



Strategy Science

Publication details, including instructions for authors and subscription information:
<http://pubsonline.informs.org>

Learning from Digital Failures? The Effectiveness of Firms' Divestiture and Management Turnover Responses to Data Breaches

GuiDeng Say, Gurneeta Vasudeva

To cite this article:

GuiDeng Say, Gurneeta Vasudeva (2020) Learning from Digital Failures? The Effectiveness of Firms' Divestiture and Management Turnover Responses to Data Breaches. *Strategy Science* 5(2):117-142. <https://doi.org/10.1287/stsc.2020.0106>

This work is licensed under a Creative Commons Attribution 4.0 International License. You are free to copy, distribute, transmit and adapt this work, but you must attribute this work as "*Strategy Science*. Copyright © 2020 The Author(s). <https://doi.org/10.1287/stsc.2020.0106>, used under a Creative Commons Attribution License: <https://creativecommons.org/licenses/by/4.0/>."

Copyright © 2020 The Author(s)

Please scroll down for article—it is on subsequent pages



With 12,500 members from nearly 90 countries, INFORMS is the largest international association of operations research (O.R.) and analytics professionals and students. INFORMS provides unique networking and learning opportunities for individual professionals, and organizations of all types and sizes, to better understand and use O.R. and analytics tools and methods to transform strategic visions and achieve better outcomes.

For more information on INFORMS, its publications, membership, or meetings visit <http://www.informs.org>

Learning from Digital Failures? The Effectiveness of Firms' Divestiture and Management Turnover Responses to Data Breaches

GuiDeng Say,^a Gurneeta Vasudeva^b

^a Lee Kong Chian School of Business, Singapore Management University, Singapore 178899; ^b Carlson School of Management, University of Minnesota, Minneapolis, Minnesota 55455

Contact: gdsay@smu.edu.sg,  <https://orcid.org/0000-0002-6089-0215> (GS); gurneeta@umn.edu,  <https://orcid.org/0000-0002-3099-5534> (GV)

Received: October 31, 2018

Revised: January 5, 2019; July 6, 2019; November 12, 2019

Accepted: March 20, 2020

Published Online in Articles in Advance: May 21, 2020

<https://doi.org/10.1287/stsc.2020.0106>

Copyright: © 2020 INFORMS

Abstract. We examine whether firms learn from digital technology failures in the form of data breach events, based on the effectiveness of their failure responses. We argue that firms experiencing such technological failures interpret them broadly as organizational problems, and undertake unrelated divestitures and top management turnover to achieve better standardization and to remove dysfunctional routines. We test our hypotheses on unrelated subsidiary divestitures and chief technology officer (CTO) turnovers undertaken by 8,760 publicly traded U.S. firms that were at risk of experiencing data breaches involving the loss of personally identifiable information during the period 2005–2016. We find that data breaches significantly increase the hazard of unrelated divestitures and CTO turnover, and that these failure responses are sensitive to firms' aspiration-performance feedback. However, whereas unrelated divestitures reduce the reoccurrence of data breaches, CTO turnover has no significant effect. Our findings suggest a corrective role of unrelated divestitures for failure learning, and the symbolic nature of CTO turnover as a failure response. Our study unpacks failure learning that hitherto has been inferred from a firm's own failure experience and industry-wide failures, and highlights the interplay between the digital and nondigital components of a firm in the understudied context of data breaches.

Keywords: digitalization • organizational routines • failure learning • aspiration-performance feedback • cybersecurity • data breach • divestitures • top management turnover

Introduction

Failures in complex technological systems have long been considered as broader problems of organizing rather than narrowly defined technical problems (Perrow 1984). According to this view, technological failures, encompassing a broad array of product defects and large-scale industrial accidents, exemplify how technologies "interact with managerial, structural, and other factors inside and outside the organization" (Pearson and Clair 1998, p. 65; see also Starbuck and Milliken 1988, Vaughan 1990). A combination of technological-structural and social-political forces that operate within and outside organizations (Pearson and Clair 1998) are thus often attributed to such failures. Despite the challenges in detecting the causes and devising appropriate remedies, failures provide firms with information-rich learning opportunities for organizational improvements to avert future failures (Sitkin 1992, Haunschild and Sullivan 2002, Baum and Dahlin 2007, Madsen and Desai 2010, Diwas et al. 2013, Dahlin et al. 2018). Firms are known to respond to this failure learning by introducing new organizational routines, incorporating additional

safety procedures and protocols (Haunschild et al. 2015, Clay-Williams and Colligan 2015), acquiring infrastructure (Desai 2011), and establishing new organizational units (Rathert and May 2007). Ironically, pressures to appease stakeholders and competition for resources that redirect firms' investments and managerial efforts toward profitability over safety priorities can hinder failure learning (Haunschild et al. 2015, Dahlin et al. 2018, Gaba and Greve 2019). Consequently, organizational responses may prove ineffective, leading to repeated failures (Bennett and Snyder 2017).

In light of this dialectic, how firms respond in the aftermath of a technological failure, and the effectiveness of their organizational responses in averting subsequent failures remains an open question.

We address the question of failure learning based on the effectiveness of the resulting organizational responses in the context of digital vulnerabilities. Such digital vulnerabilities often arise from the increased embeddedness of information and communication technologies (ICTs) within and between firms in an interdependent ecosystem. Consequently, catastrophic

failure events in the form of cyberhacking events can result from “the compromise of confidentiality, integrity, or availability of data or information technology (IT) assets that are responsible for the creation, storage, processing, transport and safeguarding of data assets” (Benaroch and Chernobai 2017, p. 1). The most prevalent outcome of cyberhacking is a data breach, whereby data are exposed to an unauthorized party (Verizon 2016). More than 10 billion data records of individuals’ sensitive information have been compromised globally,¹ and the United States alone saw more than 54 million detected network attacks in the first quarter of 2015 (McAfee Labs 2016).

Importantly, data breaches often involve complex interactions between the digital and nondigital elements of firms, and embody the amalgamation of human and technological deficiencies until a system loses its robustness and viability (Vaughan 1990, Pearson and Clair 1998, Fischbacher-Smith 2010). Such failures become even more likely in tightly coupled systems of human and machine interactions, whereby weakness in one component could trigger a cascading series of failures (Perrow 1984, Roux-Dufort 2007). Consequently, a central problem for firms that experience failures such as data breaches is not only technical but also organizational in nature. Despite this imperative, we know little about how and with what effects firms address the problem of failures such as data breaches.

