\frac{T_{S,t}}{N}$ that appears in equation (13).

[15] In Appendix Table IA6 we repeat the baseline analyses of Tables 3 and 4 in the supplier-level panel data and show that we obtain qualitatively very similar conclusions.

In each subsample we estimate the model:

$$\log\left(\frac{Risk_{s,t+1}}{Risk_{s,t-1}}\right) = \alpha + \beta_1 SV_{s,t} + \beta_2 Market\ Share_{s,t} + \beta_3 SV_{s,t} \times Market\ Share_{s,t} + \gamma X_{s,t} + \epsilon_{s,t+1} \quad (20)$$

where the unit of observation is a supplier s in quarter t. The dependent variables are the log change in the equal-weighted averages of return volatility, value-at-risk (VaR), expected shortfall, and the second-order LPM of software supplier s' customers in quarter $t+1$. $SV_{s,t}$ is an indicator variable that takes a value of 1 when a product of supplier s is affected by a SV in quarter t. For a given supplier s, $Market\ Share_{s,t}$ is defined as supplier s's sales divided by total sales of the software sector in quarter t. $Market\ Share_{s,t}$ is meant to capture the role of the ratio $\frac{Z_{s,t}}{T_{S,t}}$ in equation (13).[16] The set of controls $X_{s,t}$ includes market capitalization, book-to-market, ROA, previous 12-month return, leverage, and the number of cybersecurity incidents that the software supplier s customers experienced over the previous year. α indicates different sets of fixed effects, including year-quarter and software company fixed effects. Standard errors are clustered at the supplier level.

Across all four proxies of risk, Table 9 reports a consistent pattern. In Panel A, where we focus on periods when the software sector is comparatively larger, coefficient β_3 is positive and significant. This means that the larger the market share of the software company, the greater the impact that an SV discovery has on firm risk. In contrast, point estimates in Panel B, where we focus on periods when the software sector is smaller, are not statistically significant or display the wrong sign.

6.2 Aggregate Implications

In this section we test the economy-level predictions generated by the theoretical framework of Section 3. Mirroring the software company-level analysis, we expect the number of cyberattacks in the economy to be larger when the software sector S is larger, i.e, when usage of software is more

[16] To ease the economic interpretation of our coefficients, we do not use the squared $\frac{Z_{S,t}}{T_t}$ in our empirical tests, but our results are qualitatively very similar if we square our *Market Share* variable.

widespread in the economy. Similarly, equation (11) shows that an additional vulnerability leads to higher market risk when both the size ($\frac{T_{S,t}}{N}$) and the concentration ($HHI_{S,t}$) of the software sector are larger.

We bring the first prediction to the data in our sample by running:

$$\frac{Cyberattacks_{t+1}}{N_{t+1}} = \alpha + \beta_1 Size_{S,t} + \beta_2 SV_{S,t} + \beta_3 Size_{S,t} \times SV_{S,t} + \epsilon_{t+1} \tag{21}$$

where $Cyberattacks_{t+1}$ is either: the number of cybersecurity incidents of any type (column (1)), the number of cybersecurity incidents of any type occurred starting in 2010 (column (2)), related to vulnerabilities (column (3)), or due to causes different from vulnerabilities (column (4)) that hit firms in our sample in quarter $t+1$. We scale all these variables by the number of firms in our sample at time $t+1$. $Size_{S,t}$, is defined as the total sales across all software companies in our data normalized by total sales across all firms in CRSP/Compustat data in quarter t. This represents the empirical counterpart of the fraction $\frac{T_{S,t}}{N}$ in equation (5), and is meant to capture the size of the software sector. $SV_{S,t}$ reflects the expected number of vulnerabilities hitting software products in the economy, which in the model appears as the parameter Λ. We construct this variable as the number of vulnerabilities emerging in quarter t, divided by the number of software companies in our sample in quarter t. Standard errors are heteroskedasticity-robust.

Results in Table 10 are consistent with the model predictions. Coefficients on the interaction term $Size_{S,t} \times SV_{S,t}$ are positive and significant in all columns except for the last one, which focuses attacks due to causes different from software vulnerabilities. The largest economic magnitude is achieved in Column (3), which studies attacks related to vulnerabilities, and indicates that one-sigma increases in $Size_{S,t}$ amplifies the impact of vulnerabilities by 0.3 standard deviations.

Next, we study the impact of SVs on aggregate stock market volatility. With a similar approach to that used in Table 9, we estimate a variant of equation (21) in two separate subsamples. In the first two columns of Table 11, we include all dates in which the size of the software sector is above its time-series median. The last two columns focus on periods when the size of the software sector is below its time-series median. We compute the size of the software sector as the total sales of software companies in our data normalized by total sales of firms in CRSP/Compustat data in

quarter t. This variable proxies for the ratio $\frac{T_{S,t}}{N}$ that appears in equation (11).

In each subsample we estimate the model:

$$log\left(\frac{Vol_{t+1}}{Vol_t}\right) = \alpha + \beta_1 HHI_{S,t} + \beta_2 SV_{S,t} + \beta_3 HHI_{S,t} \times SV_{S,t} + \epsilon_{t+1} \tag{22}$$

where the dependent variable is the log change in stock market volatility from quarter t to quarter $t+1$. We use two proxies of market volatility: the quarterly standard deviation of the CRSP value-weighted index, computed using the daily returns in a quarter; the quarterly average VIX index. We measure $HHI_{S,t}$ as the Herfindahl–Hirschman index of the software sector based on the sales of the software companies in our sample. SV_t is the average number of vulnerabilities per software companies in each quarter t, and is meant to capture the parameter Λ. We standardize all variables for ease of interpretation.

The results in Table 11 align with the predictions of our theoretical framework. The point estimates on the interaction term $HHI_{S,t} \times SV_{S,t}$ are positive and significant only in the first two columns, which cover periods when the software sector is larger. The coefficients on β_3 show that a one–standard deviation increase in $HHI_{S,t}$, when $SV_{S,t}$ is at its mean, raises the volatility of the CRSP value-weighted (VIX) index by 13% (8%), which correspond to 28% (31%) of the respective standard deviation. In the last two columns of the table, which cover periods when the sector is smaller, the interaction shows no significant effect.

7 Conclusion

This paper shows that the expansion and concentration of the software industry are significant factors contributing to the increase in cybersecurity risk in the economy. The proliferation of software products leads to a greater number of potential targets for cyberattacks, as software vulnerabilities affecting software programs represent potential entry points for malicious actors. Consequently, the expansion of the software industry amplifies the overall exposure of the corporate sector to cyber risk. At the same time, the concentration of the software industry implies that the same software vulnerability affects a large fraction of the market simultaneously and generates

significant correlation in the exposure to cyber risk. A direct consequence of this is that software vulnerabilities have a measurable impact on stock market volatility when the software sector is large and concentrated.

This paper contributes to the growing literature on how the diffusion of new technologies can create novel sources of risk for firms and the economy. In that respect, our findings on the role of software industry structure speak directly to the recent debate on whether software companies are a systemic source of cyber risk (Welburn, 2024; Baker and Lee, 2026). The paper also sheds light on how cybersecurity risk originates and spreads, even before an actual attack occurs. In doing so, it extends and complements recent studies on the effects of cyberattacks on firms and financial institutions. Our findings are also important for policy institutions around the world that are trying to measure exposure to cyber risk in the economy. Incorporating information on SVs in such measures could go a long way in detecting the potential for cyber threats early.

Finally, several avenues for future research emerge from our analysis. First, our results indicate that the negative impact of SVs can be mitigated when companies are more knowledgeable about the software used and/or hire the services of cybersecurity firms. The impact of SVs on firms emerging from our results suggests that there are frictions preventing companies from adopting those solutions. More research is needed to shed light on the nature and implications of these frictions. Second, the exponential growth of artificial intelligence (AI) in recent years has put a significant strain on the software sector due to concerns that AI can replace software programs (Pitcher and Martinez, 2026). More work is needed to understand whether the changes to the software sector fueled by AI are making it more or less resilient to cyber risk (McMillan, 2026).

Lastly, our paper opens interesting directions for research on intangible assets, of which software is one of the most prominent examples. A large body of research has been devoted to the measurement of intangible assets, as well as their effect on firm policies and economic output (see Crouzet et al. (2022) for a review). Our analysis suggests that intangible assets could provide a gateway for malicious actors to damage a company's business. Incorporating this risk into standard models of intangible capital to study its equilibrium implications is a promising avenue for future work.

References

Acemoglu, Daron, and Pascual Restrepo, 2020, Robots and jobs: Evidence from us labor markets, *Journal of Political Economy* 128, 2188–2244.

Adelino, Manuel, Miguel A Ferreira, Mariassunta Giannetti, and Pedro Pires, 2023, Trade credit and the transmission of unconventional monetary policy, *The Review of Financial Studies* 36, 775–813.

Ademović, Emina, Vasso Ioannidou, and Thomas C. Mosk, 2025, Stung into action? cyber risk management after a breach, Working Paper 25869, National Bureau of Economic Research.

Akerman, Anders, Ingvil Gaarder, and Magne Mogstad, 2015, The Skill Complementarity of Broadband Internet *, *The Quarterly Journal of Economics* 130, 1781–1824.

August, Terrence, Marius Florin Niculescu, and Hyoduk Shin, 2014, Cloud implications on software network structure and security risks, *Information Systems Research* 25, 489–510.

