# Friendly Hackers and Information Value: Discovery of External Vulnerability and Operational Reliability


## Abstract

This paper examines whether vulnerability disclosure programs (VDPs), which invite external security researchers to report software and system vulnerabilities, create operational and information value. The informational meaning of program adoption is ambiguous. Inviting outside researchers may reveal limitations in internal detection and latent vulnerability, but it may also demonstrate confidence, transparency, and preparedness to identify and remediate defects. Using manually collected data on 404 programs adopted by U.S. public firms between 2010 and 2025, we study program adoption, stock-market reactions to disclosed cyberattacks, and subsequent breach frequency. VDP adoption is concentrated among large, innovative, profitable firms with substantial intangible assets and higher market risk exposure. Event-study evidence shows that the negative stock-market reaction to a cyberattack is concentrated among firms without such a program. Investors appear to place greater weight on the preparedness interpretation than on the vulnerability interpretation when evaluating a realized breach. A propensity-score-matched difference-in-differences analysis further shows that program adoption is associated with lower breach frequency, with the largest reduction in the first year after adoption. The association is stronger when monitoring and firm-specific board knowledge support remediation, and when formal risk or cybersecurity committees are absent. The findings show that external vulnerability discovery can be associated with improved operational reliability while also changing the information conveyed by digital failures.



Keywords: Vulnerability disclosure programs; Cybersecurity operations; Operational risk; Information value; Event study; Operational resilience

JEL: L23, L86, G14, G34

## 1. Introduction

Digital operations increasingly depend on interconnected software, data, employees, suppliers, and service providers. This dependence creates exposure to cyberattacks and data breaches, which can interrupt production, compromise service delivery, expose customers' personal information, and generate longer-term consequences through financial losses, erosion of customer trust, and reputational damage. Cyberattacks therefore constitute operational failures with consequences that extend well beyond information security.

Research has long examined the economic consequences of operational failures. Supply chain glitches lead to substantial shareholder losses (Hendricks & Singhal, 2003), service failures in customer information security destroy value across triadic relationships (Modi et al., 2015), and cyberattacks can propagate through interconnected supply-chain actors (Jeong et al., 2025). A related operations stream studies how software producers and users manage vulnerabilities through disclosure timing, patch release, inspection, and security maintenance (Arora et al., 2008; Kim et al., 2011; Sen et al., 2020; Bensoussan et al., 2020; Mookerjee & Samuel, 2023). This literature highlights the importance of vulnerability information and the value consequences of realized failures. However, this literature provides less evidence on the firm-level adoption of external detection processes, their association with subsequent realized failures, and their information value when failures occur.

We examine vulnerability disclosure programs (VDPs), formal channels through which firms invite external security researchers, often called ethical hackers, to identify and report vulnerabilities. A VDP expands the set of individuals searching for defects and directs their information into a firm-sanctioned workflow. This design applies the logic of broadcast search, crowd-based problem solving, and multiagent problem solving by allowing firms to access diverse external knowledge to address uncertain technical problems (Terwiesch & Xu, 2008; Jeppesen & Lakhani, 2010; Boudreau et al., 2011). It is also related to vulnerability markets and bug-bounty design, which examine how firms incentivize external researchers and attract vulnerability reports (Kannan & Telang, 2005; Zhang et al., 2024). Our focus differs from those studies. We study whether establishing the organizational process produces observable operational and capital-market outcomes, as the operational value of a VDP does not arise from disclosure alone. It requires the firm to screen reports, prioritize vulnerabilities, assign responsibility, remediate defects, and verify closure.

The operating challenge addressed by these programs differs from conventional security monitoring. Internal teams design and maintain the systems being tested, which gives them detailed contextual knowledge but can also narrow the range of assumptions and search paths they use. External researchers approach the same systems with different technical backgrounds, tools, incentives, and attack models. Their value therefore does not depend on replacing internal engineers. It arises from widening the search process around a complex and dynamic operational system. The firm still determines which assets are in scope, how reports are evaluated, which vulnerabilities receive priority, and whether corrective action is completed.

This distinction also clarifies why adoption may not produce uniform benefits. A reporting channel can increase the volume of incoming information without improving reliability if reports are poorly specified, triage is slow, responsibility is fragmented, or software teams lack the resources to remediate defects. In the worst case, unresolved vulnerabilities may remain exploitable, be disclosed publicly, or be used against the firm before the firm can resolve them. Conversely, even a modest flow of high-quality reports can create substantial value when the firm rapidly validates, fixes, and learns from them. The relevant operating process therefore extends from external search to internal execution. We use the adoption of a formal program as an observable starting point and examine outcomes that reflect this broader process, while recognizing that the available data do not directly observe every intermediate activity.

We therefore manually collect 404 firm-level VDPs adopted by U.S. public firms from 2010 to September 2025 from HackerOne, Bugcrowd, and firms' official websites. We merge these data with financial fundamentals from Compustat, board characteristics from BoardEx, ownership data from LSEG, cyber events, and stock performance data from CRSP. The final sample contains 282 unique firms with VDPs from 2010 to 2024.

First, we find that VDP adoption is concentrated among large, innovative, and profitable firms with substantial intangible assets and higher market risk exposure. The results indicate that VDP adoption is more common among firms with greater organizational resources and may be particularly valuable when operations depend heavily on digital assets and innovation.

Second, we use stock-market evidence surrounding actual cyberattacks to examine the information value of VDPs. The expected investor response is not unambiguous. A VDP may reveal that internal engineers and security controls cannot identify all relevant vulnerabilities and that the firm requires outside assistance. Alternatively, voluntarily inviting external scrutiny may

demonstrate confidence, transparency, and preparedness to detect and remediate defects. Following operations event studies of supply chain glitches and information-security failures (Hendricks & Singhal, 2003; Modi et al., 2015), we test which interpretation is better supported by investors' reactions when a cyberattack occurs. We find a significant negative market reaction for firms without VDPs, while the reaction is muted for firms with VDPs in the shorter event windows. The results indicate that investors place greater weight on the preparedness interpretation when evaluating a realized cyberattack.

Third, we examine whether VDP adoption is associated with fewer subsequent data breaches using a propensity-score-matched difference-in-differences design. We show that breach frequency declines after adoption, with the largest reduction in the first post-adoption year. We interpret this evidence cautiously because VDP adoption is not random. The delayed reduction in breaches is in line with an operational learning mechanism in which external reports identify latent defects and prompt remediation.

Finally, the value of a VDP depends on the organizational capacity to act on external information. The breach-reducing association is stronger when institutional investors and blockholders sustain managerial attention, when boards possess firm-specific knowledge, and when formal risk or cybersecurity committees are absent. These results suggest that external detection and internal remediation are distinct but interdependent elements of operational reliability.

This paper makes three contributions. First, it extends the literature on software vulnerability management from the design of individual disclosure, inspection, patching, and bounty decisions to the firm-level establishment of an external vulnerability-discovery process. Prior research examines disclosure timing, patching and maintenance decisions, and the design of bug bounty programs, including how rewards and disclosure rules influence external discovery, internal security effort, and software-release decisions (Arora et al., 2008; Sen et al., 2020; Mookerjee & Samuel, 2023; Zhang et al., 2024; Gal-Or et al., 2026; Zhou & Hui, 2026). We distinguish our study by examining the firm-level adoption of a standing external vulnerability-discovery process and its operational and informational value. This change in unit of analysis allows us to examine adoption determinants, subsequent realized breach outcomes, and organizational conditions associated with implementation.

Second, we distinguish external problem detection from internal problem resolution. Research on external problem solving, innovation contests, and distributed search shows that firms can benefit from external knowledge when addressing uncertain technical problems (Terwiesch & Xu, 2008; Jeppesen & Lakhani, 2010; Boudreau et al., 2011). In conventional innovation contests, outsiders commonly generate candidate solutions. In a VDP, outsiders primarily generate verified problem information, while the focal firm retains responsibility for evaluating reports, remediating vulnerabilities, and learning from identified defects. We therefore extend this literature from external solution generation to external problem detection and show why external discovery and internal execution operate as complementary processes.

Third, we connect real operational value and information value. Operations event studies show that supply chain glitches and information-security failures destroy shareholder value (Hendricks & Singhal, 2003; Modi et al., 2015). The informational meaning of a VDP is theoretically ambiguous because external participation can indicate either limitations in internal detection or confidence in the firm's ability to withstand scrutiny and act on reported defects. We examine how investors resolve this ambiguity when a failure occurs. By combining stock-market reactions with subsequent breach frequency, we distinguish whether VDPs alter beliefs about response capability from whether they are associated with fewer realized failures. This joint test is distinct from studies of failure consequences alone and from vulnerability-management models that do not observe firm-level market and operating outcomes.

The findings offer practical implications for operations managers. The findings indicate that a VDP should not be treated as a communications policy or stand-alone technology initiative. Its value depends on the operating process that receives reports, prioritizes vulnerabilities, assigns remediation responsibility, and verifies closure. Firms can therefore improve the value of VDPs by integrating them with incident response, software development, supplier management, and board-level risk oversight.

## 2. Literature Review and Theoretical Background

We position the paper at the intersection of operational failures, vulnerability management, and external problem detection. Prior research has examined vulnerability disclosure policies, disclosure timing, patch incentives, security-system maintenance, and bug-bounty design (Kannan & Telang, 2005; Arora et al., 2008; Kim et al., 2011; Sen et al., 2020; Bensoussan et al., 2020;

Mookerjee & Samuel, 2023; Zhang et al., 2024). A related stream documents the financial consequences of operational and cybersecurity failures, including supply-chain disruptions and data breaches (Hendricks & Singhal, 2003; Gatzlaff & McCullough, 2010; Modi et al., 2015; Kamiya et al., 2021; Jeong et al., 2025). We distinguish our study by examining the firm-level adoption of a standing external vulnerability-discovery process rather than individual disclosure, patching, inspection, or bounty decisions. This shift in the unit of analysis allows us to study whether establishing such a process is associated with subsequent realized breaches at the firm level. We further investigate whether the existence of a VDP changes the information conveyed to investors when a cyberattack occurs. Prior research has examined these operational and financial consequences largely in isolation. By studying both within the same setting, we assess the operational value of external vulnerability discovery as well as its information value when failures occur.

We consequently review three connected literature streams. The first examines vulnerability disclosure, patching, and security maintenance decisions. The second focuses on operational failures and their information value. The third studies external problem detection and the organizational process required to translate external knowledge into operational response and remediation.