Drawing on perspectives from the literature on failure learning (Baum and Dahlin 2007, Desai 2015, Dahlin et al. 2018), we propose that data breaches motivate two major organizational responses by affected firms—divestitures of unrelated subsidiaries, and the turnover of the chief technology officer (CTO). Failure learning occurs when these organizational responses lower the likelihood of a future failure. Divestitures that result in fewer unrelated organizational units under a firm’s direct control allow for better standardization of organizational routines and practices to prevent future failures (Brauer 2006). Likewise, replacing the CTO may lead to improved performance by eradicating problematic routines (Cyert and March 1963, Levinthal and March 1993) that may have contributed to the failure in the first place (Fisher and White 2000). Yet, given that firms often encounter multiple and conflicting goals such as safety and profitability (Gaba and Greve 2019), we argue that firms’ propensity to initiate substantive organizational changes is likely predicated on their financial performance relative to their own historical aspiration level, and social comparison with relevant industry peers. Accordingly, failure responses may not always constitute failure learning by way of mitigating failure reoccurrence, but rather signal

responsiveness to external stakeholders, thereby mitigating negative consequences such as loss in market value, increased public scrutiny, and pressure from regulators following a data breach (Bundy et al. 2017).

We test our theory in the context of cyberhacking-related data breach occurrences during the period 2005–2016 at publicly traded U.S. firms. The breaches in our sample involve the loss of personally identifiable information (PII). Examples of PII include medical and credit card information, personal addresses, and social security numbers. The context of PII-related data breaches represents a good test of our theory because virtually all firms process and store such data to some extent, and thus are at risk for experiencing such failures. Results from our hazard models reveal that following a data breach event, firms demonstrate a significantly greater likelihood of divesting unrelated subsidiaries and replacing the CTO. Whereas the hazard of unrelated divestiture is amplified by firms’ underperformance relative to their historical earnings per share (EPS), CTO turnover is more likely when firms overperform relative to their social and historical benchmarks. However, whereas divestitures significantly reduce the likelihood of firms experiencing subsequent failures, CTO turnovers are not as effective for failure mitigation. These findings are suggestive of the corrective learning effects of unrelated divestitures, and perhaps more symbolic “scapegoating” driving CTO turnovers as failure responses.

Our study extends theoretical developments in the technological failure-induced learning literature in at least three ways. First, our study departs from prior works that infer organizational learning from failure experiences such as industrial accidents or product defects (e.g., Baum and Dahlin 2007, Madsen and Desai 2010) but do not directly observe the effectiveness of organizational responses in mitigating subsequent failures. As Bennett and Snyder (2017) note, evidence of failure learning has remained elusive. We infer unrelated divestitures as a failure response that aims to address the structural aspects, and CTO turnover as a response to the social-political considerations underpinning a technological failure. By observing subsequent failure reoccurrences, we distinguish between substantive failure learning and the symbolic underpinnings of failure responses. Second, prevailing wisdom suggests that firms tend to build organizational resilience in the face of new technological challenges by acquiring new capabilities (Karim and Mitchell 2004, Capron and Mitchell 2009, Puranam et al. 2009, Williams et al. 2017). In this regard, our findings highlight that firms may need to first remove organizational units and along with them any dysfunctional routines in the aftermath of

failures, before acquiring new capabilities. Third, our theoretical framework incorporates the contingent role of aspiration-performance feedback (Baum and Dahlin 2007, Desai 2015), which we show serves as an important mechanism underpinning organizational responses to failures.

Our study also extends prior research on organizational responses to failures and failure learning from an empirical standpoint. In this regard, first, our study draws attention to cybersecurity threats that have become pervasive with advances in ICTs. Despite the perennial threat of cyberhacking, systematic inquiry of this important form of digital failure by strategy scholars is virtually nonexistent. Second, inferences of failure learning from prior failure experiences alone (e.g., Haunschild and Sullivan 2002, Baum and Dahlin 2007, Madsen and Desai 2010), may be prone to problems of model misspecification (Bennett and Snyder 2017). To address such issues, we assess failure learning based on the effectiveness of organizational responses in mediating the relationship between failure experience and subsequent failures. Our analyses based on a hazard model account for the time to process failure information and execute an appropriate organizational response. Third, in contrast to most single-industry case studies of product failures or industrial accidents, our empirical context enhances the generalizability of our findings beyond specific industries. An important empirical challenge of studying cyberhacking concerns its observability and information availability. By employing PII-related data breaches as our empirical setting, for which all U.S. states have enacted laws mandating disclosure, our study includes all firms from multiple industries that experience such breaches, permitting fine-grained quantitative analysis of its organizational impacts.

Literature Review and Hypotheses

Technological Change and Organizational Vulnerabilities

Although new technologies allow advancement on many frontiers, technology implementation processes often require nontechnical organizational capabilities (Tushman and Anderson 1986, Tyre and Hauptman 1992, Rahmandad and Repenning 2016). Bottlenecks in these organizational processes and capabilities can create systemic weaknesses that increase the likelihood of technological failure (Weick 1990, Pearson and Clair 1998, Vaughan 1999, Weick and Quinn 1999, Ramanujan 2003, Haunschild et al. 2015, Dahlin et al. 2018). For example, the technological repair costs following the Fukushima nuclear accident and Union Carbide's chemical explosion in Bhopal necessitated major organizational

changes such as divestitures (Smith and Sipika 1993, Hosoe and Tanaka 2012).

Separately, studies in a variety of technological domains have observed how new technologies can generate unintended organizational consequences for firms. Bernstein's (2012) examination of state-of-the-art monitoring technologies implemented at a factory space revealed workers' hiding behaviors as a counter response, reducing overall productivity. Similarly, task-notification technologies to facilitate timely behaviors resulted in dual-task interference, arising from the limitation of human cognition whereby the brain must rapidly switch attention between multiple simultaneous activities (Jenkins et al. 2016). Thus, the adoption of new technologies often result in unanticipated interferences with established tasks and routines at the individual and organizational levels.

Apart from these internal organizational challenges, even well-intended technologies aimed at ameliorating societal problems, such as genetically modified organisms (Easley and Lenox 2006, Rerup 2009), have raised concerns among the public and subjected firms to unanticipated stakeholder pressures. Such stakeholder pressures become even more severe when technological failures in the form of antimicrobial resistance owing to the overuse of particular drugs, for instance, create negative externalities.² Thus, technological advancement can have strategic ramifications of the type that warrant internally and externally oriented organizational responses (Gulati and Puranam 2009).