August, Terrence, Daehoon Noh, Noam Shamir, and Hyoduk Shin, 2022, Cyberattacks, operational disruption and investment in resilience measures, *Available at SSRN 4032257* .

Autor, David H, Frank Levy, and Richard J Murnane, 2003, Skill demand, inequality, and computerization: Connecting the dots, *Technology, growth, and the labor market* 107–129.

Baker, Steven D., and Michael Junho Lee, 2026, Systemic cyber risk, Staff Report 1186, Federal Reserve Bank of New York.

Barrot, Jean-Noël, and Julien Sauvagnat, 2016, Input Specificity and the Propagation of Idiosyncratic Shocks in Production Networks *, *The Quarterly Journal of Economics* 131, 1543–1592.

Bloom, Nicholas, 2009, The impact of uncertainty shocks, *Econometrica* 77, 623–685.

Bloom, Nicholas, Tarek Alexander Hassan, Aakash Kalyani, Josh Lerner, and Ahmed Tahoun, 2021, The diffusion of new technologies, Working Paper 28999, National Bureau of Economic Research.

Bloom, Nick, Stephen Bond, and John Van Reenen, 2007, Uncertainty and investment dynamics, *Review of Economic Studies* 74, 391–415.

Carvalho, Vasco M, Makoto Nirei, Yukiko U Saito, and Alireza Tahbaz-Salehi, 2021, Supply chain disruptions: Evidence from the great east japan earthquake, *The Quarterly Journal of Economics* 136, 1255–1321.

Chetty, Raj, Adam Looney, and Kory Kroft, 2009, Salience and taxation: Theory and evidence, *American economic review* 99, 1145–1177.

Crosignani, Matteo, Marco Macchiavelli, and André F. Silva, 2023, Pirates without borders: The propagation of cyberattacks through firms' supply chains, *Journal of Financial Economics* 147, 432–448.

Crouzet, Nicolas, and Janice Eberly, 2023, Rents and intangible capital: A q+ framework, *The Journal of Finance* 78, 1873–1916.

Crouzet, Nicolas, and Janice C Eberly, 2019, Understanding weak capital investment: the role of market concentration and intangibles, Working Paper 25869, National Bureau of Economic Research.

Crouzet, Nicolas, Janice C. Eberly, Andrea L. Eisfeldt, and Dimitris Papanikolaou, 2022, The economics of intangible capital, *Journal of Economic Perspectives* 36, 29–52.

Curti, Filippo, Ivan Ivanov, Marco Macchiavelli, and Tom Zimmemrmann, 2023, City hall has been hacked! the financial costs of lax cybersecurity.

Duffie, Darrell, Andreas Eckner, Guillaume Horel, and Leandro Saita, 2009, Frailty correlated default, *The Journal of Finance* 64, 2089–2123.

Duffie, Darrell, and Joshua Younger, 2019, Cyber runs.

Eisenbach, Thomas M., Anna Kovner, and Michael Junho Lee, 2022, Cyber risk and the u.s. financial system: A pre-mortem analysis, *Journal of Financial Economics* 145, 802–826.

Eisenbach, Thomas M., Anna Kovner, and Michael Junho Lee, 2023, When it rains, it pours: Cyber risk and financial conditions.

Florackis, Chris, Christodoulos Louca, Roni Michaely, and Michael Weber, 2022, Cybersecurity Risk, *The Review of Financial Studies* 36, 351–407.

Gabaix, Xavier, 2011, The granular origins of aggregate fluctuations, *Econometrica* 79, 733–772.

Gómez-Cram, Roberto, and Alastair Lawrence, 2025, The value of software, *American Economic Review* 115, 3514–58.

Hassan, Tarek A, Stephan Hollander, Laurence van Lent, and Ahmed Tahoun, 2019, Firm-Level Political Risk: Measurement and Effects*, *The Quarterly Journal of Economics* 134, 2135–2202.

Hertzel, Michael G, Zhi Li, Micah S Officer, and Kimberly J Rodgers, 2008, Inter-firm linkages and the wealth effects of financial distress along the supply chain, *Journal of Financial Economics* 87, 374–387.

Jamilov, Rustam, Hélène Rey, and Ahmed Tahoun, 2025, The anatomy of cyber risk, Working Paper 28906, National Bureau of Economic Research.

Kogan, Leonid, Dimitris Papanikolaou, Amit Seru, and Noah Stoffman, 2017, Technological Innovation, Resource Allocation, and Growth*, *The Quarterly Journal of Economics* 132, 665–712.

Kotidis, Antonis, and Stacey L. Schreft, 2025, The propagation of cyberattacks through the financial system: Evidence from an actual event, *The Journal of Finance* 80, 3313–3358.

Kruttli, Mathias S, Brigitte Roth Tran, and Sumudu W Watugala, 2025, Pricing poseidon: Extreme weather uncertainty and firm return dynamics, *The Journal of Finance* 80, 783–832.

McMillan, Robert, 2026, Anthropic set to preview powerful mythos model to ward off ai cyberthreats, *The Wall Street Journal* .

Pitcher, Jack, and Javier Martinez, 2026, The $1.6 trillion meltdown that swept through software stocks, *The Wall Street Journal* .

Pástor, Ľuboš, and Pietro Veronesi, 2009, Technological revolutions and stock prices, *American Economic Review* 99, 1451–83.

Software.org, 2021, Software: Supporting US Through COVID https://software.org/reports/software-supporting-us-through-covid-2021/.

Stein, Luke CD, and Elizabeth Stone, 2013, The effect of uncertainty on investment, hiring, and r&d: Causal evidence from equity options, *Working Paper (SSRN 1649108)* .

Ward, Colin, 2020, Is the it revolution over? an asset pricing view, *Journal of Monetary Economics* 114, 283–316.

Welburn, Jonathan, 2024, Crowdstrike is too big to fail, *Wall Street Journal* https://www.wsj.com/articles/crowdstrike-is-too-big-to-fail-77d20f1d.

Table 1: Summary Statistics

This table presents mean, standard deviation, 10th percentile, median, 90th percentile and number of observations for the main customer-level variables used in the paper. A complete list of definitions is provided in the Data appendix. The sample period runs from 2006 to 2024.

	Mean	SD	P10	P50	P90	Observations	Unit
Dependent Variables							
All Attacks$_{c,t}$	0.01	0.59	0.00	0.00	0.00	98,885	Integer
Return Volatility$_{c,t}$	0.81	45.58	-52.22	-0.45	55.21	89,199	%
Value-at-Risk$_{c,t}$	0.22	49.53	-59.38	-0.39	61.08	89,199	%
Expected Shortfall$_{c,t}$	0.42	52.86	-64.19	-0.23	65.87	89,199	%
Lower Partial SD	0.51	57.20	-69.04	-0.19	71.61	89,199	%
Independent Variables							
SV$_{c,t}$	0.17	0.38	0.00	0.00	1.00	98,885	Integer
Size$_{c,t}$	7.84	2.20	4.80	7.98	10.63	98,885	$ B
Book-to-Market$_{c,t}$	-0.80	0.91	-1.97	-0.71	0.24	98,885	Integer
Profitability$_{c,t}$	0.00	0.04	-0.03	0.01	0.03	98,885	%
Leverage$_{c,t}$	0.24	0.20	0.00	0.21	0.52	98,885	%
Past 12-month Return$_{c,t}$	0.10	0.48	-0.44	0.06	0.61	98,885	%

Table 2: Firm-Level Determinants of SVs

This table studies firm-level determinants of SVs. The dependent variable is an indicator that takes value 1 if any of customer c's software suppliers has a vulnerability in one of its software products disclosed in quarter t. All right-hand-side variables are measured with one quarter lag. A complete list of definitions for these variables is provided in the Data appendix. t-statistics based on standard errors clustered by customer are shown in parentheses. *, **, and *** denote significance at the 10%, 5%, and 1% levels, respectively. The sample period runs from 2006 to 2024.

	$SV_{c,t}$			
	(1)	(2)	(3)	(4)
$Size_{c,t-1}$	-0.042***	-0.008	-0.006	-0.006
	(-8.26)	(-0.63)	(-0.51)	(-0.51)
$Book\text{-}to\text{-}Market_{c,t-1}$	-0.027***	-0.001	-0.002	-0.002
	(-6.46)	(-0.16)	(-0.39)	(-0.39)
$Profitability_{c,t-1}$	-0.004*	-0.001	-0.001	-0.001
	(-1.80)	(-0.98)	(-0.91)	(-0.91)
$Leverage_{c,t-1}$	-0.020***	0.008*	0.003	0.003
	(-4.83)	(1.69)	(0.56)	(0.56)
Past 12-month $Return_{c,t-1}$	-0.001	0.001	0.000	0.000
	(-0.64)	(0.50)	(0.08)	(0.08)
Past $CyberAttacks_{c,t-1}$				0.000
				(0.10)
Time FE	Yes	Yes		
Customer FE		Yes	Yes	Yes
Industry x Time FE			Yes	Yes
Observations	98,885	98,885	98,885	98,885
Adjusted r^2	0.110	0.510	0.531	0.531

Table 3: Vulnerabilities and Cybersecurity Incidents

This table studies the relation between the probability of cybersecurity attacks and exposure to SVs. We report estimates of the model:

$$P(\text{CyberAttack}_{c,t+1} = 1 \mid \text{SV}_{c,t}, X_{c,t}, \alpha_{i,t}) = \Lambda(\alpha_{i,t} + \beta \text{SV}_{c,t} + X'_{c,t}\gamma)$$

the dependent variables are the number of cybersecurity incidents of any type (columns (1)), the number of cybersecurity incidents of any type occurring after 2010 (columns (2)), those related to vulnerabilities (columns (3)), or those due to causes different from vulnerabilities (columns (4)) that hit the software customer c in quarter $t+1$. In all columns, the main independent variable is an indicator with value 1 if customer c is exposed to a vulnerability through one of its software suppliers in quarter t. Controls include market capitalization, book-to-market, ROA, previous 12-month return, and leverage. We also include the number of cybersecurity incidents that the software customer c has experienced over the previous year. $\alpha_{i,t}$ indicates Fama-French 48-industry $\times$ time fixed effects. t-statistics based on standard errors clustered by customer are shown in parentheses. *, **, and *** denote significance at the 10%, 5%, and 1% levels, respectively. A complete list of definitions for these variables is provided in the Data Appendix.