### 2.1. Vulnerability Disclosure and Security Maintenance

Research on software vulnerability management has primarily examined decisions made after a vulnerability is discovered or under uncertainty about system condition. Kannan and Telang (2005) compare market-based and intermediary mechanisms for acquiring vulnerability information. Arora et al. (2008) model how disclosure policy affects vendor patch timing and quality. Kim et al. (2011) study patch release and software liability as mechanisms for improving security quality. Sen et al. (2020) investigate the discoverer's disclosure-timing decision and show that perceptions of producer patch responsiveness influence delayed disclosure. Bensoussan et al. (2020) and Mookerjee and Samuel (2023) model maintenance and inspection decisions when security deterioration or vulnerability is imperfectly observed. More recent research analyzes the design and governance of bug bounty programs. Zhang et al. (2024) examine how bounty design depends on security posture, patching complexity, researcher heterogeneity, and legal protection. In addition, Gal-Or et al. (2026) investigate how bug bounty programs influence vulnerability discovery, disclosure, remediation, and software-release decisions, while Zhou and Hui (2026)

study how bounty programs affect hacker behavior and the interaction between external discovery and firms' internal security effort.

These studies show that vulnerability management involves a set of interrelated operational choices concerning information disclosure, inspection, patching, researcher incentives, and the allocation of effort between external discovery and internal security. Our study differs in four distinct aspects. First, the unit of analysis is the adopting firm rather than an individual vulnerability, discoverer, software product, or modeled decision-maker. Second, we study the establishment of a standing organizational process for external vulnerability discovery rather than the design of a particular disclosure, patching, inspection, or bounty decision. Third, we observe realized firm-level breach outcomes following adoption. Fourth, we examine whether the existence of this process changes the information conveyed to investors when a subsequent breach occurs. The paper therefore complements recent analytical work on the design and governance of vulnerability-discovery programs by providing firm-level empirical evidence on adoption, realized operational outcomes, and capital-market information.

The distinction between vulnerability discovery and vulnerability disclosure is important in our setting. Disclosure models typically begin after a vulnerability has been identified and analyze how information should move between the discoverer, the vendor, users, and potential attackers. A VDP operates one step earlier by influencing whether and where discovery effort occurs. The program communicates that external search is authorized within specified boundaries and that the firm has created a route for receiving the resulting information. Adoption can therefore affect both the supply of vulnerability information and the organizational process through which that information is handled.

### 2.2. Operational Failures and Information Value

Operational failures reveal information about a firm's underlying process reliability and recovery capability. Hendricks and Singhal (2003) are among the first who show that supply chain glitch announcements generate substantial negative shareholder returns. Modi et al. (2015) provide evidence that customer information-security breaches create value losses in service triads, demonstrating that a focal firm's operational failure can impose consequences across interorganizational relationships. Jeong et al. (2025) further show that cyber vulnerability is chained across internal and external actors. Kumar and Mallipeddi (2022) identify cybersecurity

as a key operations and supply-chain research domain. These studies establish cyber incidents as operational events rather than isolated technology failures.

Cyberattacks can interrupt production and service delivery, compromise customer-facing processes, and propagate through suppliers or digital infrastructure providers. The market response to a breach therefore reflects both the direct cost of exposed information and investors' assessment of operating-system reliability, managerial preparedness, and expected recovery costs. A VDP can change this assessment in opposing ways. On one side, inviting external researchers may reveal that internal engineers, audits, or security controls cannot identify all relevant defects. Investors could interpret adoption as evidence of latent vulnerability, insufficient internal expertise, or unusually high risk exposure. On the other side, a firm that voluntarily opens itself to external scrutiny may signal confidence, transparency, and a formal commitment to detect and remediate weaknesses before they are exploited. A VDP does not indicate that the firm cannot be hacked or that it is immune from attack. It indicates that the firm has created a recognized channel through which external security researchers, commonly referred to as friendly hackers, can report vulnerabilities for internal remediation.

These competing interpretations make the informational value of a VDP theoretically ambiguous. A program may expose limitations in internal detection, reassure investors about preparedness, or convey both signals at once. Its market interpretation may also differ from its real operational value. A VDP could reassure investors without reducing failures, or reduce failures without providing a sufficiently visible or credible signal to investors. We therefore examine both stock-market reactions and subsequent breach frequency rather than assuming that VDP adoption is inherently favorable information.

The ambiguity is especially relevant when investors observe a subsequent breach. If program adoption primarily reveals weak internal detection, a breach may confirm that the firm's systems were vulnerable despite seeking outside assistance. Under this interpretation, the program could intensify the negative signal. If adoption instead indicates that the firm has anticipated the possibility of defects and established routines for receiving and remediating them, the same breach may be viewed as less informative about managerial unpreparedness. Investors may expect faster containment, lower recurrence, and a more credible response. We therefore use information from stock-market reactions to examine whether a pre-existing operating process changes how investors interpret a realized failure, rather than whether it signals immunity from attack.

### 2.3. External Problem Detection and Operational Remediation

Cyber risk detection alone does not create operational value for the firm. Reports must be screened, prioritized, assigned, fixed, and verified. VDP effectiveness therefore depends on the firm's ability to absorb external technical information and integrate it into software-development, and risk-management routines. A similar logic appears in near-miss management, where reporting creates value only when the information leads to remediation (Bakshi & Peura, 2022). We therefore conceptualize VDP effectiveness as the firm's ability to convert externally generated vulnerability information into effective remediation and operational learning. The firm establishes reporting rules, legal safe harbor, communication channels, and sometimes financial rewards, while external researchers self-select into searching for vulnerabilities. Prior research on broadcast search and innovation contests shows that access to a larger and more diverse group of external contributors can increase the likelihood of identifying effective solutions to uncertain technical problems (Terwiesch & Xu, 2008; Jeppesen & Lakhani, 2010; Boudreau et al., 2011). In a VDP, however, the primary output is information about a latent operational defect rather than a completed product or technical solution.

From an operations perspective, VDPs extend quality-control activities beyond the firm by incorporating externally generated information about digital vulnerabilities. Traditional quality systems place inspection at selected points within the production process. A VDP adds an external inspection layer that can operate continuously and from the perspective of a motivated adversary. The mechanism is particularly relevant for software because releases are frequent, components are interconnected, and the possible attack surface changes as systems, suppliers, and user behavior evolve. Internal testing remains necessary, but its coverage can be complemented by distributed search after deployment.

### 2.4. An Operational Information-Processing View

The operational value of external vulnerability discovery can be understood as a sequence of linked information-processing stages. The first stage is search. Program rules define which assets may be tested, which methods are permitted, and how researchers can submit findings. These choices influence who participates and which parts of the digital operation receive attention. A broad search boundary may increase discovery coverage, but it can also produce more low-value or duplicative reports. The program therefore creates an operating design problem rather than a

simple decision to accept or reject outside assistance. Firms must balance the benefits of wider search against the capacity required to process the resulting information.

The second stage is translation and triage. External reports must be converted into information that internal teams can evaluate and act on. This requires validating whether a vulnerability can be reproduced, determining which products and processes are affected, assessing severity, and identifying the responsible owner. Breakdowns at this interface can prevent technically valuable discoveries from producing operational value. A report may be accurate but remain unresolved because it lacks context, crosses organizational boundaries, or competes with product-release and uptime priorities. Program quality therefore depends partly on the interface between external researchers and the internal units that control remediation resources.

The third stage is response and learning. Firms may address identified vulnerabilities through code changes, configuration changes, access controls, supplier coordination, customer communication, or the redesign of development and testing routines. Resolving individual reports can reduce immediate exposure, while patterns across reports may also inform broader improvements in operating routines. This perspective provides a common interpretation for the organizational conditions examined later in the paper. External monitoring can sustain attention to unresolved reports, firm-specific knowledge can improve technical interpretation and coordination, and a program can have greater marginal value when formal oversight structures are absent. These conditions do not replace external vulnerability discovery. They influence whether reported vulnerabilities are effectively addressed by the firm.

This process view also clarifies the paper's empirical claims. We observe the establishment of the reporting mechanism and subsequent firm-level outcomes, but we do not observe individual reports, triage decisions, or remediation tasks, as these activities involve highly sensitive security information and are generally not publicly disclosed. The analyses therefore examine whether adoption is followed by outcomes that reflect effective information processing within the firm. Lower subsequent breach frequency would suggest real operational value, while a less adverse market response to a later breach would suggest information value. Examining both outcomes helps distinguish a program that is merely visible from one that is associated with changes in realized reliability, without assuming that adoption alone proves the quality of the underlying routines.

## 3. Hypothesis Development

### 3.1. VDP Adoption and Operational Risk Reduction

We expect VDP adoption to reduce cybersecurity risk by expanding the firm's capacity to identify vulnerabilities before they are exploited. Internal security teams face limits in time, expertise, and familiarity with every component of increasingly complex digital operations. Prior research shows that access to a larger and more diverse group of external contributors can increase the likelihood of identifying solutions to uncertain technical problems because contributors differ in knowledge, experience, and search approaches (Terwiesch & Xu, 2008; Jeppesen & Lakhani, 2010; Boudreau et al., 2011). A VDP extends this logic to vulnerability discovery by allowing external researchers to search for defects that may remain undetected through internal monitoring alone. VDPs also affect how vulnerability information reaches the firm. Without a recognized reporting channel, external researchers may remain silent, disclose vulnerabilities publicly, or communicate through channels that do not reach the responsible internal unit. A formal VDP establishes where vulnerabilities should be reported and provides clearer rules for communication, legal protection, and, in some programs, financial rewards.

Receiving such information alone, however, does not reduce operational risk. The firm must evaluate reported vulnerabilities and resolve the underlying defects. A VDP therefore expands external detection, while its operational value depends on the firm's ability to act on the information it receives. When identified vulnerabilities are successfully addressed, fewer exploitable weaknesses should remain, reducing the likelihood of subsequent data breaches. This process also suggests that the effect may emerge after adoption rather than immediately. External researchers require time to identify and report vulnerabilities, while firms require time to evaluate and resolve them. The initial period following adoption may offer particularly strong opportunities for risk reduction because external researchers can identify vulnerabilities that were already present when the program was introduced.

Moreover, operational frictions can weaken this process. Incoming reports may be incomplete, duplicative, or difficult to evaluate. Addressing vulnerabilities also competes with product development, system availability, and other operating priorities, while some problems require coordination across business units or external suppliers. A formal program does not eliminate these constraints, but it creates a structured channel through which externally identified vulnerabilities

can reach the firm and be addressed. We therefore expect VDP adoption to be associated with fewer subsequent data breaches.

*H1: Firms that adopt VDPs experience fewer subsequent data breaches than firms that do not adopt such programs.*

### 3.2. External Monitoring and VDP Effectiveness

The argument underlying H1 implies that VDP adoption alone is insufficient to reduce breach risk. External vulnerability information creates operational value only when the firm devotes sufficient attention and resources to addressing reported weaknesses. Yet remediation involves immediate costs, while its benefits arise through the avoidance of uncertain future losses. Managers may therefore delay or underinvest in addressing vulnerabilities, particularly when security demands compete with product development, system availability, and other operating priorities.