A similar dynamic unfolds in the context of ICTs, which offer firms in a wide range of industries an important avenue for exploiting novel sources of competitive advantage. In particular, ICTs that facilitate machine-to-machine and human-to-machine interactions allow firms to leverage advances in artificial intelligence and generate big data for value creation (George et al. 2016). By providing the means for granular information collection and processing in real time (McAfee et al. 2012), digitalization facilitates a deeper understanding of markets, while enabling collaborative forms of organizing and value creation (Puranam et al. 2014, Adner 2017, McIntyre and Srinivasan 2017, Helfat and Raubitschek 2018). Despite these promising features, digitalization also exposes firms to cybersecurity vulnerabilities and failures that manifest in the form of data breaches.

Drawing on organizational learning theory, the literature on firms' failure experiences observes that less frequent failures such as airline and railroad accidents (Haunschild and Sullivan 2002, Baum and Dahlin 2007), and orbital launch failures (Madsen and Desai 2010), tend to be highly visible and salient events, thereby motivating significant learning efforts (Baum and Dahlin 2007). Although the causes of such

failures are usually complex, as negative events that receive widespread publicity, such failures become the subject of greater managerial scrutiny and attention from external audiences. Consequently, failure experiences can generate important lessons and inferences about underlying organizational problems and weaknesses, which could reduce the likelihood of subsequent failure occurrences. It follows that failure learning perpetuates organizational practices, strategies, and structures that reduce subsequent failure occurrences (Cyert and March 1963, Levitt and March 1988, Argote et al. 1990, Baum and Dahlin 2007).

However, even well-intended organizational changes could result in organizational disruptions with adverse consequences, and organizational changes aimed at appeasing external audiences, such as investors, analysts, regulators, and customers for mitigating legitimacy concerns (Oliver 1991), may not generate the desired benefits. Moreover, organizational attention and the associated responses to failures tend to be highly contextual (Ocasio 1995). The likelihood of taking corrective actions in response to failures may therefore increase when organizations are performing further away from their aspirational levels relative to their own historical performance or that of their industry peers (Greve 1998, Baum and Dahlin 2007, Desai 2015). In the hypotheses that follow, we employ these perspectives from organizational learning to theorize about the effectiveness of unrelated divestitures and top management turnover as organizational responses to digital data breach events.

Divestiture as a Failure Response

Our theory of divestiture as a strategic response to digital failure in the form of data breaches draws on the technological-structural perspective of crisis (Perrow 1984) that has been applied to various domains such as space shuttle (Vaughan 1990) and chemical accidents (Pauchant and Mitroff 1992). According to this approach, technology is conceptualized “not only as organizational machines or tools, but also includes management procedures, policies, practice and routines” (Pearson and Clair 1998, p. 65), and the cause of failure is attributable to complex interactions between the technical and structural components of the larger system (Perrow 1984, Shrivastava 1987, Starbuck and Milliken 1988, Pauchant and Mitroff 1992). Although the causes of failure are often ambiguous and difficult to pinpoint, as Pearson and Mitroff (1993, p. 53) observed, “the best prepared organizations do not follow the hackneyed principle of ‘if it ain’t broke, don’t fix it’”, but instead “continuously search for potential breaks before they are too big to fix.” Consequently, the search for solutions attributable to organizational learning (Argote 1993, Levinthal and March 1993)

propels firms to evaluate their organizational arrangements for addressing technological bottlenecks and failures (e.g., Benaroch and Chernobai 2017).

Notwithstanding the benefits that diversification may offer in terms of market opportunities and risk mitigation, studies have found that firm characteristics such as firm scope tend to associate with more organizational decentralization and compartmentalization because a high degree of unrelatedness between business units can result in negative synergies and weakened monitoring efforts (Duhaime and Grant 1984, Hoskisson et al. 1994, Bergh 1995). These structural attributes also amplify variability and less control, leading to a higher risk of accumulation of latent errors that can increase the risk of failure (Haunschild and Sullivan 2002). As a result, diversified organizational structures can hamper decision makers’ timely responses to problematic routines. Although coordination across even related business units can become costly (Rawley 2010), having fewer but similar business subsidiaries in the portfolio could allow for more efficient redeployment of vital nonscale free resources (Levinthal and Wu 2010). In particular, scarce resources such as managerial time, attention, and budget to develop threat monitoring and information sharing routines can be applied to develop appropriate measures for the shared risk profile of business units (Woo et al. 1992, Brauer 2006). Consistent with this approach, a simulation study of crisis-laden organizations with complex structures found that an organization benefited in terms of decision making accuracy by shifting to a simpler organizational form (Lin et al. 2006).

Applied to our context, more diversified organizations with unrelated units will tend to employ more disparate digital technological structures, making it difficult to standardize operations across different businesses (Chen et al. 2012). In the absence of standardized technological structures and processes needed to achieve coordination across a complex web of interactions, weakness or errors in one component could remain undetected and trigger a cascade of failures. Moreover, diversified firms, in addition to possessing a greater variety of data sought by attackers, also risk exposing themselves through myriad points of intrusion (or contact points) across different business segments. To prevent technological lapses resulting in data breaches, the harmonization of failure prevention routines is crucial given that cyber attackers exploit interactions and incompatibilities among a parent firm’s portfolio of businesses (or across the supply chain) to launch further attacks (Letzing 2012, Verizon 2016). Incompatibilities may arise when parent firms and subsidiaries belong to different industries, place different emphases on security practices, or use different IT systems, thereby

creating idiosyncratic routines that persist. Narduzzo et al. (2001), for instance, examined technical teams in a wireless telecommunications company and found that efforts to homogenize routines were exceedingly difficult once local heterogeneity of routines was established. Moreover, divestitures remove frictions associated with unrelated business units, such as cultural differences and rivalry, which can exacerbate communication problems and generate inefficient reporting practices and complexity in governing a firm's IT security network.

Thus, if digital failures in the form of data breaches, or technological failures more broadly, are interpreted as problems of organizational configuration (Pearson and Clair 1998), they should accelerate divestitures of unrelated units that reduce a firm's scope and improve standardization with the expectation of reducing subsequent failures. Divestitures of unrelated units enable the standardization of technological systems by removing subsidiaries with dissimilar practices, thereby harmonizing practices and routines across the remaining subsidiaries. For individuals performing these routines, standardization translates to a reduced workload, which also increases their ability and willingness to identify and learn from unanticipated anomalies that may lead to a failure (Lawton et al. 2012, Jenkins et al. 2016, Dahlin et al. 2018). From the standpoint of organizational rigidity (Rawley 2010), unrelated divestitures may also encounter less organizational resistance than related divestitures, owing to fewer shared facilities between unrelated units, thereby lowering exit barriers (Harrigan 1981, Zuckerman 2000). The following hypothesis follows from these observations.