	All Attacks$_{c,t+1}$ (1)	Attacks > 2010$_{c,t+1}$ (2)	Vulnerability Attacks$_{c,t+1}$ (3)	Other Attacks$_{c,t+1}$ (4)
SV$_{c,t}$	3.273***	3.540***	5.017***	1.331
	(5.25)	(5.39)	(5.62)	(0.75)
Customer Controls$_{c,t}$	Yes	Yes	Yes	Yes
Industry x Time FE	Yes	Yes	Yes	Yes
Observations	98,885	76,356	76,356	76,356
Pseudo r^2	0.159	0.163	0.168	0.189

Table 4: Vulnerabilities and Firm Risk

This table studies the relation between firm risk and exposure to SVs. We report estimates of the model:

$$log\left(\frac{Risk_{c,t+1}}{Risk_{c,t-1}}\right) = \alpha + \beta_1 SV_{c,t} + \gamma X_{c,t} + \epsilon_{c,t+1}$$

the dependent variables are the log change in return volatility, value-at-risk (VaR), expected shortfall, and the second-order LPM of software customer c between quarter $t-1$ and quarter $t+1$. The main independent variable is an indicator with value 1 if customer c is exposed to a vulnerability through one of its software suppliers in quarter t. Controls include market capitalization, book-to-market, ROA, previous 12-month return, and leverage. We also include the number of cybersecurity incidents that the software customer c has experienced over the previous year. α indicates customer and Fama–French 48-industry $\times$ time (year-quarter) fixed effects. t-statistics based on standard errors clustered by customer are shown in parentheses. *, **, and *** denote significance at the 10%, 5%, and 1% levels, respectively. A complete list of definitions for these variables is provided in the Data Appendix.

	Return Vol.$_{c,t+1}$ (1)	Value-at-Risk$_{c,t+1}$ (2)	Exp. Shortfall$_{c,t+1}$ (3)	Lower Partial SD$_{c,t+1}$ (4)
SV$_{c,t}$	0.087***	0.089***	0.074***	0.072***
	(7.47)	(7.86)	(6.35)	(6.15)
Customer Controls$_{c,t}$	Yes	Yes	Yes	Yes
Customer FE	Yes	Yes	Yes	Yes
Industry x Time FE	Yes	Yes	Yes	Yes
Observations	89,199	89,199	89,199	89,199
Adjusted r^2	0.098	0.111	0.086	0.057

Table 5: Vulnerabilities and Expected Returns

This table studies firms' stock returns around the discovery of SVs. The table reports estimates of the model:

$$CAR_{c,t+n\to t+m} = \alpha + \beta SV_{c,t} + \gamma X_{c,t} + \epsilon_{c,t+n\to t+m}$$

the dependent variables are the cumulative abnormal returns computed using the FF5-factor model and four different windows (measured in number of days after t): $n = 10$ and $m = 20$, $n = 10$ and $m = 30$, $n = 10$ and $m = 40$, $n = 10$ and $m = 60$. To calculate each CAR, we utilize an estimation window of 220 trading days (-251, -31), with day 0 being the date of the vulnerability discovery. A minimum of 63 non-missing returns is required within this estimation window. α indicates Fama–French 48-industry $\times$ time (year-quarter) fixed effects. t-statistics are based on standard errors clustered by vulnerability discovery event and are shown in parentheses. *, **, and *** denote significance at the 10%, 5%, and 1% levels, respectively. A complete list of definitions for these variables is provided in the Data Appendix.

	$CAR_{c,10\to 20}$ (1)	$CAR_{c,10\to 30}$ (2)	$CAR_{c,10\to 40}$ (3)	$CAR_{c,10\to 60}$ (4)
SV_c	0.138*	0.316***	0.330***	0.714***
	(1.96)	(2.90)	(2.63)	(3.35)
Customer Controls$_{c,t}$	Yes	Yes	Yes	Yes
Industry x Time FE	Yes	Yes	Yes	Yes
Observations	154,135	154,135	154,135	154,135
Adjusted r^2	0.012	0.023	0.029	0.041

Table 6: The Heterogeneous Impact of Software Vulnerabilities

This table studies the heterogeneity in the relation between the probability of cybersecurity attacks, risk variables and exposure to SVs. In this table we repeat the analyses of Tables 3 and 4 for different subsamples of firms. The first four columns focus on sample splits based on proxies of ex-ante firm-level cyber risk. In columns (1) and (2) we report estimates for two sub-samples based on below and above median number of past cyberattacks, respectively. In columns (3) and (4) we report estimates for two sub-samples based on below and above median number of sentences mentioning cyber risks in the 10-K. In columns (5) and (6) we report estimates for two sub-samples based on whether firms have relationships with cybersecurity firms or not. In columns (7) and (8) we report estimates for companies with low and high software expertise. We define a company with low (high) software expertise if it has a below- (above-) median relationship length with its suppliers. We run a regression of each sorting variable on Fama-French 48-industry × time fixed effects and use the resulting residuals to compute the median used for each sub-sample. Controls include market capitalization, book-to-market, ROA, previous 12-month return, and leverage. We also include the number of cybersecurity incidents that the software customer c has experienced over the previous year. We include the following sets of fixed effects: software customer and time fixed effects. t-statistics based on standard errors clustered by customer are shown in parentheses. *, **, and *** denote significance at the 10%, 5%, and 1% levels, respectively. A complete list of definitions for these variables is provided in the Data Appendix.

	Past Cyberattacks		Cyber 10-K Disclosure		Cybersecurity		Software Expertise	
	Low	High	Low	High	Without	With	Low	High
All Attacks$_{c,t+1}$	2.142**	5.498***	2.571***	4.077***	3.616***	1.970	6.228***	2.459***
	(2.44)	(5.17)	(2.76)	(3.62)	(4.70)	(1.55)	(4.30)	(3.05)
Return Vol.$_{c,t+1}$	0.067***	0.132***	0.053***	0.140***	0.107***	0.044	0.118***	0.081***
	(4.97)	(5.49)	(2.62)	(6.54)	(8.00)	(1.11)	(5.67)	(5.11)
Value-at-Risk$_{c,t+1}$	0.065***	0.145***	0.046**	0.127***	0.110***	0.051*	0.125***	0.082***
	(5.18)	(5.58)	(2.48)	(5.70)	(7.87)	(1.78)	(5.85)	(4.97)
Exp. Shortfall$_{c,t+1}$	0.048***	0.133***	0.036*	0.101***	0.090***	0.057*	0.101***	0.067***
	(3.69)	(5.33)	(1.71)	(4.65)	(6.32)	(2.06)	(4.71)	(4.38)
Lower Partial SD$_{c,t+1}$	0.048***	0.128***	0.038*	0.099***	0.085***	0.064**	0.094***	0.068***
	(3.83)	(5.29)	(1.78)	(4.61)	(6.42)	(2.20)	(4.83)	(4.18)

Table 7: Firm's Reaction to Software Vulnerabilities

This table studies the real effects of customers' exposure to SVs. We report estimates of the model:

$$Y_{c,t+1} = \alpha + \beta SV_{c,t} + \gamma X_{c,t} + \epsilon_{c,t+1}$$

the dependent variables are firm c's capital investment rate $\mathrm{I}_{c,t+1}/\mathrm{K}_{c,t}$, sales growth, an indicator variable that takes value of 1 if customer c has a relationship with a cybersecurity company in quarter t+1, and the MSCI Data Privacy score. The main independent variable is an indicator with value 1 if customer c is exposed to a vulnerability from one of its software suppliers in quarter t. Controls include market capitalization, book-to-market, ROA, previous 12-month return, leverage. We also include the number of cybersecurity incidents that the software customer c has experienced over the previous year. α indicates customer and Fama–French 48-industry × time (year-quarter) fixed effects. t-statistics based on standard errors clustered by customer are shown in parentheses. *, **, and *** denote significance at the 10%, 5%, and 1% levels, respectively. A complete list of definitions for these variables is provided in the Data Appendix.