External monitoring can strengthen this implementation process by increasing managerial accountability and sustaining attention to unresolved cyber risks. Institutional investors and blockholders have strong incentives to monitor cybersecurity because major breaches can disrupt operations, generate financial losses, and reduce firm value (Kamiya et al., 2021; Lending et al., 2018). Prior research also shows that institutional investors can discourage managerial short-termism, while concentrated owners have stronger incentives and greater ability to influence managerial and board decisions (Bushee, 1998; Desender et al., 2013; Aguilera et al., 2015).

These monitoring incentives are particularly relevant after VDP adoption. A formal reporting channel can bring previously unidentified vulnerabilities into the organization, but management still determines how quickly they receive attention and whether resources are allocated to resolve them. Investors with significant ownership stakes can increase pressure for stronger cyber-risk management and reduce the likelihood that reported vulnerabilities remain a low-priority technical issue. External monitoring may therefore strengthen the firm's ability to convert vulnerability information into lower operational risk. Accordingly, we expect the association between VDP adoption and subsequent breach frequency to be stronger when external monitoring is greater.

*H2: The negative relationship between VDP adoption and subsequent data breach occurrence is stronger in firms with higher levels of external monitoring.*

### 3.3. Board Capability and VDP Effectiveness

External monitoring can increase attention to vulnerability information, but effective implementation also depends on the firm's ability to interpret that information and coordinate a response. VDPs can generate technically complex reports that cut across information technology, software development, legal, communications, and operating units. Board characteristics may therefore influence whether externally identified vulnerabilities receive sufficient attention, are understood in the context of the firm's operations, and are addressed effectively. Research on board gender diversity suggests that female directors can broaden board deliberation, strengthen attention to risk-related issues, and increase transparency and cybersecurity oversight (Bear et al., 2010; Nielsen & Huse, 2010; Radu & Smaili, 2022). In the context of a VDP, greater attention to cyber risk may increase the likelihood that reported vulnerabilities are escalated and addressed rather than remaining within technical functions.

Firm-specific knowledge may also matter for the effective use of externally generated vulnerability information. Inside directors possess greater familiarity with the firm's systems, decision rights, and operating processes. Prior research suggests that such internal knowledge can strengthen board oversight of technically complex and firm-specific risks, while Lending et al. (2018) document a lower risk of financial data breaches when boards have stronger inside representation. In a VDP setting, this knowledge may help directors assess the operational implications of reported vulnerabilities and facilitate coordination across the units responsible for addressing them. Director tenure provides another source of firm-specific knowledge. Board capital theory emphasizes that directors accumulate human and social capital through their experience with the firm (Hillman & Dalziel, 2003). Longer-tenured directors are therefore likely to possess greater knowledge of organizational routines, technology investments, and prior risk-management decisions. This accumulated knowledge may improve their ability to interpret vulnerability information and manage the organizational response to identified cyber risks. We therefore expect the association between VDP adoption and subsequent breach frequency to be stronger when boards possess greater capacity to sustain attention, interpret firm-specific information, and support coordination across the organization.

*H3: The negative relationship between VDP adoption and subsequent data breach occurrence is stronger in firms with (H3a) more female directors, (H3b) more inside directors, and (H3c) greater director tenure.*

### 3.4. Formal Risk Structures and VDP Effectiveness

The preceding arguments suggest that the operational value of a VDP depends partly on the firm's existing capacity to identify, escalate, and address cyber risks. Dedicated risk or cybersecurity committees can provide specialized attention, clearer responsibility, and more structured coordination around these activities. Firms without such structures may therefore have less developed internal processes for detecting and escalating vulnerabilities.

In this setting, a VDP can fill a larger operational gap. By introducing an external source of vulnerability information and a formal reporting channel, the program can strengthen detection and create a clearer path through which identified weaknesses enter the organization. When dedicated risk or cybersecurity committees are already in place, these functions are more likely to be supported by existing risk-management structures. VDPs may still contribute additional information, but their incremental effect on breach risk should be smaller. This substitution logic therefore predicts that the association between VDP adoption and subsequent breach frequency is stronger when formal internal risk structures are absent. Accordingly, we hypothesize that:

*H4: The negative association between VDP adoption and subsequent data breach occurrence is stronger in firms without a dedicated risk or cybersecurity committee, and weaker in firms with such formal oversight structures.*

## 4. Data and Methodology

### *4.1 Sample Construction and Data Sources*

We construct a novel firm-level dataset of VDP adoption among publicly listed U.S. firms from 2010 to September 2025. Because no comprehensive database identifies when public firms establish VDPs, we manually collect adoption information from HackerOne and Bugcrowd and supplement these records with information from firms' official websites. We combine the resulting VDP dataset with cyber event data from the Privacy Rights Clearinghouse (PRC) Chronology of Data Breaches and Harry and Gallagher (2018), firm financial data from Compustat, board characteristics from BoardEx, ownership data from LSEG, and stock price data from CRSP. The sample period begins in 2010, the earliest year for which we identify VDP adoption. Because financial data were available only through 2024 when the study was initiated, the empirical analyses subsequently cover the period from 2010 to 2024.

### *4.2. Main Variables*

#### *4.2.1. Vulnerability Disclosure Program*

We gathered program-level data from HackerOne and Bugcrowd, two leading platforms through which firms publicly host and manage VDPs and external security researchers identify programs in which to participate. For firms that did not list programs on these platforms, or where program details were incomplete, we supplemented the data with information collected directly from company websites.

We initially identify 404 public firms that launched VDPs between 2010 and September 2025. Table 1 presents the distribution of VDP adoption by program type, bounty status, industry (SIC division), and launch year. Because VDPs differ in whether they offer financial rewards to external researchers, we control for bounty status in the subsequent analyses. In our sample, 108 firms (26.73%) operate a bounty program, while 296 firms (73.27%) do not. By industry, the largest groups are services (185 firms, 45.79%) and manufacturing (107 firms, 26.49%). Launches are concentrated between 2020 and 2024, with the highest number in 2020 (65 firms, 16.09%), reflecting the recent growth of VDP adoption.[1]

[Insert Table 1 About Here]

#### *4.2.2. Cyber Events*

Cyber events data was collected from the Privacy Rights Clearinghouse (PRC) Chronology of Data Breaches and Harry and Gallagher (2018). We use the PRC Chronology as our primary source of cyber event data, following prior studies that rely on this database and facilitating comparability with established empirical work on data breaches (e.g., Kamiya et al., 2021; Huang & Wang, 2021; Lending et al., 2018). We supplement these records with the cyber event data compiled by Harry and Gallagher (2018). The PRC Chronology compiles publicly reported breach notifications from U.S. government agencies and provides information on affected organizations, breach types, compromised information, and reporting dates. By standardizing and clustering multiple notifications of the same event, the Chronology offers structured access to otherwise fragmented

[1] The program sample is broader than the samples used in the outcome analyses because the empirical tests require additional firm and time-series information. Programs launched near the end of the collection period cannot provide a complete multi-year post-adoption window, and firms differ in the availability of accounting, ownership, board, breach, and market data. We therefore report the relevant observation counts for each analysis rather than treating the 404 identified programs as a single balanced estimation sample.

public records, supporting research, risk analysis, policy development, and investigative reporting.[2]

Since we do not have access to the updated release of PRC data and only have data available from 2005 through February 2023, we need to supplement them with the Cyber Events Database from Harry and Gallagher (2018). They first automatically scan public sources such as news websites, blogs, and cybersecurity portals using Python scripts to find possible events. All potential events are then manually checked to make sure they meet the database's definition of a cyber event. Verified events are finally merged with key information, including attack type, target sector, attacker motivation, and breach details. This approach ensures that the Cyber Events Database has broad, accurate, and long-term record of cyber incidents for research purposes.[3]

Combining the two sources increases the coverage of observed cyber events. More generally, both databases capture reported events, so the dependent variable reflects observed breach incidence rather than every underlying intrusion. Reporting practices may vary across firms and over time, and firms with stronger security processes may detect or disclose incidents more readily. To the extent that VDP adoption increases detection or transparency, such reporting differences would work against finding a decline in recorded breaches after adoption. Changes in disclosure regulation, reporting requirements, or media attention may also affect the number of observed events independently of underlying security performance. Year fixed effects absorb common changes over time, e.g. due to economy-wide shocks or trends.

#### *4.2.3. Other variables*

We include a set of firm, governance, and market level control variables following Kamiya et al. (2021). *Firm Size* captures the scale of operations and is measured as the natural logarithm of total assets. *Asset Intangibility* reflects the proportion of intangible assets to total assets. *R&D Intensity* (*R&D/Assets*) and *Capital Expenditure Intensity* (*CAPX/Assets*) measure investment in innovation and physical capital, respectively. *Return on Assets* (*ROA*) serves as an indicator of profitability, while *Tobin's Q* proxies for growth opportunities and market valuation relative to assets. *Leverage* accounts for financial risk, and *Sales Growth* captures firm expansion dynamics. *Financial Constraint* is included as a binary indicator to capture whether a firm faces relatively limited access to external financial resources. Financially constrained firms may have fewer

[2] https://privacyrights.org/data-breaches
[3] https://www.cissm.umd.edu/cyber-events-database

resources available to invest in cybersecurity infrastructure, monitor vulnerabilities, and remediate identified security weaknesses. We therefore control for financial constraints because differences in firms' financial capacity may affect both their decision to adopt a VDP and their ability to translate vulnerability information into effective remediation. We also control for market-related performance and risk measures, including *Stock Performance* and *Stock Volatility*, which may influence both exposure to and response to cyber events. Ownership and governance are captured through *Blockholder Ownership*, the *Number of Board Committees*, and the presence of a *Risk* Committee (indicator), reflecting formal risk management capacity. Appendix A1 provides a detailed description of all variables.

Descriptive statistics are reported in Table 2 separately for firm-year observations with and without a VDP from 2010 to 2024. Observations with missing values for any of the variables used in the analysis are excluded. The sample includes 979 firm-year observations with a VDP and 30,908 firm-year observations without a VDP. Firm size, ROA, and Tobin's Q ratio are on average higher for firm-year observations with a VDP. These firms likewise exhibit higher asset intangibility, greater R&D to assets ratio, and higher leverage, but lower capital expenditure to assets ratio and stock volatility. In terms of governance, firms with VDPs exhibit higher blockholder ownership and more board committees. The differences in means and medians are statistically significant for most variables, suggesting systematic differences between firm-year observations with a VDP and those without. These differences motivate the use of matching in the subsequent panel analysis to improve comparability between adopting and non-adopting firms.