Hypothesis 1. (a) Technological failure in the form of data breach increases the likelihood that a firm divests its unrelated subsidiaries. (b) Firms that divest unrelated subsidiaries following a data breach experience a lower likelihood of subsequent failure, *ceteris paribus*.

Top Management Turnover as a Failure Response

Even as firms try to respond to failures by reducing their organizational scope through unrelated divestitures, the cognitive routines, processes, and mental models of their organizational members may persist (Nelson and Winter 1982, Helfat 1994, Tripsas and Gavetti 2000, Sydow et al. 2009). In other words, dysfunctional routines may remain deeply embedded in the technological, cultural, and social structures of the firm even after divestitures. An important reason for this path dependency is the role of top leadership, such as the CTO or a senior manager holding a similar role,³ tasked with the firm's technology strategy and resource-allocation decisions (Adler and Ferdows 1990, Smith 2003). Accordingly, the social-political

perspective on failures suggests that "an organization most likely will experience a crisis of leadership following a triggering event . . . [and] organizational leadership is likely to come under close scrutiny and turnover of (or revolt against) leadership may be likely as well" (Pearson and Clair 1998, p. 64).

It follows that failure is often attributed to the behaviors or other cognitive limitations of those in leadership roles (Pearson and Clair 1998). In line with this tendency, factors that impede error reporting and analysis at the organizational level can be linked to the culture of blaming individuals rather than exploring other error causes (Khatri et al. 2009, Lawton et al. 2012). As Dahlin et al. (2018) note on p. 18, "It is a common and simple solution for organizations to blame an error on an individual (Hofmann & Stetzer 1998, Rathert & May 2007)."

At the same time, real deficiencies in an existing top manager, such as incompetence and overconfidence, can stymie the adoption of preventive routines to avert failures (Knott 2003). For instance, managerial overconfidence could create a climate of low psychological safety toward the receptivity of negative information, thereby indirectly fostering norms of nonreporting (Carmeli et al. 2012). In the same vein, CTOs that overly emphasize industry security compliance requirements may inadvertently disregard the idiosyncratic risks a firm faces in relation to an evolving external threat environment (Clinton and Perera 2016). Incompetence may become evident when a CTO is unable to recast IT risks as issues of regulatory costs and reputational damage, translate technical aspects of the threat into strategic business decisions, or fail to galvanize organizational resources (Blau 2017). By directing organizational attention only to well-understood issues, a CTO may perpetuate adherence to dysfunctional routines and introduce rigidities in understanding new threats and problem-solving approaches. Further, the inability to garner financial and organizational support for a more comprehensive cybersecurity posture may reinforce the status quo, and entrench existing dysfunctional routines leading to digital technological failures. Such deficiencies in leadership could render a firm ill-equipped to handle escalating cyber threats. Thus, consistent with studies that have highlighted the link between the top management's cognition and an entrepreneurial outlook (e.g., Eggers and Kaplan 2009, Salvato 2009, Tripsas 2009), the replacement of the CTO can set in motion a series of "unlearning processes" that could reduce the likelihood of recurrent failures.

Although the aforementioned arguments imply that CTO turnover could serve as an effective response to technological failures, such an action is likely costly and disruptive to the firm. The decision

to replace the CTO has serious implications, particularly for firms that are heavily dependent on IT. Moreover, dismissal of the CTO could threaten firms' existing relationships with IT vendors, lower business-IT alignment, or even expose the firm to even greater failure threats (Tanriverdi and Du 2009, Gerth and Peppard 2014, Benaroch and Chernobai 2017). New CTOs may also encounter challenges of coping with the legacy and decisions of predecessors pertaining to the redeployment of IT resources.

Taken together, although top management turnover may not always yield the intended benefits of displacing dysfunctional routines or incompetence entirely, such turnover is still likely to signal to both internal and external audiences the management's commitment to addressing the problems underpinning the failure. Our next hypothesis follows from these arguments.

Hypothesis 2. (a) Technological failure in the form of data breach increases the likelihood that a firm replaces its CTO or a senior executive holding a similar responsibility. (b) Firms that replace their CTO or a senior executive holding a similar responsibility following a data breach experience a lower likelihood of subsequent failures, *ceteris paribus*.

Contingent Role of Financial Aspiration-Performance Feedback

As Hypotheses 1 and 2 suggest, organizational changes in the form of unrelated divestitures and CTO turnovers could remedy a host of internal organizational routines and agency problems underpinning failures such as data breaches. Yet, interventions in the form of organizational restructuring and top management turnover can be risky and spark organizational turbulence that could offset any performance benefits. Moreover, organizations often need to balance multiple goals such as profits and safety (Gaba and Greve 2019), such that the top management's search for appropriate solutions to address technological failures is likely to occur in the context of how well the firm is performing in terms of its financial goals (Haunschild et al. 2015, Kotlar et al. 2018). Related literature on organizational learning recognizes that an organization's willingness to learn and undertake exploratory steps to improve performance rather than simply refine existing practices depends on its performance-aspiration levels (Greve 1998, Greve 2003). These aspiration levels may be benchmarked to the organization's own historical performance, or emerge from vicarious learning and social comparison with industry peers.

Drawing on these insights, we suggest that the experience of technological failure coupled with financial performance shortfalls creates a stronger imperative for top management to undertake more

drastic interventions, such as unrelated divestitures. Under such conditions, unrelated divestitures hold the potential to address organizational weaknesses underlying technological failures while at the same time freeing up resources to alleviate the firm's financial problems (Baum and Dahlin 2007). Divestitures may also release important resources that could help firms cope with the anticipated increase in financial strain while updating technological systems to prevent future failures. Although unrelated businesses may hold strategic importance, decision makers coping with technological failures, while also facing profitability pressures, may place greater emphasis on the long-term cost savings afforded by the standardization of organizational routines resulting from unrelated divestitures. In the same vein, Gaba and Greve (2019) found that airlines managers interpreted safety and profitability concerns as threats to survival, motivating the divestment of certain aircraft assets. In contrast, financial underperformance may not perpetuate the termination or replacement of a firm's CTO whose role and attention is largely focused on a firm's technology strategy, and because such an approach is likely to have little direct impact for improving the firm's financial condition.

Firms that perform above financial aspirations but experience technological failure, however, encounter opposing forces for change. On the one hand, financial success by outperforming peers may engender hubris as management underestimates the impact of technological failure on overall firm profitability, leading to potential inertia against drastic organization-wide changes (Cyert and March 1963, March and Shapira 1987, Hayward and Hambrick 1997). On the other hand, as prior research notes (Baum and Dahlin 2007, p. 372), "success provides organizational decision makers with access to resources and instills confidence in their abilities to pursue new initiatives." Moreover, technological failure for high-performing firms may increase visibility, and therefore, invite greater scrutiny from external stakeholders who demand change aimed at addressing the technological weaknesses. Under such conditions, the replacement of the CTO could provide a credible signal to external audiences that the firm is actively addressing the technological weaknesses, without too much organizational upheaval that could threaten financial profitability. Such an organizational response becomes feasible also because firms that perform well financially may also attract new talent more easily to replace existing top management.