	$\mathrm{I}_{c,t+1}/\mathrm{K}_{c,t}$ (1)	CapEx Growth$_{c,t+1}$ (2)	Cyber Security$_{c,t+1}$ (3)	Data Privacy Score$_{c,t+1}$ (4)
$\mathrm{SV}_{c,t}$	-0.063***	-0.132***	0.222***	0.052***
	(-4.13)	(-12.88)	(8.26)	(2.97)
Customer Controls$_{c,t}$	Yes	Yes	Yes	Yes
Customer FE	Yes	Yes	Yes	Yes
Industry x Time FE	Yes	Yes	Yes	Yes
Observations	94,731	94,731	94,731	94,731
Adjusted r^2	0.209	-0.015	0.531	0.736

Table 8: Vulnerabilities and Cybersecurity Incidents at the Software Company-Level

This table studies how the diffusion of a software supplier's products affects the relation between the probability of cybersecurity attacks and exposure to software vulnerabilities. We report estimates of the model:

$$\frac{Cyberattacks_{s,t+1}}{N_{t+1}} = \alpha + \beta_1 SV_{s,t} + \beta_2 Size_{s,t} + \beta_3 SV_{s,t} \times Size_{s,t} + \gamma X_{s,t} + \epsilon_{s,t+1}$$

the dependent variables are the number of cybersecurity incidents of any type (columns (1)), the number of cybersecurity incidents of any type occurring after 2010 (columns (2)), those related to vulnerabilities (columns (3)), or those due to causes different from vulnerabilities (columns (4)) that hit software supplier s' customers in quarter $t+1$, scaled by the total number of firms in our sample at time $t+1$. The main independent variable is an indicator with value 1 if one of the software products of supplier s has a vulnerability in quarter t. $Size_{s,t}$ is defined as supplier s's sales normalized by total sales across firms in CRSP/Compustat data in quarter t. We control for the average market capitalization, book-to-market, ROA, previous 12-month return, leverage of software supplier s customers. We also include the number of cybersecurity incidents that the software supplier s customers have experienced over the previous year. α indicates time and software supplier fixed effects. t-statistics based on standard errors clustered by supplier are shown in parentheses. *, **, and *** denote significance at the 10%, 5%, and 1% levels, respectively. A complete list of definitions for these variables is provided in the Data Appendix.

	All Attacks$_{s,t+1}$ (1)	Attacks > 2010$_{s,t+1}$ (2)	Vulnerability Attacks$_{s,t+1}$ (3)	Other Attacks$_{s,t+1}$ (4)
SV$_{s,t}$	-0.021*	-0.021*	-0.034**	-0.001
	(-1.91)	(-1.85)	(-2.04)	(-0.29)
Size$_{s,t}$	0.086**	0.050	-0.008	0.073*
	(2.27)	(1.26)	(-0.31)	(1.85)
SV$_{s,t}$ × Size$_{s,t}$	0.065***	0.063***	0.111***	-0.002
	(6.62)	(6.28)	(7.16)	(-0.65)
Supplier Controls$_{s,t}$	Yes	Yes	Yes	Yes
Supplier FE	Yes	Yes	Yes	Yes
Time FE	Yes	Yes	Yes	Yes
Observations	34,336	25,811	25,811	25,811
Adjusted r^2	0.199	0.186	0.087	0.147

Table 9: Vulnerabilities and Firm Risk at the Software Company-Level

This table studies how the market share of a software supplier and the size of the software sector affect the relation between risk variables and exposure to software vulnerabilities. In two subsamples based on the size of the software sector, we estimate the model:

$$log\left(\frac{Risk_{s,t+1}}{Risk_{s,t-1}}\right) = \alpha + \beta_1 SV_{s,t} + \beta_2 Market\ Share_{s,t} + \beta_3 SV_{s,t} \times Market\ Share_{s,t} + \gamma X_{s,t} + \epsilon_{s,t+1}$$

the dependent variables are the log change in the equal-weighted averages of the return volatility, value-at-risk (VaR), expected shortfall, and the second-order LPM of software supplier s customers in quarter $t+1$. The main independent variable is an indicator with value 1 if one of the software products of supplier s has a vulnerability in quarter t. *Market Share* is computed as the ratio of software supplier s sales to the total sales of the software sector in quarter t. Panel A reports estimates for the subsamples of dates when the software sector is larger than its time-series median size, whereas Panel B focuses on dates when the software sector is smaller than its time-series median size. We control for the average market capitalization, book-to-market, ROA, previous 12-month return, leverage of software supplier s customers. We also include the number of cybersecurity incidents that the software supplier s customers have experienced over the previous year. α indicates time and software supplier fixed effects. t-statistics based on standard errors clustered by supplier are shown in parentheses. *, **, and *** denote significance at the 10%, 5%, and 1% levels, respectively. A complete list of definitions for these variables is provided in the Data Appendix.

Panel A: Above Median Software Sector Size

	Return Vol.$_{s,t+1}$	Value-at-Risk$_{s,t+1}$	Exp. Shortfall$_{s,t+1}$	Lower Partial SD$_{s,t+1}$
SV$_{s,t}$	-0.001	-0.002	-0.003***	-0.003
	(-0.45)	(-0.76)	(-2.68)	(-1.11)
Market Share$_{s,t}$	0.042***	0.035**	0.100***	0.040**
	(2.77)	(2.01)	(2.97)	(2.38)
SV$_{s,t}$ × Market Share$_{s,t}$	0.005**	0.008***	0.006***	0.009***
	(2.11)	(3.30)	(3.18)	(3.83)
Supplier Controls$_{s,t}$	Yes	Yes	Yes	Yes
Supplier FE	Yes	Yes	Yes	Yes
Time FE	Yes	Yes	Yes	Yes
Observations	15,842	15,842	15,842	15,842
Adjusted r^2	0.217	0.182	0.529	0.223

Panel B: Below Median Software Sector Size

	Return Vol.$_{s,t+1}$	Value-at-Risk$_{s,t+1}$	Exp. Shortfall$_{s,t+1}$	Lower Partial SD$_{s,t+1}$
SV$_{s,t}$	0.062**	0.070**	0.009	0.073***
	(2.00)	(2.15)	(0.23)	(2.81)
Market Share$_{s,t}$	-0.000	-0.004	-0.014	-0.003
	(-0.06)	(-0.57)	(-0.48)	(-0.37)
SV$_{s,t}$ × Market Share$_{s,t}$	-0.035	-0.041	-0.004	-0.041*
	(-1.46)	(-1.57)	(-0.15)	(-1.91)
Supplier Controls$_{s,t}$	Yes	Yes	Yes	Yes
Supplier FE	Yes	Yes	Yes	Yes
Time FE	Yes	Yes	Yes	Yes
Observations	16,690	16,690	16,690	16,690
Adjusted r^2	0.295	0.210	0.490	0.276

Table 10: The Aggregate Impact on Cyberattacks

This table studies the impact of SVs and software industry size on the total number of cyberattacks in the economy. We report estimates of the model:

$$\frac{Cyberattacks_{t+1}}{N_{t+1}} = \alpha + \beta_1 Size_{S,t} + \beta_2 SV_{S,t} + \beta_3 Size_{S,t} \times SV_{S,t} + \epsilon_{t+1}$$

The dependent variable is the number of cybersecurity incidents affecting firms in our sample in quarter $t+1$: all incidents (Column 1); all incidents from 2010 onward (Column 2); incidents linked to vulnerabilities (Column 3); and incidents due to other causes (Column 4). We scale all these variables by the number of firms in our sample at time $t+1$. $Size_{S,t}$ is computed as total sales across all software companies in our data, normalized by total CRSP/Compustat sales in quarter t. $SV_{S,t}$ is the number of vulnerabilities emerging in quarter t, divided by the number of software companies in our sample in that quarter. t-statistics based on heteroscedasticity-robust standard errors are shown in parentheses. *, **, and *** denote significance at the 10%, 5%, and 1% levels, respectively. A complete list of definitions for these variables is provided in the Data Appendix.

	All Attacks$_{t+1}$	Attacks > 2010$_{t+1}$	Vulnerablity Attacks$_{t+1}$	Other Attacks$_{t+1}$
SV$_{S,t}$	0.143	0.145	0.208**	-0.057
	(1.54)	(1.56)	(2.35)	(-0.86)
Size$_{S,t}$	0.451***	0.457***	0.299***	-0.108*
	(4.87)	(4.94)	(2.92)	(-1.89)
SV$_{S,t}$ × Size$_{S,t}$	0.267***	0.260***	0.316***	0.033
	(4.32)	(4.19)	(4.88)	(0.87)
Observations	77	77	77	77
Adjusted r^2	0.409	0.407	0.400	-0.025

Table 11: The Aggregate Impact on Market Volatility

This table reports the impact of SVs, software industry concentration, and software industry size on stock market volatility. We estimate the following model in two subsamples defined by the size of the software sector:

$$log\left(\frac{Vol_{t+1}}{Vol_t}\right) = \alpha + \beta_1 HHI_{S,t} + \beta_2 SV_{S,t} + \beta_3 HHI_{S,t} \times SV_{S,t} + \epsilon_{t+1}$$

the dependent variables are computed using the standard deviation of quarterly CRSP value-weighted index returns or the VIX index. $HHI_{S,t}$ is the Herfindahl–Hirschman Index of the software sector, based on the sales of the software companies in our sample. $SV_{S,t}$ is the number of vulnerabilities emerging in quarter t, divided by the number of software companies in our sample in that quarter. Columns (1) and (2) report estimates for quarters in which the sales-based size of the software sector is above its time-series median; Columns (3) and (4) report estimates for quarters in which it is below the median. t-statistics based on heteroscedasticity robust standard errors are shown in parentheses. *, **, and *** denote significance at the 10%, 5%, and 1% levels, respectively. A complete list of definitions for these variables is provided in the Data Appendix.