[Insert Table 2 About Here]

### 4.3. Empirical Strategy and Identification Considerations

The empirical analyses address three related questions. The adoption regressions describe which firms establish VDPs. The event study examines whether a pre-existing VDP is associated with a different stock-market response when a breach is disclosed. The matched panel analysis examines whether breach frequency changes after adoption relative to similar firms that have not adopted a program. These analyses provide complementary evidence, but they rely on different samples and identify different relationships.

The principal identification challenge is that VDP adoption is a managerial choice. Firms may adopt as part of a broader cybersecurity investment, after an internal review, in response to

regulation, or because managers anticipate changing exposure. Matching reduces differences in observed firm characteristics, and firm fixed effects absorb stable unobserved differences, but neither approach removes time-varying adoption motives. We therefore interpret the panel estimates as evidence suggestive of a risk-reduction effect. The timing analysis helps assess the proposed mechanism by examining whether the effect emerges only after reports have been received and acted upon rather than immediately in the adoption year.

The stock-market reaction analysis addresses a different identification issue. The univariate comparisons establish whether market reactions differ between firms with and without a pre-existing VDP, but they do not isolate the program from all event- and firm-level characteristics. We therefore interpret these results as evidence on the presence and direction of information value rather than as causal estimates of the market effect of VDP adoption. Narrower event windows reduce the likelihood that estimated market reactions capture unrelated corporate news, following the approach commonly used in cyberattack event studies (e.g., Kamiya et al., 2021).

## 5. Results

### *5.1. Firm Characteristics and VDP Adoption*

We examine which firms are more likely to adopt a VDP by estimating logistic regressions with a binary variable for VDP adoption as dependent variable. All control variables are lagged by one year so that firm characteristics are measured before the VDP adoption decision. Results are reported in Table 3. In Column (1), we only include firm fundamentals. We add stock-related variables in Column (2) and further add governance characteristics in Column (3). We control for year and industry fixed effects across these three specifications. In Column (4), we include firm fundamentals and industry indicator variables for Finance Industry, Service Industry, and Transportation, Communication and Electronic Industry, while controlling year fixed effects.

Across all specifications, firm size is significantly positive, indicating that larger firms are more likely to adopt a VDP. R&D intensity is likewise consistently positive and significant at the 1% level, indicating that more innovation-oriented firms are more likely to implement a VDP. In addition, asset intangibility becomes positive and significant in column (4), suggesting that firms with more intangible assets, whose value likely be more vulnerable to cyber risks, are more inclined to adopt a VDP. Performance and growth opportunities also matter. ROA and Tobin's Q are significantly positive across all models, indicating that more profitable firms and firms with

stronger growth prospects are more likely to launch a VDP. In contrast, sales growth is significantly negative in several specifications, suggesting that rapidly expanding firms may delay adoption, possibly due to competing resource demands. In columns (2) and (3), stock volatility is positive and significant, indicating that firms facing higher market uncertainty are more likely to implement a VDP. Industry patterns are reported in Column (4), where industry fixed effects are replaced with specific industry indicators. Firms in the service and wholesale and retail sectors are significantly more likely to adopt a VDP, while financial service firms are less likely to do so. The lower adoption rate among financial service providers is particularly interesting given their substantial exposure to cyber risk. It also accords with earlier industry evidence showing relatively limited adoption of public vulnerability disclosure programs among financial institutions.[4]

Overall, the results suggest that VDP adoption is more common among large, innovative, profitable firms with strong growth opportunities and greater exposure to intangible assets and market risk.

[Insert Table 3 About Here]

### 5.2. The Information Value of VDPs Following Data Breaches

A VDP discloses that a firm has established a process for receiving external vulnerability information, but its informational meaning is not necessarily perceived positively. Dependence on outside researchers may reveal incomplete internal detection, while voluntary scrutiny and a formal remediation channel may indicate preparedness. These competing interpretations imply that the expected market response cannot be signed ex ante. We therefore examine whether a breach conveys more or less adverse information when the affected firm has a VDP.

Following established event-study applications in prior research (e.g., Ba et al., 2013; Xia et al., 2016), we measure investor responses around breach disclosure dates using cumulative abnormal returns (CAR). Market-model parameters are estimated over 220 trading days from day -280 to day -61 relative to the breach disclosure, using the CRSP equal-weighted return as the market benchmark. CARs are calculated over the event windows [-1,1], [-2,2], and [-5,5]. The shorter windows capture the market response close to the disclosure date, while the wider window

[4] HackerOne's 2018 Hacker-Powered Security Report found that only 4% of financial-services firms in the Forbes Global 2000 had vulnerability disclosure policies. https://www.hackerone.com/blog/118-fascinating-facts-hackerones-hacker-powered-security-report-2018.

allows for information leakage or delayed investor response but is more exposed to unrelated news. We also examine abnormal trading volume (AVOL) as a complementary measure of investor response. Following DellaVigna and Pollet (2009), among others, abnormal volume is calculated as the difference between the logarithm of actual trading volume and the logarithm of expected trading volume, where expected volume is the average over the estimation window [-280,-61].

Table 4 reports stock-market reactions to data breach events and compares firms with and without existing VDPs. For the full sample, cumulative abnormal returns are significantly negative across all event windows, while abnormal trading volume is significantly positive. This results is in line with prior research showing that cyber incidents destroy shareholder value and attract investor attention (Modi et al., 2015; Kamiya et al., 2021). However, we find that the negative market reaction is concentrated among firms without VDPs. These firms experience significant stock-price declines and elevated trading volume. In contrast, firms with VDPs do not experience significantly negative returns in the shorter windows, and their trading-volume response is statistically insignificant. Because Table 4 is univariate, these results should be interpreted as evidence of information value rather than as a causal estimate of the market effect of VDP adoption. The results provide an empirical resolution of the competing interpretations in this sample. Investors appear to place greater weight on the view that a pre-existing VDP reflects preparedness and a structured process for detecting, triaging, and remediating vulnerabilities than on the view that outside participation reveals internal weakness. A breach at such a firm may therefore convey less adverse information about underlying operational preparedness. This interpretation remains cautious because the analysis cannot directly observe investor beliefs. As the [-5,5] window is also more exposed to confounding announcements, the shorter windows provide the cleaner evidence.

[Insert Table 4 About Here]

The finding should not imply that investors view VDP adoption as evidence of low vulnerability. A realized breach demonstrates that a vulnerability that could potentially have been identified through the firm's external disclosure process was instead exploited by a malicious actor. We interpret the weaker market reaction as suggestive evidence that a pre-existing VDP changes the information conveyed by that failure. When a firm has already established a formal channel through which friendly hackers can identify and report vulnerabilities, the occurrence of a breach may reveal less adverse information about its preparedness to respond than an otherwise

comparable breach at a firm without such a process. The finding therefore indicates that a pre-existing VDP carries information value when an operational failure occurs. It concerns the conditional interpretation of a realized breach in the presence of an existing VDP, rather than an unconditional valuation effect of program adoption.

### 5.3. VDP Adoption and Subsequent Breaches

Next, we use propensity-score matching to identify a control firm that does not have VDP for each treated firm. We calculate the propensity score using the logit regression of *VDP Indicator* on *Firm Size*, *R&D/Assets*, *ROA*, *Tobin's Q*, *Sales Growth*, and *Stock Volatility*, the factors shown to affect VDP adoption decision in Table 3. Following Kamiya et al. (2021), we require both treated and matched control firms to belong to the same industry, as measured by two-digit SIC codes, since Table 1 shows that VDP adoption is heavily concentrated in a few industries. We also match treated and control firms within the same fiscal year, assigning the control firm an "artificial" adoption year following Chan et al. (2013) and Kamiya et al. (2021). This approach allows us to account for contemporaneous changes in firm characteristics and corporate policies around the time of VDP adoption. Finally, each treated firm is matched to a single control firm without replacement, using the nearest propensity score within a 0.1 caliper and a 0.1 to 0.9 common support (Caliendo & Kopeinig, 2008; Kamiya et al., 2021).

Panel A of Table 5 shows the distribution of 168 matched firms by adoption year, 84 treated firms and 84 control firms. The sample ranges from 2011 to 2021, with most firms concentrated in 2020 (36.9%) and 2021 (26.2%). Panel B of Table 5 presents the descriptive statistics of treated firms and control firms. We find no significant differences between treated firms and their matched controls, indicating that our matching procedure successfully pairs firms with similar characteristics.

Next, we estimate a difference-in-differences specification around staggered VDP adoption:

$$y_{i,t} = \alpha + \beta VDP_{i,t} \times Post_{i,t} + \gamma X_{i,t-1} + \mu_i + \lambda_t + \varepsilon_{i,t} \quad (1)$$

where $y_{i,t}$ represents breach count for firm $i$ at year $t$. $Post_{i,t}$ is an indicator equal to 1 for firm-years after the adoption of VDP (year $t$+1, year $t$+2, and year $t$+3) and 0 otherwise (year $t$, year $t$-1, year $t$-2, and year $t$-3), where year $t$ is the year when a firm adopts VDP. $VDP_{i,t}$ is an indicator

equal to 1 for firms that adopt a VDP (treated firms) and 0 otherwise. The coefficient of the interaction term $VDP_{i,t} \times Post_{i,t}$ captures the post-adoption difference between treated and matched control firms. $X_{i,t-1}$ is a vector of lagged control variables, including the variables *Firm Size*, *R&D/Assets*, *ROA*, *Tobin's Q*, *Sales Growth*, and *Stock Volatility*. All specifications include firm fixed effects ($\mu_i$) to control for time-invariant firm characteristics and year fixed effects ($\lambda_t$) to capture economy-wide shocks or trends.

To capture the dynamic effect of VDP on cyber events, we follow Kamiya et al. (2021) and Huang and Wang (2021) to break down the interaction term between $VDP_{i,t}$ and $Post_{i,t}$, as follows:

$$y_{i,t} = \alpha + \beta_1 VDP_{i,t} \times Year\ 0 + \beta_2 VDP_{i,t} \times Year\ 1 + \beta_3 VDP_{i,t} \times Year\ 2 + +\gamma X_{i,t-1} + \mu_i + \lambda_t + \varepsilon_{i,t} \quad (2)$$

where *Year 0* denotes the year of VDP adoption, *Year 1* refers to the first year following adoption, and *Year 2+* represents the second and third years after adoption (with the years prior to VDP adoption as the benchmark period). Since we controlled for firm and year fixed effects, we do not include the main effects of *VDP* and year dummies (Huang & Wang, 2021).

Panel C of Table 5 reports the results. In Column (1), the coefficient on *VDP* × *Post* is significantly negative (-0.126), indicating that breach frequency declines after VDP adoption relative to the matched control firms. Column (2) examines the timing of the association. The coefficient for *Year 1* is negative and statistically significant, while the adoption-year coefficient is insignificant and the *Year 2+* coefficient remains negative but is not statistically significant. The delayed onset may reflect the time required to receive reports, triage vulnerabilities, and complete remediation.