Hypothesis 3. (a) The more a firm underperforms relative to its aspiration levels set by its historical financial performance or that of industry (social) peers, the higher the likelihood that it divests its unrelated

subsidiaries in response to a data breach. (b) The more a firm outperforms relative to its aspiration levels set by its historical financial performance or that of industry (social) peers, the higher the likelihood that it replaces its CTO or a senior executive holding a similar responsibility in response to a data breach

Research Context

Cyberhacking and Data Breach Events in the United States

In this study, we focus on PII-related data breach events as a technological failure involving the compromise of customer and employee credentials. The growing severity of cybersecurity threats leading to such data breaches globally have been described as “among the gravest national security dangers to the United States” (White House 2015).⁴ Highlighting the prioritization of cybersecurity at the corporate level, the U.K. chairman of the accounting firm, KPMG, noted that “Chief executives and company boards have gone from having ‘an anecdotal understanding’ of cybersecurity to seeing it as a key item on the agenda” (Agnew 2014, p. 1).

Data breaches can be broadly classified into confidentiality, integrity, and availability events (Goldstein et al. 2011). Confidentiality events, such as PII data breaches, involve unauthorized access to data and IT assets. In 2016, there were 1,935 confirmed PII data breaches globally, among which the United States accounted for 8% (Verizon 2017). Integrity events compromise the authenticity and accuracy of data, such as website defacements or malicious deletion of data. Finally, availability events prevent the provision of timely service to parties that require them. Examples of availability events include ransomware attacks that willfully encrypt the user’s data in exchange for financial compensation or denial-of-service attacks and viruses that rapidly reproduce information and overwhelm a firm’s network. Although such distinctions of event types are conceptually useful, in practice, data breaches span multiple categories, suggesting considerable ambiguity of cause and uncertainty in outcomes that are characteristic of failures (Pearson and Clair 1998, p. 1).

In terms of economic impact, PII data breach events are estimated to cost a firm between \$6.5 million and \$572 million (Romanosky 2016), with direct costs accruing largely to forensic investigations, customer and employee notifications, public relations, customer support, monitoring, insurance, actual theft, and litigation (Romanosky 2016). Indirect costs comprise lost revenues, reputation loss, and management turnover. Although stock market reactions to breach

announcements have found mixed results (e.g., Cavusoglu et al. 2004, Acquisti et al. 2006, Kashmiri et al. 2017), the direct and indirect costs of data breaches can have delayed and long-lasting effects. LinkedIn, a business-oriented social networking platform, for instance, saw its customers’ sensitive information published online four years after its breach.

Data breaches are typically preceded by a series of managerial missteps manifested as dysfunctional routines. Recounting Home Depot’s breach in 2014, former employees alluded to the firm’s slow response to early threats since 2008. In particular, when employees sought new software and training, managers’ persistent response was “We sell hammers.” In contrast, Target Corporation replaced its chief information officer (CIO), chief executive officer (CEO), and chairman within six months of its massive breach, along with the launch of its Cyber Fusion Centre. These strategic changes foreshadowed its ascendance as an industry leader in dealing with cybersecurity threats and a sustained increase in shoppers. Similarly, ChoicePoint, a company that aggregates and analyzes consumers’ personal information, divested its noncore businesses of direct marketing, forensic DNA, and shareholder services as part of its company-wide strategic review following its breach in 2005 (Campanelli 2006). The firm reemerged as an industry exemplar for securing personnel data and subsequently served as an expert witness in legal proceedings on cybersecurity and privacy issues. Although these examples do not provide conclusive evidence of the effectiveness of organizational responses such as firm divestiture or top management turnover, they illustrate how managers increasingly view data breaches as a strategic and organizational issue rather than a purely technical challenge. We examine such effects empirically next.

Method

Samples

We employ two samples for our analyses of firms’ organizational responses to data breach events and the reoccurrence of such data breaches. The first sample (divestiture sample) is a firm-year panel observing all U.S. public firms during the period 2005–2016. The second sample (turnover sample) incorporates corporate governance and top management team variables from the Institutional Shareholder Services (ISS) Directors database and Execucomp (described later) and is limited to U.S. S&P 1500 firms. Each sample includes both firms that experienced data breaches and those that did not. Specifically, 180 out of 8,760 (2.1%) firms in the divestiture sample experienced a total of 275 PII data breach events.

Similarly, 108 out of 1,807 (6%) firms in the turnover sample experienced a total of 178 PII data breach events.

Data breach events were obtained from the Privacy Rights Clearinghouse (PRC) archives, which aggregates information on data breach events disclosed by regulatory bodies (e.g., attorney general offices and the Federal Bureau of Investigation) and third parties, including customers and public media sources. In 2005, the year when the PRC database started, U.S. federal and state laws mandated the disclosure of data breaches pertaining to PII, allowing for the systematic observation of such breaches within the PRC archives,⁵ thus justifying our study period. Nevertheless, nonreporting could exist for two reasons. First, firms may rationally weigh the pros and cons of disclosure and opt for a cover-up. Privacy attorneys, however, have suggested that firms find this practice too risky and generally obey the law (Romanosky et al. 2014). Second, states within the United States have different thresholds for reporting. Romanosky et al. (2014) observed that firms generally find it more cost-efficient to simply notify all individuals and relevant authorities regardless of their state. These mitigating factors alleviate sample selection bias from firms' nondisclosure.

We focused on cyberhacking-related data breaches classified in the archives as "hacking or malware" and "insider," which indicates the involvement of either an external hacker or an employee of the firm who (intentionally or unintentionally) abetted the breach. These breaches account for 37% of all data breach incidents in the archives. Other types of breaches not involving a computer/network intrusion include payment card fraud not accomplished by hacking, for example, skimming devices at point-of-sale terminals, misplacement of physical documents and electronic devices, and unintended disclosure wherein sensitive information was posted publicly or sent to a wrong party. We obtained similar findings if we retained these breaches in the analyses. Upon dropping observations with incomplete data, we arrived at a final unbalanced panel comprising of 46,182 firm-year observations for the divestiture sample and 10,553 firm-year observations for the turnover sample.