	Large Software Sector		Small Software Sector	
	CRSP VW Vol.$_{t+1}$	VIX$_{t+1}$	CRSP VW Vol.$_{t+1}$	VIX$_{t+1}$
SV$_{S,t}$	0.397*	0.357	-1.052	-1.591
	(1.83)	(1.62)	(-0.57)	(-0.93)
HHI$_{S,t}$	0.047	-0.022	-0.687*	-0.529
	(0.32)	(-0.15)	(-1.77)	(-1.31)
SV$_{S,t}$ × HHI$_{S,t}$	0.283**	0.308**	-2.395	-1.781
	(2.17)	(2.28)	(-1.47)	(-1.15)
Observations	37	37	38	38
Adjusted r^2	-0.054	-0.013	-0.035	-0.030

Internet Appendix for "Software Diffusion and Cyber Risk"

by Giorgio Ottonello and Emanuele Rizzo

Data appendix: Variable definitions

Variable	Definition
Dependent Variables - Customer-Level Data	
All Attacks$_{c,t+1}$	Defined as the number of cyberattacks of any type that customer c experiences in quarter $t+1$. Source: Our database (PRC + VERIS + Hackmageddon)
Attacks >= 2010$_{c,t+1}$	Defined as the number of cyberattacks of any type that customers of software company s experience in quarter $t+1$. Restricted to the sample period from January 2010 through December 2024. Source: Our database (PRC + VERIS + Hackmageddon)
$VulnerabilityAttacks_{c,t+1}$	Defined as the number of cyberattacks directly caused by a vulnerability in our sample that customer c experiences in quarter $t+1$. Restricted to the sample period from January 2010 through December 2024. Source: Our database (PRC + VERIS + Hackmageddon)
$OtherAttacks_{c,t+1}$	Defined as the number of cyberattacks that we are unable to link to a vulnerability in our sample that customer c experiences in quarter $t+1$. Restricted to the sample period from January 2010 through December 2024. Source: Our database (PRC + VERIS + Hackmageddon)
$ReturnVolatility_{c,t+1}$	Computed as the standard deviation of daily stock returns over a quarter. A minimum number of 21 daily returns is required for the calculation. Source: CRSP.
$Value-at-Risk_{c,t+1}$	Computed as the absolute value of the worst 5% daily return over a quarter. A minimum number of 21 daily returns is required for the calculation. Source: CRSP.
$ExpectedShortfall_{c,t+1}$	Computed as the (absolute) average value across the worst 5% daily returns over a quarter. A minimum number of 21 daily returns is required for the calculation. Source: CRSP.
$LowerPartialSD_{c,t+1}$	Computed as the standard deviation of negative daily stock returns over a quarter. A minimum number of 21 daily returns is required for the calculation. Source: CRSP.
$CAR_{c,t+n\to t+m}$	The cumulative abnormal return of firm c computed starting at date $t+n$ days and ending at date $t+m$ days, where t is the date of the SV discovery. To compute abnormal returns we use the Fama-French 5-factor model and an estimation window of 220 trading days (-251, -31) where day 0 is the date of the event. We require at least 63 nonmissing returns in the estimation window. Source: CRSP.
$I_{c,t+1}/K_{c,t}$	The capital stock $K_{c,t}$ is computed recursively using a perpetual-inventory method, as described in Stein and Stone (2013). $I_{c,t+1}$ represents capital expenditures (CAPX) Source: CRSP/Compustat Merged.
CAPEX Growth$_{c,t+1}$	The difference in firm capital expenditures (CAPX) in t minus capital expenditures in $t-$, divided by capital expenditures in $t-1$. Source: CRSP/Compustat Merged.
Cybersecurity Relation$_{c,t+1}$	Indicator variable that takes value of 1 if customer c hires a cybersecurity company in quarter $t+1$. Source: Factset Revere.
Data Privacy Score$_{c,t+1}$	Privacy & Data Security Score. High values of this score reflect companies with comprehensive privacy policies and data security management systems. The score ranges from 0 to 10. Source: MSCI ESG.

Continued on next page

– continued from previous page

Variable	Definition
Dependent Variables - Supplier-Level Data	
All Attacks$_{s,t+1}$	Defined as the number of cyberattacks of any type that hit customers of software company s in quarter $t+1$. Source: Our database (PRC + VERIS + Hackmageddon)
Attacks >= 2010$_{s,t+1}$	Defined as the number of cyberattacks of any type that hit customers of software company s in quarter $t+1$. Restricted to the sample period from January 2010 through December 2024. Source: Our database (PRC + VERIS + Hackmageddon)
$VulnerabilityAttacks_{s,t+1}$	Defined as the number of cyberattacks directly caused by a vulnerability in our sample that hit customers of software company s in quarter $t+1$. Restricted to the sample period from January 2010 through December 2024. Source: Our database (PRC + VERIS + Hackmageddon)
$OtherAttacks_{s,t+1}$	Defined as the number of cyberattacks that we are unable to link to a vulnerability in our sample that hit customers of software company s in quarter $t+1$. Restricted to the sample period from January 2010 through December 2024. Source: Our database (PRC + VERIS + Hackmageddon)
$ReturnVolatility_{s,t+1}$	Computed as the equal-weighted average of the standard deviation of daily stock returns over a quarter across customers of software company s. A minimum number of 21 daily returns is required for the calculation. Source: CRSP.
$Value-at-Risk_{s,t+1}$	Computed as the equal-weighted average of the absolute value of the worst 5% daily return over a quarter across customers of software company s. A minimum number of 21 daily returns is required for the calculation. Source: CRSP.
$ExpectedShortfall_{s,t+1}$	Computed as the equal-weighted average of the (absolute) average value across the worst 5% daily returns over a quarter across customers of software company s. A minimum number of 21 daily returns is required for the calculation. Source: CRSP.
$LPSD_{s,t+1}$	Computed as the equal-weighted average of the standard deviation of negative daily stock returns over a quarter across customers of software company s. A minimum number of 21 daily returns is required for the calculation. Source: CRSP.
Dependent Variables - Economy-Level Data	
All Attacks$_{t+1}$	Defined as the number of cyberattacks of any type that hit firms in our sample in quarter $t+1$. Source: Our database (PRC + VERIS + Hackmageddon)
Attacks >= 2010$_{t+1}$	Defined as the number of cyberattacks of any type that hit firms in our sample in quarter $t+1$. Restricted to the sample period from January 2010 through December 2024. Source: Our database (PRC + VERIS + Hackmageddon)
$VulnerabilityAttacks_{t+1}$	Defined as the number of cyberattacks directly caused by a vulnerability in our sample that hit firms in our sample in quarter $t+1$. Restricted to the sample period from January 2010 through December 2024. Source: Our database (PRC + VERIS + Hackmageddon)
$OtherAttacks_{t+1}$	Defined as the number of cyberattacks that we are unable to link to a vulnerability in our sample that hit firms in our sample in quarter $t+1$. Restricted to the sample period from January 2010 through December 2024. Source: Our database (PRC + VERIS + Hackmageddon)
$CRSP\ VW\ Vol._{t+1}$	Computed as the standard deviation of daily returns of the CRSP Value-Weighted index over a quarter. A minimum number of 21 daily returns is required for the calculation. Source: CRSP.

Continued on next page

– continued from previous page

Variable	Definition
VIX_{t+1}	Computed as the average level of the VIX index over a quarter. A minimum number of 21 daily returns is required for the calculation. Source: CRSP.
Independent Variables - Customer-Level Data	
$SV_{c,t}$	Defined as an indicator with a value of 1 if customer c is affected by a software vulnerability in quarter t. Source: NIST database.
$Size_{c,t}$	The market value of common equity. Market value of equity is the product of the price (PRC) at the end of quarter t times the contemporaneous number of shares outstanding (SHROUT). Source: CRSP.
$Book-to-market_{c,t}$	The ratio of the book equity divided by the market value of equity. The book value of equity is calculated as stockholder equity, plus deferred taxes and credits, minus the book value of preferred stock. Stockholders' equity is the first available from the following list: i) the Compustat item (SEQ); ii) the book value of common equity (item CEQ), plus preferred stock (item PSTK); iii) the book value of total assets (AT) minus the book value of total liabilities (LT). Deferred taxes and credits are measured through the first available of the following: i) the Compustat item (TXDITC); ii) the sum of balance-sheet deferred taxes (TXDB) and investment tax-credit, (TCB); iii) zero. The book value of preferred stock is the first available of the following: i) redemption value (PSTKRV); ii) liquidation value (PSTKL); iii) par value (PSTK); iv) zero. Source: CRSP/Compustat Merged.
$Past12-monthReturn_{c,t}$	The cumulated continuously compounded stock return from month $j-12$ to month $j-1$, where j is the first month of quarter t. Source: CRSP.
$Profitability_{c,t}$	Ratio of a firm EBITDA over the firm total assets (AT). Source: CRSP/Compustat Merged.
$Leverage_{c,t}$	The ratio of a firm's total debt (long-term debt plus short-term debt) over the firm's total asset value. Source: CRSP/Compustat Merged.
$PastCyberattacks_{c,t}$	Number of cyberattacks attacks a firm has experienced over the past 12 months. Source: Our database (PRC + VERIS + Hackmageddon)
Independent Variables - Supplier-Level Data	
$SV_{s,t}$	Defined as an indicator with a value of 1 if a product of software supplier s is affected by a software vulnerability in quarter t. Source: NIST database.
$Size_{s,t}$	Computed as the ratio of software company s's sales to the total sales across all companies in the CRSP/Compustat merged database. Source: Factset Revere and CRSP/Compustat.
$MarketShare_{s,t}$	Computed as the ratio of software company s's sales to the total sales across all software companies in our sample. Source: Factset Revere and CRSP/Compustat.
$CustomerSize_{s,t}$	Equal-weighted average of the market value of common equity across all customers of software company s. Source: CRSP.
$Book-to-market_{s,t}$	Equal-weighted average of the ratio of the book equity divided by the market value of equity across all customers of software company s. Source: CRSP/Compustat Merged.
$Past12-monthReturn_{s,t}$	Equal-weighted average of the cumulated compounded stock return from month $j-12$ to month $j-1$ across all customers of software company s. Source: CRSP.