We next split the sample into firms in the service industry (SIC = 73) and all other industries, given that VDPs are disproportionately concentrated in the service sector. Results are presented in Columns (3) to (6). The findings suggest that the risk-mitigation effect of VDPs is stronger in the service industry than in other industries, both in magnitude and statistical significance. One possible explanation is that service firms tend to rely heavily on digital infrastructure and collect large volumes of customer data. As a result, they may face greater exposure to cybersecurity threats and stronger stakeholder expectations regarding data protection. In such environments, VDPs might play a more important role in identifying vulnerabilities and supporting risk reduction. Consequently, the adoption of VDPs appears to provide greater risk-reduction benefits for service firms than for firms operating in other industries.

[Insert Table 5 About Here]

Overall, these results support Hypothesis 1. VDP adoption is associated with a decline in breach frequency, with the strongest reduction in the first year after implementation. Matching and firm and year fixed effects reduce observable and time-invariant differences between treated and control firms, but they do not eliminate selection on time-varying cybersecurity investments or adoption motives. We therefore interpret the estimates as suggestive evidence of a risk-reduction effect rather than definitive causal evidence.

The concentration of the reduction in the first post-adoption year may reflect a front-loaded learning effect. Early reports may reveal a backlog of latent defects or recurring weaknesses that can be corrected across multiple systems. As these issues are addressed, the marginal benefit of additional reports may decline, or the remaining vulnerabilities may be more difficult to remediate. The insignificant *Year 2+* estimate does not establish that the program ceases to create value. It rather indicates that the available matched sample does not provide a precise estimate of a persistent average reduction beyond the first year.

### 5.4. Organizational Conditions for Converting External Reports into Remediation

We next examine the organizational conditions under which external vulnerability information is converted into fewer breaches. These analyses provide evidence on whether managerial attention, firm-specific knowledge, and existing risk structures affect the implementation of the VDP process.

#### *5.4.1. External Monitoring and Remediation Attention*

We examine whether VDP effectiveness depends on external monitoring, measured using institutional and blockholder ownership. External monitors may increase managerial attention to remediation because reported vulnerabilities require immediate expenditure while their benefits arise through avoided future losses.

Panel A of Table 6 splits firms by the median value of institutional ownership in the sample. The results show a clear asymmetry. Among firms with high institutional ownership, the coefficient on *VDP* × *Post* is significantly negative (-0.259), whereas the effect is economically small and statistically insignificant in firms with low institutional ownership (-0.029). The dynamic specifications further reinforce this pattern. In high institutional ownership firms, breach frequency declines significantly beginning in *Year 1* (-0.329) and persists in *Year 2+* (-0.380). No

such pattern emerges in the low institutional ownership subsample. These findings suggest that VDP adoption is associated with substantive reductions in breach frequency only when supported by strong external monitoring. Institutional investors, who are typically long-term oriented and sensitive to reputational and regulatory risk, may pressure management to address disclosed vulnerabilities rather than allow reports to remain unresolved. Panel B of Table 6 presents results based on blockholder ownership. The breach-reducing association is again concentrated in firms with high blockholder ownership. The dynamic results indicate that the reduction in breaches becomes particularly pronounced in *Year 2+*, with a statistical significant coefficient of -0.314, suggesting that concentrated owners may facilitate sustained implementation rather than short-term adjustments.

[Insert Table 6 About Here]

#### *5.4.2. Board Knowledge and Coordination Capacity*

We next examine whether board monitoring efficiency affects the effectiveness of VDP adoption. Specifically, we split the sample by board gender diversity, the proportion of executive directors, and board director tenure, respectively.

Panel A of Table 7 examines whether the effect of VDP adoption on breach risk varies with board gender diversity. In Columns (1) and (2), the coefficient on *VDP* × *Post* lacks significance for firms with low gender diversity but significantly negative for firms with high gender diversity (-0.353). The dynamic estimates show the same pattern. We find that for firms with high gender diversity, the coefficient for *VDP* × *Year 1* is significantly negative (-0.483) but remains insignificant for firms with low board gender diversity. These results suggest that greater board gender diversity is associated with a stronger relationship between VDP adoption and improved cybersecurity outcomes. One possible explanation is that gender-diverse boards place more relevance on risk management, transparency, and stakeholder protection, which may support more effective implementation of VDPs.

[Insert Table 7 About Here]

Panel B of Table 7 shows that the reduction in breach counts is mainly observed among firms with relatively more inside directors, whereas no significant effect can be found among firms with fewer inside directors. Dynamic results indicate sustained reductions in *Year 1* and *Year 2+* within the higher-inside-director subsample. One interpretation based on board capital theory is that

directors with deeper firm-specific involvement may better understand internal IT architecture and operating processes, supporting more effective responses to reported vulnerabilities. Although board independence remains important in broader governance settings, the results indicate that firm-specific knowledge may be particularly relevant when firms must respond to technically complex cybersecurity issues. Panel C of Table 7 further supports the firm-specific expertise mechanism. The breach-reducing effect of VDPs is statistically significant only in firms with longer director tenure. Dynamic estimates indicate that reductions emerge in *Year 1* and remain thereafter. Long-tenured directors may accumulate contextual knowledge that improves their ability to evaluate technical risk disclosures and oversee remediation processes. This pattern suggests that cybersecurity governance is not merely a matter of formal oversight but of informed oversight.

Overall, the results support Hypothesis 3, as VDP effectiveness is stronger among firms whose boards appear better able to sustain attention, interpret firm-specific technical information, and coordinate remediation. Because these tests use median splits, they should be viewed as exploratory boundary-condition evidence rather than precise estimates of nonlinear effects.

#### *5.4.3. VDPs and Formal Risk Structures*

Finally, we examine whether VDPs substitute for the absence of formal risk management structures, as indicated by whether a firm has a risk committee or a cyber-related committee. Following Kamiya et al. (2021), we classify a risk committee when the committee name includes the word "risk." Similarly, we identify a cyber committee when the committee name, obtained from BoardEx, includes terms such as "cyber," "information system," "data privacy," "cybersecurity," "digital," or "technology".

Panel A of Table 8 shows that the breach-reducing effect of VDPs is primarily observed among firms without a risk committee, whereas no significant reduction is observed among firms that maintain a formal risk committee. Dynamic results indicate reductions beginning in *Year 1* and continuing in *Year 2+* for firms with no formal cyber committee. This pattern suggests that VDPs serve as an external mechanism that partially compensates for the absence of formal internal oversight structures. Panel B of Table 8 yields a similar pattern. VDP adoption significantly reduces breaches in firms without a dedicated cyber committee, whereas the effect is statistically insignificant in firms with such committees. The results suggest that VDPs can serve as a

functional substitute for specialized risk management structures. In firms that already maintain formal cyber risk structures, the incremental benefit of VDP adoption appears more limited.

[Insert Table 8 About Here]

## 6. Conclusions

This paper examines whether VDPs create operational and information value by integrating friendly hackers into a formal external vulnerability-discovery process. The informational meaning of VDPs is not obvious. Inviting outsiders may expose limitations in internal detection, while voluntary external scrutiny may indicate confidence, transparency, and preparedness. The market evidence shows that the negative stock-market response to a breach is primarily observed among firms without VDPs. Investors therefore appear to place greater weight on the preparedness interpretation when evaluating a realized failure. The operational evidence provides a complementary result. VDP adoption is associated with fewer subsequent breaches, with the strongest reduction occurring in the first post-adoption year. The association is also stronger under organizational conditions associated with greater external monitoring, board attention and firm-specific knowledge, and the absence of formal risk or cybersecurity committees.

The paper differs from the closest vulnerability-management literature. Prior studies examine disclosure deadlines, disclosure timing, patch release, inspection, security maintenance, and bounty design (Arora et al., 2008; Kim et al., 2011; Sen et al., 2020; Bensoussan et al., 2020; Mookerjee & Samuel, 2023; Zhang et al., 2024). We instead study firm-level adoption of a standing external detection process. This analysis allows us to examine adoption, subsequent realized failures, capital-market interpretation, and implementation conditions within one empirical setting.

Our main contribution is that firms can improve reliability by opening their problem-detection boundary. Research on external search explains why outside contributors can help address difficult technical problems. Our setting introduces an important distinction. External researchers identify limitations, while the firm retains responsibility for evaluating reports, resolving vulnerabilities, and learning from identified weaknesses. External discovery and internal execution are therefore complementary. This logic is also relevant for product-safety reporting, supplier defect alerts, near-miss systems, and other settings in which outsiders observe latent operational problems.

The paper also contributes to research on the capital-market consequences of operational failures. Prior studies show that operational failures lower shareholder value. We show that a process established before a failure can alter the information conveyed by that failure. A VDP may reveal incomplete internal detection, but it may also demonstrate a credible willingness and process to address weaknesses. Market reactions and subsequent operational outcomes capture distinct dimensions of VDP value, allowing us to separate the information conveyed by the process from its association with realized reliability.

Several limitations define the scope of the findings. VDP adoption is endogenous, and the available data do not directly measure report volume, vulnerability severity, response time, or closure quality. The difference-in-differences estimates therefore cannot fully separate VDP adoption from concurrent cybersecurity investments. The event-study comparisons are univariate and may reflect differences in breach severity or confounding news, especially in wider event windows. Future research should use program-level data on bounty design, participation, response time, and remediation outcomes and examine how internal security capacity interacts with external discovery. Such data would allow more direct tests of the process linking external reports to operational reliability.

For managers, the findings imply that the value of a VDP depends less on launching the program than on the firm's ability to act on the vulnerability information it receives. A formal reporting channel can widen external detection capacity, but the operational benefits appear stronger when organizational conditions support attention, firm-specific interpretation, and implementation. VDPs should therefore be viewed as part of a broader operational process rather than as stand-alone disclosure initiatives. Firms that effectively connect external vulnerability discovery with internal response processes may be better positioned to reduce breach risk and may also be perceived as better prepared when failures occur. The market evidence also has implications for how firms communicate VDPs. Rather than presenting these programs as evidence of invulnerability, firms should emphasize preparedness, openness to good-faith external reporting, and the ability to respond when vulnerabilities are identified.

The findings also contribute to a broader view of operational transparency. Firms may hesitate to invite external scrutiny because it exposes deficiencies and increases the flow of issues requiring attention. In digital operations, however, opacity does not remove latent defects and may instead delay their discovery until vulnerabilities are exploited. A VDP formalizes a trade-off between the

cost of receiving and processing adverse information and the benefit of identifying weaknesses before they result in more damaging failures. Conditional on a breach, our stock-market evidence suggests that investors may value the existence of an established process for receiving and addressing such information.