Dependent Variables

This study uses three dependent variables, the hazard (instantaneous probability) of *Unrelated divestiture*, the hazard of *CTO turnover*, and the hazard of *Data breach* (subsequent breaches following firms' divestiture and turnover response). Following prior research, *Unrelated divestiture* takes a value of 1 when the focal firm divests a subsidiary from a different two-digit industry North American Industry Classification System (NAICS) code after it experiences a

data breach, and 0 when the firm does not engage in any divestiture within a given year (Palepu 1985, Wiersema and Liebeskind 1995). A broader two-digit NAICS code was chosen to ensure that the technologies, data, and management processes of both the parent firm and its subsidiary were sufficiently distinct. Results remained consistent when a four-digit NAICS code was used. Divestiture data were obtained from SDC Platinum Mergers and Acquisitions database.⁶ Since we focus on divestitures that result in changes to corporate scope, we excluded divestitures that result from parent firm death, that is, merger with another company, such that target parent firms exist in the year after the divestiture (Berry 2013). We also eliminated divestitures that were in fact tracking stock issuances that do not involve actual changes in business structure (Feldman 2016). We further removed divestitures of financial buyers (e.g., leverage buyout firms) who make acquisitions with the intention of a later sale, because such divestitures are an unlikely response to data breaches.⁷ Finally, we restricted divestitures to U.S. subsidiaries to avoid confounding factors involving country risk and different institutional arrangements (Hayward and Shimizu 2006). Including the aforementioned divestitures, however, does not substantively alter our findings. Of a total of 3,902 divestitures in our sample, 1,455 were unrelated divestitures.

CTO turnover takes a value of 1 if the focal firm replaced or laid off its CTO in a given year, and 0 otherwise. This variable is derived from a yearly dummy that indicates whether the CTO, or an executive officer that performs a similar role, retains the position from the previous year. Data on CTOs was obtained from the Form 10-K annual reports and Form DEF 14A proxy statements that firms file annually with the Securities and Exchange Commission (Benaroch and Chernobai 2017). For firms that do not have a CTO, we explored whether other senior executives could have fulfilled this information security-related role. We first created a search dictionary comprising 78 possible designations (e.g., CIO, chief operating officer, digital) using Bureau Van Dijk's list of IT managers and directors. We then conducted a textual analysis of each filing using the search terms and examined the role description of the officer when a match was found. For instance, in 2009, ICOP Digital Inc., which did not list a CTO/CIO in its 10-K filing, instead listed David Nicholl as a director of technology. An examination of his role description revealed that he made key decisions concerning IT and security, thereby fulfilling the responsibility of a CTO. The turnover rate in our sample is 4.7% during the study period.

The main explanatory variable (also the dependent variable for testing Hypotheses 1(b) and 2(b))

concerning failure reoccurrence) employed to capture technological failure is *Data breach*, which is a binary variable that equals 1 if a firm experienced a data breach in a given year, and 0 otherwise. This operationalization reflects the bimodal distribution of firms that experience breaches, wherein the majority of breached firms had up to two breaches.

Moderator Variables

We explore the performance-aspiration feedback mechanism using performance gap variables calculated from a firm's EPS. Prior work has suggested that managers attend closely to a firm's EPS given the importance placed by the business press, stock analysts, and organizational incentive systems (Bromiley and Harris 2014). EPS is commonly specified by firms' boards of directors as an earnings target in top management compensation contracts. This makes it a more relevant performance measure associated with strategic decision making especially in terms of top management turnover (Puffer and Weintrop 1991, Farrell and Whidbee 2003). We use separate historical and social aspiration measures to allow for the possibility that firms view both self and external (industry) referents as salient, thereby providing more granularity for our estimated relationships. Recent empirical work provides robust support for this approach across a number of organizational performance metrics, such as a firm's return on assets, in contrast to combining both historical and social aspiration measures, which demonstrated inferior model fit (Bromiley and Harris 2014). Our results are largely consistent albeit with weaker significance when we used a weighted average measure or when we allowed firms' attention to switch between self and external referents (e.g., Greve 2003, Gaba and Joseph 2013).

Historical performance gap is the difference between a firm's EPS in the current year and its historical aspiration level, measured as the average EPS in the three years prior to the current year (Vidal and Mitchell 2015). We defined social performance gap as the difference between the firm's EPS in the current year and industry average performance in the same year (social aspiration level). Following prior studies, we created spline functions to contrast the effects of the performance-aspiration gap above and below the aspiration level. We thus split each performance gap variable (historical and social) into two variables. *Historical aspiration performance greater (less) than 0* equals the historical performance gap; and 0 for all observations in which the performance of the focal firm is less (greater) than its aspiration. *Social performance greater (less) than 0* variables were created in a similar fashion. For ease of interpretation we used absolute values for negative performance gaps.

Control Variables

We include several control variables that predict a firm's likelihood of experiencing data breaches, and are commonly associated with divestitures and top management turnover.

Firms' divestiture and turnover responses may be driven by vicarious learning from peers as well as their own prior experience with a breach. We operationalize vicarious learning as *Industry breach experience*, measured as the sum of breaches experienced by a firm's industry peers in a three-year rolling window period. *Prior breach experience* takes a value of 1 if a firm experienced a breach in the three-year period prior to the current year, and 0 otherwise.

Firm size is measured as the natural log of total assets plus one. Besides being an attractive target to hackers, larger firms may seek to unlock value through divestitures (Chatterjee and Wernerfelt 1991, Feldman et al. 2016).

Diversification is a yearly count of the number of business segments in which a firm operates. Segment-level data were obtained from Compustat Historical Segments. In the divestiture sample, 80% of firms operate in multiple business segments. Diversified firms are also better positioned to improve the distribution of their resources through divestitures than less diversified firms, such that diversified firms may divest from less productive units and focus on their primary industry when prospects of their primary industry improve (Berry 2010).

Financially constrained firms may lack resources to invest in adequate IT security,⁸ thereby increasing their risk of being breached, while at the same time choose to divest to generate financial slack. We account for firm profitability and financial constraint using five variables. The *Earnings per share* measure was net of extraordinary items and we measured *Return on assets* as the ratio of a firm's net income to its total assets. *Proportion of segments with negative cash-flow* is measured as the proportion of a firm's segments with negative earnings. The greater this value, the more likely a firm will undergo divestitures, either to generate cash or to focus attention of managers (John et al. 1992, Berger and Ofek 1999). *Leverage* indicating a firm's indebtedness is defined as the sum of short- and long-term debt, scaled by market capitalization (Chemmanur and Yan 2004, Feldman 2016). *Current ratio*, a lower ratio for which indicates more cash constraint, is defined as a firm's current assets divided by its current liabilities.