Continued on next page

– continued from previous page

Variable	Definition
$Profitability_{s,t}$	Equal-weighted average of the ratio of a firm EBITDA over the firm total assets (AT) across all customers of software company s. Source: CRSP/Compustat Merged.
$Leverage_{s,t}$	Equal-weighted average of the ratio of a firm's total debt (long-term debt plus short-term debt) over the firm's total asset value across all customers of software company s. Source: CRSP/Compustat Merged.
$PastCyberattacks_{s,t}$	Total number of cyberattacks attacks experienced by the customers of software supplier S over the past 12 months. Source: Our database (PRC + VERIS + Hackmageddon)
Independent Variables - Economy-Level Data	
$SV_{S,t}$	Defined as the ratio of the number of software vulnerabilities discovered in quarter t to the number of software companies active in the sample in quarter t. Source: NIST database.
$Size_{S,t}$	Computed as the ratio of total sales of software companies in our data to the total sales across all companies in the CRSP/Compustat merged database. Source: Factset Revere and CRSP/Compustat.
$HHI_{S,t}$	The Herfindhal-Hirschman Index of the software industry based on the sales of software companies in our data. Source: Factset Revere and CRSP/Compustat.

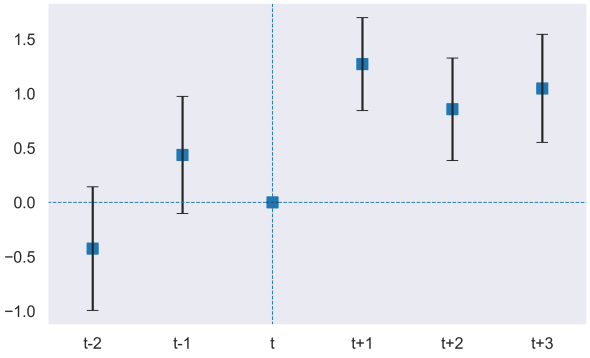
Table IA2: Vulnerable Software Suppliers

This table shows the number of common vulnerabilities and exposures (CVE), the number of customers, and the share of customers of the software suppliers in our treated sample. To construct customer share, we divide the number of customers served by each software company at time t by the total number of customers served by at least one software company at that time, and then we take the time-series average for each supplier.

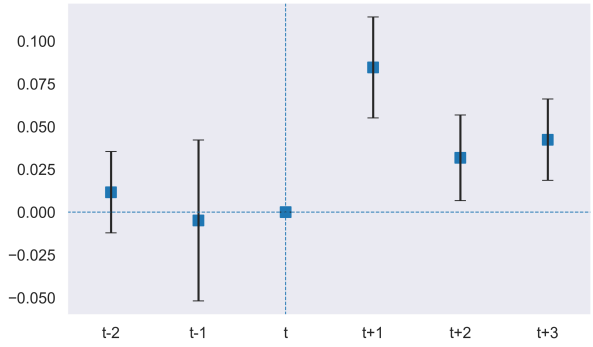
Software Supplier	Vulnerabilities	Customers	Customer Share
ADOBE INC	380	256	1.97
ADTRAN HOLDINGS INC	1	61	0.58
APPLE INC	100	579	5.27
ATLASSIAN CORP PLC	12	81	1.61
AUTODESK INC	18	57	0.34
BARRACUDA NETWORKS INC	2	49	0.72
BENTLEY SYSTEMS INC	5	2	0.05
CISCO SYSTEMS INC	71	434	4.52
CITRIX SYSTEMS INC	14	165	1.66
DELL TECHNOLOGIES INC	2	131	2.91
ELASTIC N V	1	51	1.16
EXTREME NETWORKS INC	3	102	0.76
F 5 INC	7	79	0.71
FORTINET INC	13	70	0.79
H P INC	11	564	5.69
HEWLETT PACKARD ENTERPRISE CO	2	157	2.71
INTEL CORP	2	293	3.58
INTELLISYNC CORP	9	49	1.24
INTERNATIONAL BUSINESS MACHS COR	12	759	7.62
INTERNET BRANDS INC	1	6	0.16
JUNIPER NETWORKS INC	8	139	1.33
KEYSIGHT TECHNOLOGIES INC	4	33	0.59
LEXMARK INTERNATIONAL INC NEW	6	69	0.69
MCAFEE CORP	2	19	0.58
META PLATFORMS INC	2	257	2.86
MICRO FOCUS INTERNATIONAL PLC	2	64	0.81
MICROSOFT CORP	584	1058	10.61
MITEL NETWORKS CORP	2	34	0.49
MONGODB INC	1	76	0.95
NATIONAL INSTRUMENTS CORP	2	49	0.57
NETGEAR INC	39	63	0.91
NOKIA CORP	1	131	2.12
ORACLE CORP	45	729	6.31
PALO ALTO NETWORKS INC	4	82	0.84
PROGRESS SOFTWARE CORP	4	222	2.35
QLIK TECHNOLOGIES INC	3	60	0.56
QUALCOMM INC	6	152	1.49
REALNETWORKS INC	1	62	0.44
ROCKWELL AUTOMATION INC	4	86	0.56
RUCKUS WIRELESS INC	1	17	0.46
S A P SE	15	444	3.58
SANGOMA TECHNOLOGIES CORP	1	12	0.30
SIEMENS A G	78	356	3.14
SOLARCITY CORP	3	18	0.21
SOLARWINDS CORP	61	70	1.42
SONOS INC	4	9	0.28
SYNACOR INC	9	49	1.24
T I B C O SOFTWARE INC	2	97	0.88
TECHTEAM GLOBAL INC	12	77	0.98
TENABLE HOLDINGS INC	1	49	0.75
TESLA INC	3	31	0.29
UBIQUITI INC	2	17	0.26
UNIVERSAL BROADBAND NETWORKS INC	1	7	0.20
VMWARE INC	45	208	2.37
WESTERN DIGITAL CORP	9	56	0.62

Figure IA1: Vulnerabilities and Customer Risk: Dynamic Effects

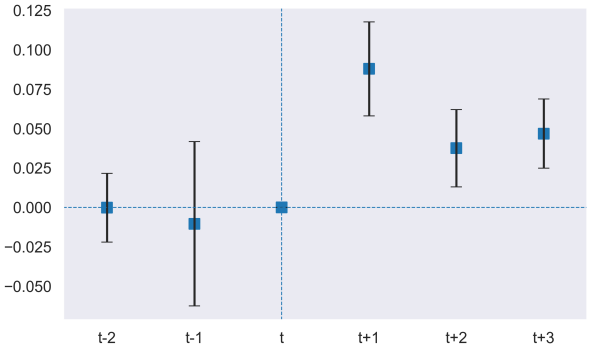
This figure studies the dynamic effect of exposure to SVs on the probability of cyberattacks and firm risk. Figure A plots estimates from equation (15), where the dependent variable is the probability of cyberattacks. Figure B through E plot estimates from equation (17), where the dependent variables are: return volatility, value-at-risk (VaR), expected shortfall, and the second-order LPM. In all figures, the main independent variable is an indicator with value 1 if customer c is exposed to a vulnerability through one of its software suppliers. Controls include market capitalization, book-to-market, ROA, previous 12-month return, leverage. We also include the number of cybersecurity incidents that the software customer c has experienced over the previous year. In Panel A α denotes Fama-French 48-industry $\times$ time fixed effects. In Panel B through E, *alpha* indicates customer and Fama-French 48-industry $\times$ time fixed effects. Confidence intervals are based on standard errors clustered by customer and using a 99% confidence level. A complete list of definitions for these variables is provided in the Data Appendix.