The study further distinguishes resilience from immunity. No vulnerability-disclosure process can guarantee that a firm will avoid attack. The information value of a VDP therefore does not arise from communicating invulnerability. Rather, a pre-existing VDP may indicate that the firm has established a process for receiving and responding to vulnerability information before a failure occurs. This interpretation accords with the less adverse market response observed for firms with VDPs and the delayed reduction in subsequent breaches.

For operations theory, the setting further broadens the role of external search. VDPs show that external contributors can generate diagnostic information about hidden defects. This creates a different allocation of work in which outsiders identify and document problems while insiders retain responsibility for resolution. The value of this arrangement therefore depends on the firm's ability to act on externally generated vulnerability information. Reporting rules, acknowledgment procedures, severity assessment, and responsibility for resolution are part of the operating process through which external discovery may improve reliability.

**References**


Aguilera, R. V., K. A. Desender, M. K. Bednar, J. H. Lee. 2015. Connecting the dots: Bringing external corporate governance into the corporate governance puzzle. Academy of Management Annals 9(1), 483–573. 10.1080/19416520.2015.1024503

Arora, A., R. Telang, H. Xu. 2008. Optimal policy for software vulnerability disclosure. Management Science 54(4), 642-656. https://doi.org/10.1287/mnsc.1070.0771

Ba, S., L. L. Lisic, Q. Liu, J. Stallaert. 2013. Stock market reaction to green vehicle innovation. Production and Operations Management 22(4), 976–990. 10.1111/j.1937-5956.2012.01387.x

Bakshi, N., H. Peura. 2022. Prevent or report? Managing near misses for safer operations. Manufacturing & Service Operations Management 24(4), 2064-2080. https://doi.org/10.1287/msom.2022.1100

Bear, S., N. Rahman, C. Post. 2010. The impact of board diversity and gender composition on corporate social responsibility and firm reputation. Journal of Business Ethics 97(2), 207–221. 10.1007/s10551-010-0505-2

Bensoussan, A., V. S. Mookerjee, W. T. Yue. 2020. Managing information system security under continuous and abrupt deterioration. Production and Operations Management 29(8), 1894-1917. https://doi.org/10.1111/poms.13198

Boudreau, K. J., N. Lacetera, K. R. Lakhani. 2011. Incentives and problem uncertainty in innovation contests: An empirical analysis. Management Science 57(5), 843-863. https://doi.org/10.1287/mnsc.1110.1322

Bushee, B. J. 1998. The influence of institutional investors on myopic R&D investment behavior. The Accounting Review 73(3), 305–333.

Caliendo, M., S. Kopeinig. 2008. Some practical guidance for the implementation of propensity score matching. Journal of Economic Surveys 22(1), 31-72. https://doi.org/10.1111/j.1467-6419.2007.00527.x

Chan, L. H., K. C. W. Chen, T.-Y. Chen. 2013. The effects of firm-initiated clawback provisions on bank loan contracting. Journal of Financial Economics 110(3), 659-679. https://doi.org/10.1016/j.jfineco.2013.08.010

DellaVigna, S., J. M. Pollet. 2009. Investor inattention and Friday earnings announcements. Journal of Finance 64(2), 709-749. https://doi.org/10.1111/j.1540-6261.2009.01447.x

Desender, K. A., R. V. Aguilera, R. Crespi, M. García-Cestona. 2013. When does ownership matter? Board characteristics and behavior. Strategic Management Journal 34(7), 823–842. 10.1002/smj.2046

Gal-Or, E., M. Z. Hydari, R. Telang. 2026. Merchants of vulnerabilities: How bug bounty programs benefit software vendors. Production and Operations Management. Advance online publication. https://doi.org/10.1177/10591478261448668

Gatzlaff, K. M., K. A. McCullough. 2010. The effect of data breaches on shareholder wealth. Risk Management and Insurance Review 13(1), 61–83. 10.1111/j.1540-6296.2010.01178.x

Harry, C., N. Gallagher. 2018. Classifying cyber events: A proposed taxonomy. Journal of Information Warfare 17(3), 17-31. https://www.jstor.org/stable/26633158

Hendricks, K. B., V. R. Singhal. 2003. The effect of supply chain glitches on shareholder wealth. Journal of Operations Management 21(5), 501-522. https://doi.org/10.1016/j.jom.2003.02.003

Hillman, A. J., T. Dalziel. 2003. Boards of directors and firm performance: Integrating agency and resource dependence perspectives. Academy of Management Review 28(3), 383–396. 10.5465/amr.2003.10196729

Huang, H. H., C. Wang. 2021. Do banks price firms' data breaches? The Accounting Review 96(3), 261-286. https://doi.org/10.2308/TAR-2018-0643

Jeong, S., Z. Rogers, T. Y. Choi. 2025. Strange dance partners: Supply chain cyberattacks and chained vulnerability. Journal of Operations Management 71(6), 763-785. https://doi.org/10.1002/joom.1374

Jeppesen, L. B., K. R. Lakhani. 2010. Marginality and problem-solving effectiveness in broadcast search. Organization Science 21(5), 1016-1033. https://doi.org/10.1287/orsc.1090.0491

Kamiya, S., J.-K. Kang, J. Kim, A. Milidonis, R. M. Stulz. 2021. Risk management, firm reputation, and the impact of successful cyberattacks on target firms. Journal of Financial Economics 139(3), 719-749. https://doi.org/10.1016/j.jfineco.2019.05.019

Kannan, K., R. Telang. 2005. Market for software vulnerabilities? Think again. Management Science 51(5), 726-740. https://doi.org/10.1287/mnsc.1040.0357

Kim, B. C., P.-Y. Chen, T. Mukhopadhyay. 2011. The effect of liability and patch release on software security: The monopoly case. Production and Operations Management 20(4), 603-617. https://doi.org/10.1111/j.1937-5956.2010.01189.x

Kumar, S., R. R. Mallipeddi. 2022. Impact of cybersecurity on operations and supply chain management: Emerging trends and future research directions. Production and Operations Management 31(12), 4488-4500. https://doi.org/10.1111/poms.13859

Lending, C., K. Minnick, P. J. Schorno. 2018. Corporate governance, social responsibility, and data breaches. Financial Review 53(2), 413-455. https://doi.org/10.1111/fire.12160

Modi, S. B., M. A. Wiles, S. Mishra. 2015. Shareholder value implications of service failures in triads: The case of customer information security breaches. Journal of Operations Management 35, 21-39. https://doi.org/10.1016/j.jom.2014.10.003

Mookerjee, R., J. Samuel. 2023. Managing the security of information systems with partially observable vulnerability. Production and Operations Management 32(9), 2902-2920. https://doi.org/10.1111/poms.14015

Nielsen, S., M. Huse. 2010. The contribution of women on boards of directors: Going beyond the surface. Corporate Governance: An International Review 18(2), 136–148. 10.1111/j.1467-8683.2010.00784.x

Radu, C., N. Smaili. 2022. Board gender diversity and corporate response to cyber risk: Evidence from cybersecurity related disclosure. Journal of Business Ethics 177(2), 351–374. 10.1007/s10551-020-04717-9

Sen, R., J. Choobineh, S. Kumar. 2020. Determinants of software vulnerability disclosure timing. Production and Operations Management 29(11), 2532-2552. https://doi.org/10.1111/poms.13120

Terwiesch, C., Y. Xu. 2008. Innovation contests, open innovation, and multiagent problem solving. Management Science 54(9), 1529-1543. https://doi.org/10.1287/mnsc.1080.0884

Xia, Y., V. R. Singhal, G. P. Zhang. 2016. Product design awards and the market value of the firm. Production and Operations Management 25(6), 1038–1055. 10.1111/poms.1252

Zhang, L., E. M. Demirezen, S. Kumar. 2024. How to make my bug bounty cost-effective? A game-theoretical model. Information Systems Research 36(2), 1031-1053. https://doi.org/10.1287/isre.2021.0349

Zhou, J., K.-L. Hui. 2026. Crowdsourcing from hackers: Strategic coopetition and governance in bug bounty programs. Management Science. Articles in Advance. https://doi.org/10.1287/mnsc.2022.02682

**Table 1: Distribution of VDP**

| Variable | Category | N | Percent(%) |
|---|---|---|---|
| Bounty | No | 296 | 73.27 |
| | Yes | 108 | 26.73 |
| SIC Division | Services | 185 | 45.79 |
| | Manufacturing | 107 | 26.49 |
| | Finance, Insurance and Real estate | 56 | 13.86 |
| | Wholesale and Retail Trade | 31 | 7.67 |
| | Transportation, Communications, Electric, Gas | 24 | 5.94 |
| | Nonclassifiable | 1 | 0.25 |
| Launch Year | 2010 | 1 | 0.25 |
| | 2011 | 2 | 0.50 |
| | 2012 | 2 | 0.50 |
| | 2013 | 2 | 0.50 |
| | 2014 | 8 | 1.98 |
| | 2015 | 16 | 3.96 |
| | 2016 | 10 | 2.48 |
| | 2017 | 15 | 3.71 |
| | 2018 | 19 | 4.70 |
| | 2019 | 23 | 5.69 |
| | 2020 | 65 | 16.09 |
| | 2021 | 45 | 11.14 |
| | 2022 | 57 | 14.11 |
| | 2023 | 48 | 11.88 |
| | 2024 | 58 | 14.36 |
| | 2025 (Till Q3) | 33 | 8.17 |
| Total | | 404 | 100 |

*Note:* This table summarizes the manually collected vulnerability disclosure programs from January 2010 to September 2025.

## Table 2: Descriptive Statistics

| | Firm-years with VDP (N=979): A | | Firm-years without VDP (N=30,908): B | | Test of Difference (A-B) | |
|---|---|---|---|---|---|---|
| Variable | Mean | Median | Mean | Median | Mean | Median |
| Firm Size | 9.135 | 9.139 | 7.03 | 7.107 | 2.105*** | 2.031*** |
| Asset Intangibility | 0.851 | 0.901 | 0.785 | 0.879 | 0.066*** | 0.022*** |
| R&D/Assets | 0.063 | 0.041 | 0.049 | 0 | 0.014*** | 0.041*** |
| CAPX/Assets | 0.024 | 0.018 | 0.034 | 0.02 | -0.010*** | -0.002 |
| ROA | 0.019 | 0.035 | -0.032 | 0.019 | 0.051*** | 0.015*** |
| Tobin's Q | 3.47 | 2.611 | 2.065 | 1.435 | 1.405*** | 1.176*** |
| Leverage | 0.673 | 0.665 | 0.592 | 0.581 | 0.081*** | 0.084*** |
| Sales Growth | 1.144 | 1.089 | 1.156 | 1.058 | -0.013 | 0.031*** |
| Financial Constraint (Indicator) | 0.225 | 0 | 0.284 | 0 | -0.059*** | 0.000*** |
| Stock Performance | 0.031 | -0.041 | -0.003 | -0.071 | 0.034 | 0.031*** |
| Stock Volatility | 0.027 | 0.024 | 0.031 | 0.025 | -0.004*** | -0.001*** |
| Blockholder Ownership | 0.25 | 0.233 | 0.226 | 0.219 | 0.024*** | 0.014*** |
| Number of Board Committees | 4.08 | 4 | 3.816 | 3 | 0.264*** | 1.000*** |
| Risk Committee (Indicator) | 0.134 | 0 | 0.094 | 0 | 0.039*** | 0.000*** |

*Note:* This table summarizes 979 firm-year observations with VDPs (282 unique firms) and 30,908 firm-year observations without VDPs (4,479 unique firms) from January 2010 to December 2024. We report t-tests (Wilcoxon z-tests) for differences in means (medians) of firm and industry characteristics between firms with and without VDPs. All continuous variables are winsorized at 1st and 99th. Definitions of all variables are provided in Table A1. Superscripts ***, **, and * indicate significance at 1%, 5%, and 10% levels, respectively.