We account for industry characteristics that attract hackers or capture divestiture trends. Specifically, a booming industry represents lucrative opportunities for financially motivated hackers and accordingly increases the risk of firms experiencing data breaches. Likewise, a mature or slowing industry may motivate

firms toward growth through divestitures (Brauer 2006, Verizon 2016). *Industry sales growth* is calculated as the average sales growth rate of all single-segment companies operating in a firm's four-digit NAICS primary industry, net of the focal firm's own sales growth rate. These variables based on accounting measures are obtained from Compustat.

Strategic events such as divestitures raise the possibility that cyber attackers may be attracted to proprietary deal-related information (Anonymous, 2017). Moreover, a firm with greater *Divestiture experience*, measured as the total number of divestitures conducted in the five years prior to a particular year, may also leverage its accumulated expertise to undertake more unrelated divestitures. This measure further accounts for routinization, where firms reuse old solutions to problem regardless of performance consequences (Kelly and Amburgey 1991). In the divestiture sample, 25% of firms conducted at least one divestiture within a five-year period.

To account for alternative explanations of CTO turnover, we control for *CEO duality*, which reflects the degree to which power is concentrated in a firm's CEO, such that a more powerful CEO is more likely to resist demands for replacing the firm's top managers. *CEO duality* is a yearly binary variable that equals 1 if the CEO and board chair position positions are combined, and 0 otherwise. In the turnover sample, 67% of firms have an executive performing the dual roles of CEO and board chair at least once. A higher *CEO stock ownership*, which is likely to reduce the likelihood of CTO turnover, is measured as the percentage of a firm's outstanding shares held by the CEO. A CEO's firm ownership level ranged from 0.03% to 69%, with a mean level of 2%. A dummy variable is coded as 1 if a CEO's firm ownership is more than one standard deviation above the mean, 0 otherwise.

We include a number of board characteristics to account for the strength of corporate governance that may affect the likelihood of CTO turnover. *Board size*, measured as the number of executives sitting on the board, is expected to dilute the board's power (Wiersema and Zhang 2013). Board size ranged from three to 34 members, with an average of nine members. *Outside director percentage* is the proportion of directors on the board that are external to the firm. In the turnover sample, 99% (1,800 of 1,818) of firms had more than half their board members represented by directors external to the firm. *Outside director stock ownership* measures the percentage of a firm's outstanding shares held by external directors. The level of firm ownership by external directors ranged from 0 to 2%, with a mean level of 0.01%. We dichotomized this variable (1 if greater than one standard deviation above the mean, 0 otherwise) to correct for the skewness in the data. A greater *Audit committee size*,

measured as the number of audit committee members within a firm's board, should enhance governance and consequently increase the likelihood of top management turnover. Firms had an average of four members within the audit committee. Finally we create a measure for *CTO turnover experience* to account for the habitual response of firms to replace their CTO. In the turnover sample, 24% of firms replaced their CTOs within a five-year period.

In sum, we include a number of firm-level control variables to account for alternative explanations for unrelated divestitures and CTO turnovers. However, given the different theoretical drivers of these outcomes, there exists a partial overlap in the control variables included in the models estimating these different types of outcomes.

Estimation

We use a stratified Cox proportional hazards model to analyze the hazard (instantaneous probability) of three events: unrelated subsidiary divestiture, CTO turnover, and the recurrence of data breaches. As with survival models, this estimation technique allows for right-censoring, which occurs when firms have not divested or replaced their top management by the end of the study period (Allison 2014). A further advantage of the Cox model leveraged by studies on firm divestiture is that it makes no assumptions on the precise nature of the hazard's probability distribution (Hayward and Shimizu 2006, Berry 2013). Importantly, since hazard models account for time duration to an event, we were able to minimize concerns regarding reverse causality.

To correct for unobserved factors that could affect both the likelihood of experiencing breaches and firms' responses, we used a two-stage estimation approach. In a first-stage regression, we estimated a probit model predicting the probability of a data breach (or unrelated divestiture and CTO turnover, respectively, in models predicting the recurrence of a data breach). We then used the predicted probabilities from this model and constructed the inverse Mills' ratio, which we included in our models (Puranam et al. 2006, Xia and Li 2013, Lee et al. 2015). We account for unobserved time-invariant firm-level confounding factors by employing stratification at the firm level, which allows each firm to have its own baseline hazard, akin to a fixed-effect model (Allison 2009).⁹

To identify the effect of a data breach on firm responses, we use the yearly total number of security incidents in a firm's industry as an exclusion restriction in the first-stage probit model estimating the likelihood of a data breach. A security incident, which is distinct from an actual data breach, includes attempts by cyberhackers to gain access to IT systems via

tricking employees into revealing passwords or exploiting vulnerabilities specific to an industry, thereby raising a firm's likelihood of experiencing a data breach. Such incidents tend to be cast as technical (rather than strategic) issues to be addressed within IT departments (Clinton and Perera 2016). Consequently, the number of security incidents peers experience should not have a direct effect on a focal firm's decision to divest or replace its CTO, which is more likely determined by the experience with confirmed data breaches. Security incidents outnumber data breaches by approximately 30-fold in our data set.

The effect of divestiture on data breach recurrence is identified using a firm's age, measured as the number of years elapsed since the firm had an initial public offering. Prior research suggests that older firms delay the divestiture of poorly performing units owing to greater organizational inertia and exhibit lower responsiveness to change (Shimizu and Hitt 2005). At the same time, a firm's age should not directly affect the likelihood of breaches since both young and old firms are regularly reported in the news media to experience data breaches. We use *Outside director percentage* to identify the effect of CTO turnover on data breach recurrence. A greater proportion of independent directors results in greater alignment with shareholder needs, thereby holding executives accountable, in this case the CTO, for actions that destroy shareholder wealth (Wiersema and Zhang 2013). The proportion of independent directors should not directly affect a firm's likelihood of experiencing a data breach. We evaluate our instruments based on three parameters: their relevance (significance) in the first-stage model predicting the endogenous variables, the correlation between the endogenous variable and the inverse Mills' ratio, and the value of the first-stage pseudo- R^2 (Certo et al. 2016).¹⁰

Occurrences of divestiture or CTO turnover events in response to data breach events may not be independent, but arise from unobserved firm heterogeneity underlying these decisions. Accordingly, we used standard errors clustered at the firm level to account for the nonindependence of observations within a firm.

Results

Tables 1–4 provide the summary statistics and correlations of the model variables. Variance inflation factor (VIF) values for our model variables range from 1.01 to 8.52, with a mean VIF of 2.32, below the rule-of-thumb cutoff of 10 (Neter et al. 1996). This suggests the absence of substantial multicollinearity.