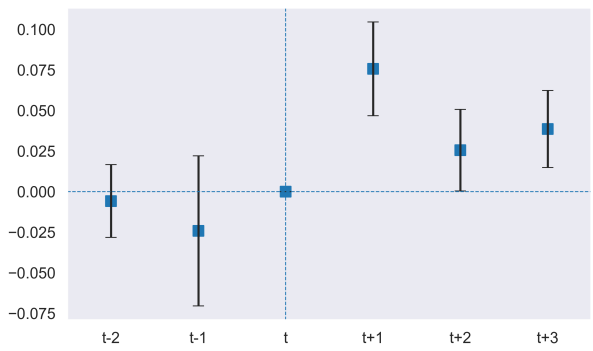
Panel A: Cyber Attacks



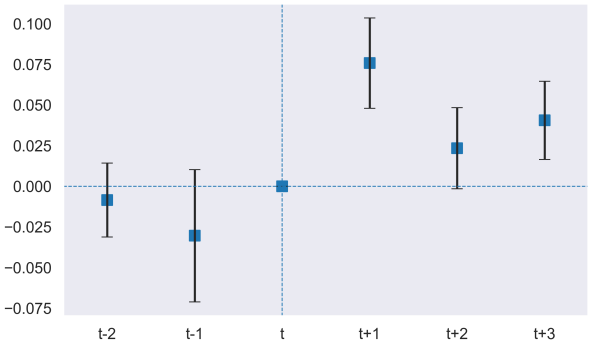
Panel B: Return Volatility



Panel C: Value-at-Risk



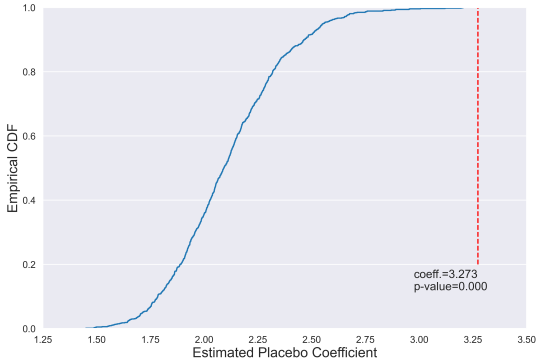
Panel D: Expected Shortfall



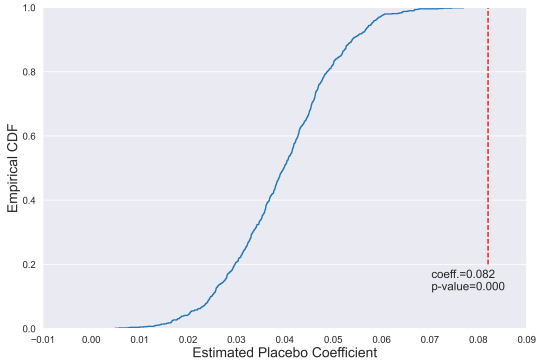
Panel E: Lower Partial Standard Deviation

Figure IA2: Non Parametric Permutation Tests

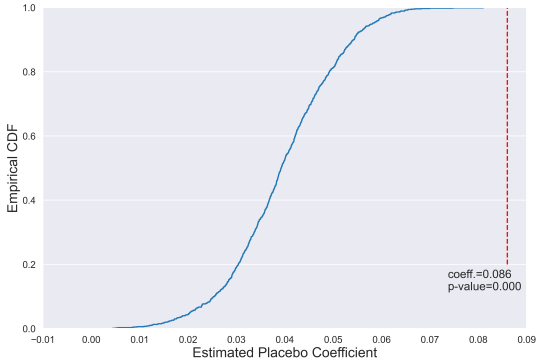
This figure shows the results of the block permutation procedure following the method in Chetty, Looney, and Kroft (2009). In each iteration, the dates of the vulnerability discoveries are randomly reassigned by firm with replacement as a placebo throughout the sample period. In Panel A we estimate the regression of column (1) from Table 3 on the falsified data and plot the empirical cumulative distribution function (cdf) generated from running 5,000 random iterations of this procedure and capturing the placebo coefficient estimate. In Panels B through E we perform this procedure for all columns of Table 4. The vertical dotted line indicates the position of the actual coefficient estimate for the impact that a vulnerability discovery has on each of the dependent variables and the implied p-value when placed in the context of the cdf. The implied p-value reported in each plot shows the proportion of the placebo coefficients that are contrasted with the actual regression coefficient.



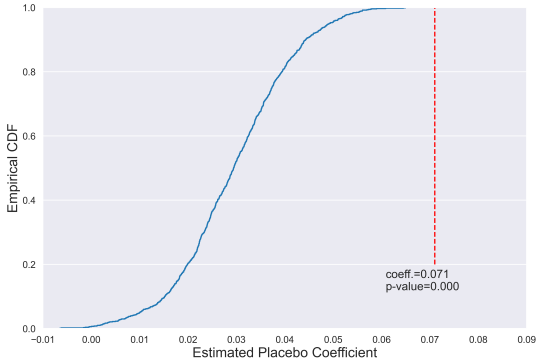
Panel A: Cyber Attacks



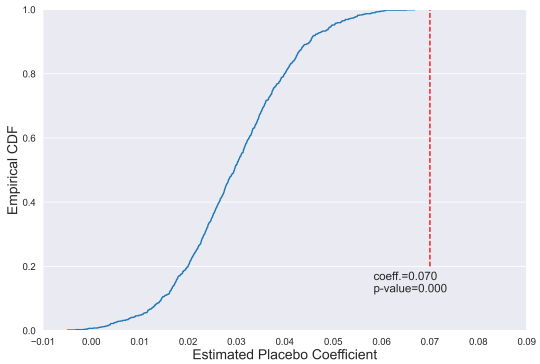
Panel B: Return Volatility



Panel C: Value-at-Risk



Panel D: Expected Shortfall



Panel E: Lower Partial Standard Deviation

Table IA3: Vulnerabilities and Cybersecurity Incidents

This table studies the relation between the probability of cybersecurity attacks and exposure to SVs. We report estimates of the model:

$$CyberAttacks_{c,t+1} = \alpha + \beta SV_{c,t} + \gamma X_{c,t} + \epsilon_{c,t+1}$$

the dependent variables are the number of cybersecurity incidents of any type (column (1)), the number of cybersecurity incidents of any type occurred after 2010 (column (2)), related to vulnerabilities (column (3)), or due to causes different from vulnerabilities (column (4)) that hit the software customer c in quarter $t+1$. In all columns, the main independent variable is an indicator with value 1 if customer c is exposed to a vulnerability through one of its software suppliers in quarter t. Controls include market capitalization, book-to-market, ROA, previous 12-month return, and leverage. We also include the number of cybersecurity incidents that the software customer c has experienced over the previous year. α indicates customer and Fama-French 48-industry $\times$ time fixed effects. t-statistics based on standard errors clustered by customer are shown in parentheses. *, **, and *** denote significance at the 10%, 5%, and 1% levels, respectively. A complete list of definitions for these variables is provided in the Data Appendix.

	All Attacks$_{c,t+1}$ (1)	Attacks > 2010$_{c,t+1}$ (2)	Vulnerability Attacks$_{c,t+1}$ (3)	Other Attacks$_{c,t+1}$ (4)
SV$_{c,t}$	0.103***	0.102***	0.117***	0.005
	(4.34)	(4.32)	(4.42)	(0.31)
Customer Controls$_{c,t}$	Yes	Yes	Yes	Yes
Customer FE	Yes	Yes	Yes	Yes
Time FE	Yes	Yes	Yes	Yes
Observations	98,885	76,356	76,356	76,356
Adjusted r^2	0.051	0.058	0.056	0.048

Table IA4: The Impact of Software Vulnerabilities: Major Vulnerabilities

This table studies the impact of software vulnerabilities on the probability of cybersecurity attacks and on risk variables. In this table we repeat the analyses of Tables 3 and 4. In all columns, the main independent variable is an indicator with value 1 if customer c is exposed to a vulnerability through one of its software suppliers in quarter t. A vulnerability is defined as major when the vulnerability scoring is above or equal seven. Controls include market capitalization, book-to-market, ROA, previous 12-month return, and leverage. We also include the number of cybersecurity incidents that the software customer c has experienced over the previous year. In Panel A α indicates Fama-French 48-industry $\times$ time fixed effects. In Panel B α indicates customer and Fama-French 48-industry $\times$ time fixed effects. t-statistics based on standard errors clustered by customer are shown in parentheses. *, **, and *** denote significance at the 10%, 5%, and 1% levels, respectively. A complete list of definitions for these variables is provided in the Data Appendix.

Panel A: Cyberattacks

	All Attacks$_{c,t+1}$ (1)	Attacks > 2010$_{c,t+1}$ (2)	Vulnerability Attacks$_{c,t+1}$ (3)	Other Attacks$_{c,t+1}$ (4)
Major SV$_{c,t}$	3.387***	3.659***	4.947***	1.336
	(5.35)	(5.49)	(5.59)	(0.68)
Customer Controls$_{c,t}$	Yes	Yes	Yes	Yes
Industry x Time FE	Yes	Yes	Yes	Yes
Observations	98,885	76,356	76,356	76,356
Pseudo r^2	0.159	0.163	0.168	0.189

Panel B: Firm Risk

	Return Vol.$_{c,t+1}$ (1)	Value-at-Risk$_{c,t+1}$ (2)	Exp. Shortfall$_{c,t+1}$ (3)	Lower Partial SD$_{c,t+1}$ (4)
Major SV$_{c,t}$	0.099***	0.109***	0.086***	0.081***
	(7.96)	(9.09)	(7.01)	(6.56)
Customer Controls$_{c,t}$	Yes	Yes	Yes	Yes
Customer FE	Yes	Yes	Yes	Yes
Industry x Time FE	Yes	Yes	Yes	Yes
Observations	89,199	89,199	89,199	89,199
Adjusted r^2	0.098	0.111	0.086	0.057

Table IA5: The Impact of Software Vulnerabilities: Minor Vulnerabilities

This table studies the impact of software vulnerabilities on the probability of cybersecurity attacks and on risk variables. In this table we repeat the analyses of Tables 3 and 4. In all columns, the main independent variable is an indicator with value 1 if customer c is exposed to a vulnerability through one of its software suppliers in quarter t. A vulnerability is defined as minor when the vulnerability scoring is below seven. Controls include market capitalization, book-to-market, ROA, previous 12-month return, and leverage. We also include the number of cybersecurity incidents that the software customer c has experienced over the previous year. In Panel A α indicates Fama-French 48-industry $\times$ time fixed effects. In Panel B α indicates customer and Fama-French 48-industry $\times$ time fixed effects. t-statistics based on standard errors clustered by customer are shown in parentheses. *, **, and *** denote significance at the 10%, 5%, and 1% levels, respectively. A complete list of definitions for these variables is provided in the Data Appendix.