**Table 3: Logistic Regression Analysis of VDP Adoption**

| | (1) VDP Indicator | (2) VDP Indicator | (3) VDP Indicator | (4) VDP Indicator |
|---|---|---|---|---|
| Firm Size | 0.938*** | 0.970*** | 0.957*** | 0.857*** |
| | (14.877) | (14.845) | (14.670) | (15.357) |
| Asset Intangibility | 1.329 | 1.313 | 1.346 | 2.908*** |
| | (1.541) | (1.537) | (1.558) | (4.037) |
| R&D/Assets | 5.849*** | 5.828*** | 5.780*** | 5.389*** |
| | (6.881) | (6.919) | (6.973) | (7.443) |
| CAPX/Assets | -0.730 | -0.798 | -0.738 | 4.160 |
| | (-0.197) | (-0.218) | (-0.203) | (1.376) |
| ROA | 1.194*** | 1.397*** | 1.401*** | 1.822*** |
| | (2.743) | (3.236) | (3.282) | (4.206) |
| Tobin's Q | 0.132*** | 0.138*** | 0.137*** | 0.160*** |
| | (6.449) | (6.499) | (6.574) | (9.148) |
| Leverage | 0.359 | 0.348 | 0.347 | 0.215 |
| | (1.317) | (1.292) | (1.278) | (0.757) |
| Sales Growth | -0.113 | -0.165 | -0.165* | -0.235** |
| | (-1.138) | (-1.619) | (-1.659) | (-2.523) |
| Financial Constraint (Indicator) | -0.134 | -0.170 | -0.156 | -0.016 |
| | (-0.774) | (-0.964) | (-0.881) | (-0.099) |
| Stock Performance | | -0.056 | -0.059 | |
| | | (-0.720) | (-0.763) | |
| Stock Volatility | | 10.687** | 10.619** | |
| | | (2.127) | (2.143) | |
| Institutional Blockholder | | | -0.435 | |
| | | | (-0.877) | |
| Number of Board Committees | | | 0.031 | |
| | | | (0.451) | |
| Risk Committee (Indicator) | | | -0.087 | |
| | | | (-0.308) | |
| Finance Industry | | | | -1.099*** |
| | | | | (-3.693) |
| Service Industry | | | | 1.657*** |
| | | | | (8.038) |
| Tran, Com, Elec Industry | | | | -0.030 |
| | | | | (-0.086) |
| Wholesale, Retail Industry | | | | 0.896*** |
| | | | | (2.946) |
| Constant | -17.501*** | -18.046*** | -18.002*** | -17.795*** |
| | (-11.277) | (-11.502) | (-11.336) | (-15.341) |
| Year FE | Yes | Yes | Yes | Yes |
| Industry FE | Yes | Yes | Yes | No |
| N | 27326 | 27326 | 27326 | 31887 |
| Pseudo R2 | 0.459 | 0.460 | 0.460 | 0.393 |

*Note:* This table presents results of logit regression in which the dependent variable is an indicator that takes the value one if a firm has VDP in a given year, and zero otherwise. The sample covers 979 firm-year observations with VDPs (282 unique firms) and 30,908 firm-year observations without VDPs (4,479 unique firms) from January 2010 to December 2024. All explanatory variables are measured one year before the dependent variable. Standard errors are clustered at the firm level. Superscripts ***, **, and * indicate significance at 1%, 5%, and 10% levels, respectively.

**Table 4: Univariable Analysis: The Role of VDP in the Stock Market Reaction to Cyber Events**

| | | (1) | (2) | (3) | (1) | (2) | (3) |
|---|---|---|---|---|---|---|---|
| | # Cyber events | | CAR(%) | | | AVOL | |
| | (# distinct firm) | [-1,1] | [-2,2] | [-5,5] | [-1,1] | [-2,2] | [-5,5] |
| All Firms: | 713 (580) | -0.423*** | -0.413** | -0.561** | 0.087*** | 0.079*** | 0.064*** |
| | | (-2.902) | (-2.277) | (-2.137) | (3.907) | (3.756) | (3.268) |
| No VDP: | 644 (554) | -0.447*** | -0.463** | -0.759*** | 0.095*** | 0.088*** | 0.073*** |
| | | (-2.853) | (-2.360) | (-2.683) | (3.955) | (3.848) | (3.481) |
| With VDP: | 69 (49) | -0.199 | 0.055 | 1.285** | 0.016 | 0.001 | -0.027 |
| | | (-0.550) | (0.136) | (2.205) | (0.282) | (0.012) | (-0.659) |
| *With Bounty:* | 36 (17) | -0.719 | -0.324 | 1.231* | 0.032 | 0.008 | -0.027 |
| | | (-1.578) | (-0.644) | (1.861) | (0.504) | (0.154) | (-0.567) |
| *No Bounty:* | 33 (32) | 0.368 | 0.468 | 1.344 | -0.002 | -0.008 | -0.028 |
| | | (0.655) | (0.741) | (1.353) | (-0.022) | (-0.095) | (-0.396) |

*Note:* This table presents univariate results of cumulative abnormal returns (CAR) and average abnormal trading volume (AVOL) for firms around cyberattack disclosure dates, the comparison of these estimates between firms with VDP and those without. The sample consists of 713 cyberattacks (580 unique firms) from January 2010 to December 2024. The abnormal stock returns are calculated using the market model, where market model parameters are estimated using 220 trading days of return data beginning 280 days before and ending 61 days before the breach disclosure, using the CRSP equal-weighted return as a proxy for the market return, following Kamiya et al. (2021). The cumulative abnormal stock return (CAR) is the sum of daily abnormal stock returns from day $t_1$ before the breach disclosure date to day $t_2$ after the breach disclosure date. We calculate abnormal trading volume based on the method outlined by DellaVigna and Pollet (2009). It is defined as the natural logarithm of the actual trading volume minus the natural logarithm of the expected trading volume, where expected volume is the average volume over the estimation window [-280, -61]. Standard errors are clustered at the firm level. Superscripts ***, **, and * indicate significance at 1%, 5%, and 10% levels, respectively.

**Table 5: The Effect of VDP Adoption on Data Breaches**

***Panel A: Distribution of Matched Firms by Year***

| Year | N | Percent |
|---|---|---|
| 2011 | 2 | 1.19 |
| 2014 | 6 | 3.57 |
| 2015 | 10 | 5.95 |
| 2017 | 6 | 3.57 |
| 2018 | 16 | 9.52 |
| 2019 | 22 | 13.10 |
| 2020 | 62 | 36.90 |
| 2021 | 44 | 26.19 |
| Total | 168 | 100.00 |

***Panel B: Difference in Variables for firms Matched by PSM (Number of Observations: 168)***

| Variable | Treated (N=84) | Control (N=84) | Diff. | P-value |
|---|---|---|---|---|
| Firm Size | 8.429 | 8.35 | 0.079 | 0.776 |
| R&D/Assets | 0.08 | 0.065 | 0.015 | 0.205 |
| ROA | -0.01 | 0.003 | -0.014 | 0.517 |
| Tobin's Q | 4.203 | 4.185 | 0.018 | 0.975 |
| Sales Growth | 1.197 | 1.151 | 0.046 | 0.427 |
| Stock Volatility | 0.03 | 0.031 | -0.001 | 0.689 |

**Table 5 (continued): The Effect of VDP Adoption on Data Breaches**

***Panel C: Relation Between VDP and Data Braches***

| | (1) | (2) | (3) | (4) | (5) | (6) |
|---|---|---|---|---|---|---|
| | All Industries | | Service Industry (SIC=73) | | Other Industries | |
| | Breach Count | Breach Count | Breach Count | Breach Count | Breach Count | Breach Count |
| VDP # Post | -0.126** | | -0.156* | | -0.097* | |
| | (-2.262) | | (-1.700) | | (-1.753) | |
| VDP # Year 0 | | -0.033 | | -0.140 | | 0.111 |
| | | (-0.379) | | (-1.075) | | (1.033) |
| VDP # Year 1 | | -0.153** | | -0.235* | | -0.060 |
| | | (-2.045) | | (-1.815) | | (-1.013) |
| VDP # Year 2+ | | -0.131 | | -0.214 | | -0.048 |
| | | (-1.589) | | (-1.550) | | (-0.655) |
| Firm Size | 0.024 | 0.022 | -0.005 | -0.002 | 0.065 | 0.073 |
| | (0.492) | (0.457) | (-0.075) | (-0.024) | (0.758) | (0.863) |
| R&D/Assets | -0.389 | -0.412 | 0.065 | 0.010 | -1.874 | -1.696 |
| | (-0.950) | (-1.016) | (0.145) | (0.023) | (-1.589) | (-1.573) |
| ROA | 0.075 | 0.075 | 0.494* | 0.486* | -0.532 | -0.543 |
| | (0.364) | (0.358) | (1.921) | (1.882) | (-1.349) | (-1.370) |
| Tobin's Q | 0.002 | 0.002 | -0.002 | -0.001 | 0.056** | 0.054** |
| | (0.190) | (0.204) | (-0.262) | (-0.133) | (2.366) | (2.372) |
| Sales Growth | -0.015 | -0.017 | 0.027 | 0.015 | -0.120* | -0.112* |
| | (-0.210) | (-0.233) | (0.276) | (0.153) | (-1.909) | (-1.706) |
| Stock Volatility | -0.465 | -0.510 | -0.265 | -0.407 | -2.781 | -2.742 |
| | (-0.187) | (-0.203) | (-0.077) | (-0.117) | (-0.853) | (-0.839) |
| Constant | 0.004 | 0.028 | 0.197 | 0.217 | -0.307 | -0.419 |
| | (0.010) | (0.063) | (0.343) | (0.367) | (-0.357) | (-0.494) |
| N | 1003 | 1003 | 575 | 575 | 428 | 428 |
| R-squared | 0.279 | 0.279 | 0.301 | 0.304 | 0.282 | 0.285 |
| Firm & Year FE | Yes | Yes | Yes | Yes | Yes | Yes |

*Note:* This table presents descriptive statistics for 84 treated firms that have adopted a VDP and 84 control firms that do not adopt a VDP from 2011 to 2021 and panel regression in which the dependent variables are breach frequency. The propensity score is calculated using the logit regressions of *VDP indicator* (equal 1 for firm-years with VDP and 0 otherwise) on *Firm Size*, *R&D/Assets*, *ROA*, *Tobin's Q*, *Sales Growth* and *Stock Volatility*. The matching procedure pairs treated firms with control firms in the same industry (the same two-digit SIC codes) and the same fiscal year. Panel C covers 1,003 firm-year observations (three years before and after the adoption year). *Post* is an indicator that takes the value one for post-attack period (year t+1, year t+2, and year t+3), and zero otherwise, where year *t* is the VDP adoption year. Standard errors are clustered at the firm level. Superscripts ***, **, and * indicate significance at 1%, 5%, and 10% levels, respectively.