Panel A: Cyberattacks

	All Attacks$_{c,t+1}$ (1)	Attacks > 2010$_{c,t+1}$ (2)	Vulnerability Attacks$_{c,t+1}$ (3)	Other Attacks$_{c,t+1}$ (4)
Minor SV$_{c,t}$	1.225	1.256	1.470	0.936
	(0.78)	(0.86)	(1.23)	(-0.14)
Customer Controls$_{c,t}$	Yes	Yes	Yes	Yes
Industry x Time FE	Yes	Yes	Yes	Yes
Observations	98,885	76,356	76,356	76,356
Pseudo r^2	0.159	0.163	0.168	0.189

Panel B: Firm Risk

	Return Vol.$_{c,t+1}$ (1)	Value-at-Risk$_{c,t+1}$ (2)	Exp. Shortfall$_{c,t+1}$ (3)	Lower Partial SD$_{c,t+1}$ (4)
Minor SV$_{c,t}$	-0.015	-0.014	-0.018	-0.012
	(-1.12)	(-1.18)	(-1.41)	(-0.92)
Customer Controls$_{c,t}$	Yes	Yes	Yes	Yes
Customer FE	Yes	Yes	Yes	Yes
Industry x Time FE	Yes	Yes	Yes	Yes
Observations	89,199	89,199	89,199	89,199
Adjusted r^2	0.097	0.111	0.086	0.056

Table IA6: The Impact of Software Vulnerabilities: Supplier Data

This table studies the impact of software vulnerabilities on the probability of cybersecurity attacks and risk variables. In Panel A, we report estimates of the model:

$$CyberAttacks_{s,t+1} = \alpha + \beta SV_{s,t} + \gamma X_{s,t} + \epsilon_{s,t+1}$$

the dependent variables are the number of cybersecurity incidents of any type (column (1)), the number of cybersecurity incidents of any type occurring after 2010 (column (2)), those related to vulnerabilities (column (3)), or those due to causes different from vulnerabilities (column (4)) that hit the software supplier s customers in quarter $t+1$. In Panel B, we report estimates of the model:

$$log\left(\frac{Risk_{s,t+1}}{Risk_{s,t-1}}\right) = \alpha + \beta SV_{s,t} + \gamma X_{s,t} + \epsilon_{s,t+1}$$

the dependent variables are the equal-weighted averages of the return volatility, value-at-risk (VaR), expected shortfall, and the second-order LPM of software supplier s customers in quarter $t+1$. In all panels, the main independent variable is an indicator with value 1 if one of the software products of software company s has a vulnerability in quarter t. We control for the average market capitalization, book-to-market, ROA, previous 12-month return, leverage of software supplier s customers. We also include the number of cybersecurity incidents that the software supplier s customers have experienced over the previous year. α indicates software supplier and time fixed effects. t-statistics based on standard errors clustered by supplier are shown in parentheses. *, **, and *** denote significance at the 10%, 5%, and 1% levels, respectively. A complete list of definitions for these variables is provided in the Data Appendix.

Panel A: Cyberattacks Aggregated at the Supplier-Level

	All Attacks$_{s,t+1}$ (1)	Attacks > 2010$_{s,t+1}$ (2)	Vulnerability Attacks$_{s,t+1}$ (3)	Other Attacks$_{s,t+1}$ (4)
SV$_{s,t}$	0.012***	0.009***	0.014	-0.001
	(3.99)	(2.68)	(1.10)	(-0.14)
Supplier Controls$_{s,t}$	Yes	Yes	Yes	Yes
Supplier FE	Yes	Yes	Yes	Yes
Time FE	Yes	Yes	Yes	Yes
Observations	40,350	31,832	31,832	31,832
Adjusted r^2	0.254	0.232	0.085	0.061

Panel B: Firm Risk Aggregated at the Supplier-Level

	RetVol$_{s,t+1}$ (1)	Var 95%$_{s,t+1}$ (2)	ES 95%$_{s,t+1}$ (3)	LPSD$_{s,t+1}$ (4)
SV$_{s,t}$	0.025***	0.024***	0.021***	0.025***
	(4.67)	(5.18)	(4.49)	(5.49)
Supplier Controls$_{s,t}$	Yes	Yes	Yes	Yes
Supplier FE	Yes	Yes	Yes	Yes
Time FE	Yes	Yes	Yes	Yes
Observations	40,376	40,376	40,376	40,376
Adjusted r^2	0.489	0.410	0.503	0.445

Table IA7: Vulnerabilities and Cybersecurity Incidents: Excluding Top Software Suppliers

This table studies the relation between the probability of cybersecurity attacks and exposure to SVs. We report estimates of the model:

$$P(\text{CyberAttack}_{c,t+1} = 1 \mid \text{SV}_{c,t}, X_{c,t}, \alpha_{i,t}) = \Lambda(\alpha_{i,t} + \beta \text{SV}_{c,t} + X'_{c,t}\gamma)$$

the dependent variables are the number of cybersecurity incidents of any type (column (1)), the number of cybersecurity incidents of any type occurred after 2010 (column (2)), related to vulnerabilities (column (3)), or due to causes different from vulnerabilities (column (4)) that hit the software customer c in quarter $t+1$. The main independent variable is an indicator with value 1 if customer c is exposed to a vulnerability through one of its software suppliers in quarter t. In Panel A, we exclude Microsoft customers from the sample. In Panel B and C we exclude customers of Adobe and Apple, respectively. Controls include market capitalization, book-to-market, ROA, previous 12-month return, leverage. We also include the number of cybersecurity incidents that the software customer c has experienced over the previous year. α indicates Fama-French 48-industry $\times$ time fixed effects. t-statistics based on standard errors clustered by customer are shown in parentheses. *, **, and *** denote significance at the 10%, 5%, and 1% levels, respectively. A complete list of definitions for these variables is provided in the Data Appendix.

	All Attacks$_{c,t+1}$ (1)	Attacks > 2010$_{c,t+1}$ (2)	Vulnerability Attacks$_{c,t+1}$ (3)	Other Attacks$_{c,t+1}$ (4)
Excluding Microsoft				
SV$_{c,t}$	2.150***	2.166***	2.605***	1.366
	(3.77)	(3.75)	(3.96)	(0.82)
Excluding Adobe				
SV$_{c,t}$	3.349***	3.595***	4.712***	1.970**
	(6.07)	(6.15)	(5.84)	(2.01)
Excluding Apple				
SV$_{c,t}$	3.283***	3.518***	4.457***	2.100**
	(5.99)	(6.07)	(5.72)	(2.23)
Customer Controls$_{c,t}$	Yes	Yes	Yes	Yes
Industry x Time FE	Yes	Yes	Yes	Yes

Table IA8: Vulnerabilities and Customer Risk: Excluding Top Suppliers

This table studies the relation between the firm risk and exposure to SVs. We report estimates of the model:

$$log\left(\frac{Risk_{c,t+1}}{Risk_{c,t-1}}\right) = \alpha + \beta_1 SV_{c,t} + \gamma X_{c,t} + \epsilon_{c,t+1}$$

the dependent variables are the log change in return volatility, value-at-risk (VaR), expected shortfall, and the second-order LPM of software customer c between quarter $t-1$ and quarter $t+1$. The main independent variable is an indicator with value 1 if customer c is exposed to a vulnerability through one of its software suppliers in quarter t. In Panel A, we exclude Microsoft customers from the sample. In Panel B and C we exclude customers of Adobe and Apple, respectively. Controls include market capitalization, book-to-market, ROA, previous 12-month return, leverage. We also include the number of cybersecurity incidents that the software customer c experienced over the previous year. *alpha* indicates customer and Fama-French 48-industry × time fixed effects. t-statistics based on standard errors clustered by customer are shown in parentheses. *, **, and *** denote significance at the 10%, 5%, and 1% levels, respectively. A complete list of definitions for these variables is provided in the Data Appendix.

	Return Vol.$_{c,t+1}$ (1)	Value-at-Risk$_{c,t+1}$ (2)	Exp. Shortfall$_{c,t+1}$ (3)	Lower Partial SD$_{c,t+1}$ (4)
Excluding Microsoft				
SV$_{c,t}$	0.145***	0.145***	0.142***	0.136***
	(12.43)	(12.30)	(11.92)	(11.30)
Excluding Adobe				
SV$_{c,t}$	0.087***	0.089***	0.075***	0.074***
	(7.55)	(7.81)	(6.55)	(6.37)
Excluding Apple				
SV$_{c,t}$	0.091***	0.092***	0.086***	0.087***
	(7.99)	(8.17)	(7.55)	(7.61)
Customer Controls$_{c,t}$	Yes	Yes	Yes	Yes
Customer FE	Yes	Yes	Yes	Yes
Industry x Time FE	Yes	Yes	Yes	Yes