**Table 6: External Monitoring Complementarity**

Panel A: Institutional Investor Percentage

| | (1) Low Inst | (2) High Inst | (3) Low Inst | (4) High Inst |
|---|---|---|---|---|
| VDP # Post | -0.029 | -0.259*** | | |
| | (-0.336) | (-2.796) | | |
| VDP # Year 0 | | | 0.141 | -0.225 |
| | | | (1.262) | (-1.358) |
| VDP # Year 1 | | | -0.010 | -0.329** |
| | | | (-0.118) | (-2.320) |
| VDP # Year 2+ | | | 0.091 | -0.380** |
| | | | (0.882) | (-2.586) |
| Constant | 0.379 | -0.353 | 0.348 | -0.252 |
| | (0.458) | (-0.492) | (0.413) | (-0.346) |
| N | 478 | 419 | 478 | 419 |
| R-squared | 0.343 | 0.308 | 0.348 | 0.317 |
| Firm Controls | Yes | Yes | Yes | Yes |
| Firm & Year FE | Yes | Yes | Yes | Yes |

Panel B: Blockholder Ownership Percentage

| | (1) Low Block | (2) High Block | (3) Low Block | (4) High Block |
|---|---|---|---|---|
| VDP # Post | -0.068 | -0.193** | | |
| | (-0.796) | (-2.048) | | |
| VDP # Year 0 | | | 0.034 | -0.157 |
| | | | (0.251) | (-0.918) |
| VDP # Year 1 | | | -0.090 | -0.213 |
| | | | (-0.967) | (-1.430) |
| VDP # Year 2+ | | | -0.014 | -0.314** |
| | | | (-0.116) | (-2.079) |
| Constant | 0.459 | -0.933 | 0.463 | -0.957 |
| | (0.676) | (-1.090) | (0.683) | (-1.114) |
| N | 445 | 446 | 445 | 446 |
| R-squared | 0.358 | 0.331 | 0.359 | 0.337 |
| Firm Controls | Yes | Yes | Yes | Yes |
| Firm & Year FE | Yes | Yes | Yes | Yes |

*Note:* This table presents results of panel regression for 84 treated firms that have adopted a VDP and 84 control firms that do not adopt a VDP from 2011 to 2021 in which the dependent variables are breach frequency. The sample covers seven firm-year observations from three years before to three years after the adoption year for each firm, from 2008 to 2024. Firm controls include *Firm Size*, *R&D/Assets*, *ROA*, *Tobin's Q*, *Sales Growth* and *Stock Volatility*. *Post* is an indicator that takes the value one for post-attack period (year t+1, year t+2, and year t+3), and zero otherwise, where year *t* is the VDP adoption year. Standard errors are clustered at the firm level. Superscripts ***, **, and * indicate significance at 1%, 5%, and 10% levels, respectively.

## Table 7: Board Monitoring Efficiency

***Panel A: Board Gender Diversity***

| | (1) Low Diversity | (2) High Diversity | (3) Low Diversity | (4) High Diversity |
|---|---|---|---|---|
| VDP # Post | -0.050 | -0.353** | | |
| | (-0.696) | (-2.453) | | |
| VDP # Year 0 | | | 0.058 | -0.148 |
| | | | (0.495) | (-0.844) |
| VDP # Year 1 | | | -0.017 | -0.483** |
| | | | (-0.211) | (-2.167) |
| VDP # Year 2+ | | | -0.018 | -0.335 |
| | | | (-0.190) | (-1.508) |
| Constant | -0.025 | -1.154 | -0.070 | -1.105 |
| | (-0.034) | (-1.169) | (-0.094) | (-1.127) |
| N | 545 | 391 | 545 | 391 |
| R-squared | 0.385 | 0.336 | 0.386 | 0.342 |
| Firm Controls | Yes | Yes | Yes | Yes |
| Firm & Year FE | Yes | Yes | Yes | Yes |

***Panel B: Board Inside Directors***

| | (2) Less Director | (1) More Director | (4) Less Director | (3) More Director |
|---|---|---|---|---|
| VDP # Post | -0.069 | -0.149*** | | |
| | (-0.665) | (-2.912) | | |
| VDP # Year 0 | | | -0.018 | -0.033 |
| | | | (-0.114) | (-0.351) |
| VDP # Year 1 | | | -0.103 | -0.173** |
| | | | (-0.813) | (-2.041) |
| VDP # Year 2+ | | | -0.057 | -0.158** |
| | | | (-0.401) | (-2.086) |
| Constant | 0.646 | -0.097 | 0.698 | -0.092 |
| | (0.696) | (-0.233) | (0.771) | (-0.217) |
| N | 391 | 549 | 391 | 549 |
| R-squared | 0.330 | 0.346 | 0.330 | 0.347 |
| Firm Controls | Yes | Yes | Yes | Yes |
| Firm & Year FE | Yes | Yes | Yes | Yes |

**Table 7 (continued): Board Monitoring Efficiency**

***Panel C: Board Director Tenure***

| | (1) Shorter Tenure | (2) Longer Tenure | (3) Shorter Tenure | (4) Longer Tenure |
|---|---|---|---|---|
| VDP # Post | -0.000 | -0.206*** | | |
| | (-0.005) | (-2.719) | | |
| VDP # Year 0 | | | -0.032 | 0.004 |
| | | | (-0.286) | (0.029) |
| VDP # Year 1 | | | -0.027 | -0.200** |
| | | | (-0.242) | (-2.316) |
| VDP # Year 2+ | | | -0.007 | -0.208* |
| | | | (-0.058) | (-1.777) |
| Constant | -0.097 | 0.353 | -0.077 | 0.351 |
| | (-0.151) | (0.264) | (-0.115) | (0.264) |
| N | 455 | 497 | 455 | 497 |
| R-squared | 0.353 | 0.336 | 0.354 | 0.336 |
| Firm Controls | Yes | Yes | Yes | Yes |
| Firm & Year FE | Yes | Yes | Yes | Yes |

*Note:* This table presents results of panel regression for 84 treated firms that have adopted a VDP and 84 control firms that do not adopt a VDP from 2011 to 2021 in which the dependent variables are breach frequency. The sample covers seven firm-year observations from three years before to three years after the adoption year for each firm, from 2008 to 2024. Firm controls include *Firm Size*, *R&D/Assets*, *ROA*, *Tobin's Q*, *Sales Growth* and *Stock Volatility*. *Post* is an indicator that takes the value one for post-attack period (year t+1, year t+2, and year t+3), and zero otherwise, where year *t* is the VDP adoption year. Standard errors are clustered at the firm level. Superscripts ***, **, and * indicate significance at 1%, 5%, and 10% levels, respectively.

**Table 8: Governance Substitution Effects**

Panel A: Firms Without a Risk Committee

| | (1) No Risk Committee | (2) Has Risk Committee | (3) No Risk Committee | (4) Has Risk Committee |
|---|---|---|---|---|
| VDP # Post | -0.172*** | 0.161 | | |
| | (-3.274) | (0.735) | | |
| VDP # Year 0 | | | -0.038 | 0.225 |
| | | | (-0.398) | (0.789) |
| VDP # Year 1 | | | -0.203** | 0.299 |
| | | | (-2.501) | (1.454) |
| VDP # Year 2+ | | | -0.178* | 0.230 |
| | | | (-1.922) | (1.050) |
| Constant | -0.090 | 0.277 | -0.061 | 0.073 |
| | (-0.209) | (0.124) | (-0.143) | (0.033) |
| N | 806 | 158 | 806 | 158 |
| R-squared | 0.309 | 0.367 | 0.309 | 0.374 |
| Firm Controls | Yes | Yes | Yes | Yes |
| Firm & Year FE | Yes | Yes | Yes | Yes |

Panel B: Firms Without a Cyber Committee

| | (1) No Cyber Committee | (2) Has Cyber Committee | (3) No Cyber Committee | (4) Has Cyber Committee |
|---|---|---|---|---|
| VDP # Post | -0.108*** | -0.093 | | |
| | (-3.339) | (-1.068) | | |
| VDP # Year 0 | | | 0.065 | -0.252 |
| | | | (1.162) | (-1.695) |
| VDP # Year 1 | | | -0.077** | -0.256 |
| | | | (-1.994) | (-1.510) |
| VDP # Year 2+ | | | -0.081** | -0.278 |
| | | | (-1.993) | (-1.610) |
| Constant | -0.246 | 3.872 | -0.265 | 3.155 |
| | (-0.792) | (1.699) | (-0.845) | (1.391) |
| N | 851 | 114 | 851 | 114 |
| R-squared | 0.293 | 0.571 | 0.295 | 0.597 |
| Firm Controls | Yes | Yes | Yes | Yes |
| Firm & Year FE | Yes | Yes | Yes | Yes |

*Note:* This table presents results of panel regression for 84 treated firms that have adopted a VDP and 84 control firms that do not adopt a VDP from 2011 to 2021 in which the dependent variables are breach frequency. The sample covers seven firm-year observations from three years before to three years after the adoption year for each firm, from 2008 to 2024. Firm controls include *Firm Size*, *R&D/Assets*, *ROA*, *Tobin's Q*, *Sales Growth* and *Stock Volatility*. *Post* is an indicator that takes the value one for post-attack period (year t+1, year t+2, and year t+3), and zero otherwise, where year *t* is the VDP adoption year. Standard errors are clustered at the firm level. Superscripts ***, **, and * indicate significance at 1%, 5%, and 10% levels, respectively.