Tests of Hypotheses

Table 5 reports hazard ratios from the stratified Cox proportional hazard models. Hazard ratios can be interpreted as the multipliers of the baseline hazard of unrelated divestiture or CTO turnover events when the variable increases by one unit (Allison 2014). An increase in the hazard ratio can also be understood as a shortened time to the event. Model 1 provides the first-stage probit estimates predicting the occurrence of a data breach. The instrument variable, *Industry security incidents*, has a strong positive and significant effect on the likelihood of a data breach ($p < 0.05$). A 0.17 correlation with the inverse Mills' ratio provides evidence of a strong instrument.

Models 2, 3, and 4 predict the hazard of an unrelated divestiture. Model 2 presents the results of the baseline model with only control variables, whereas Model 3 includes all the main explanatory variables. Model 4 presents the full model including interactions with performance feedback moderators. Similarly, Models 5, 6, and 7 present results based on the controls, main variables, and full model with interactions predicting CTO turnover, respectively. The log-likelihood improvement in the model fit is significant when the interactions are included with the main variables.

We interpret the main effect of data breach on unrelated divestiture and CTO turnover based on Models 3 and 6. Hypothesis 1(a) predicts that a data breach increases the likelihood that a firm divests its unrelated subsidiaries. The 5.06 hazard ratio for *Data breach* in Model 3 suggests that experiencing a data breach increases the hazard of unrelated divestiture approximately fivefold. Hypothesis 1(a) is therefore supported ($p < 0.001$). Hypothesis 2(a) predicts that a data breach increases the likelihood that a firm replaces its CTO. Model 6 reveals that a firm is 10.14 times more likely to replace its CTO following a data breach event, lending support for Hypothesis 2(a) ($p < 0.001$).

Models 9 through 15 examine the effect of firm responses on data breach reoccurrence. Model 9 provides the first-stage probit estimates predicting the occurrence of unrelated divestiture. The strong positive and significant effect of the instrument variable, *Firm age*, on the likelihood of a data breach, along with a 0.23 correlation with the inverse Mills' ratio provide evidence of a strong instrument. In the probit model in Model 12, the instrument variable, *Outside director percentage*, has a strong significant effect on CTO turnover ($p < 0.001$), with a correlation of 0.19 with the inverse Mills' ratio, suggesting a moderately strong instrument (Certo et al. 2016).

Hypothesis 1(b) predicts that firms that divest unrelated subsidiaries following a data breach experience lower likelihoods of subsequent breaches. Model 11 in Table 6 indicates a 0.42 hazard ratio for

Table 1. Model Variables and Summary Statistics for Divestiture Sample (8,760 firms, $N = 46,182$)

Variable	Description	Source	Mean	Std.	Min	Max
Outcome variable: <i>Unrelated divestiture</i>	1, if firm divests business units with a different two-digit NAICS code within a given year; 0, otherwise	SDC Platinum	0.03	0.18	0.00	1.00
Explanatory variable: <i>Data breach</i>	1, if firm experienced at least one data breach in focal year; 0, otherwise	PrivacyRights Clearinghouse	0.01	0.07	0.00	1.00
Moderator variables						
<i>Historical aspiration performance > 0</i>	Firm's EPS in the focal year minus its average EPS for the past three years; 0, if difference is negative	Compustat	1.71	135.511	0.00	26,307.50
<i>Historical aspiration performance < 0 (absolute)</i>	Absolute value of firm's EPS in the focal year minus its average EPS for the past three years; 0, if difference is positive	Compustat	1.70	80.05	0.00	10,980.17
<i>Social aspiration performance > 0</i>	Firm's EPS minus the industry average EPS in the same year; 0, if difference is negative	Compustat	132.79	676.02	0.00	27,772.03
<i>Social aspiration performance < 0 (absolute)</i>	Absolute value of firm's EPS minus the industry average EPS in the same year; 0, if difference is positive	Compustat	248.24	4,108.63	0.00	586,000.00
Control variables						
<i>Industry security incidents</i>	Natural logarithm of the sum of security incidents of all companies operating in focal firm's two-digit primary industry	Data Breach Incident Report	4.22	2.63	0.00	9.57
<i>Prior breach experience</i>	1, if focal firm experienced a breach in the three-year period prior to the current year; 0, otherwise	PrivacyRights Clearinghouse	0.01	0.11	0.00	1.00
<i>Industry breach experience</i>	Sum of breaches experienced by focal firm's industry peers in the three-year period prior to the current year	PrivacyRights Clearinghouse	8.94	11.76	0.00	45.00
<i>Firm size</i>	Natural logarithm of total assets	Compustat	6.06	2.75	0.001	15.07
<i>Diversification</i>	Number of business segment the focal firm operates in	Compustat Historical Segments	2.69	1.72	1.00	13.00
<i>Earnings per share (EPS)</i>	EPS net of extraordinary items	Compustat	1.35	123.71	-3,937.70	25,542.38
<i>Return on assets (ROA)</i>	Net income divided by total assets	Compustat	-2.60	190.62	-29,700.00	2,537.83
<i>Proportion segments with negative cashflow</i>	Proportion of focal firm's segments having negative earnings	Compustat Historical Segments	0.24	0.35	0.00	4.00
<i>Leverage</i>	Sum of short-and long-term debt divided by market capitalization	Compustat	18.72	1,451.72	0.00	257,000.00
<i>Current ratio</i>	Current assets divided by current liabilities	Compustat	4.52	53.12	-0.02	4,759.40
<i>Industry sales growth</i>	Average sales growth rate of all companies operating in focal firm's two-digit primary industry	Compustat	0.99	4.48	-2.88	127.76
<i>Divestiture experience</i>	Number of divestitures completed in the five-year period prior to the focal year	SDC Platinum	0.21	0.41	0.00	1.00

Table 2. Model Variables and Summary Statistics for Turnover Sample (1,807 firms, $N = 10,553$)

Variable	Description	Source	Mean	Std.	Min	Max
Outcome variable: <i>CTO turnover</i>	1, if firm replaced or laid off its CTO in a given year; 0, otherwise	10-K and DEF 14A Filings in SEC (EDGAR)	0.05	0.21	0.00	1.00
Explanatory variable: <i>Data breach</i>	1, if firm experienced at least one data breach in focal year; 0, otherwise	PrivacyRights Clearinghouse	0.01	0.12	0.00	1.00
Moderator variables						
<i>Historical aspiration performance > 0</i>	Firm's EPS in the focal year minus its average EPS for the past three years; 0, if difference is negative	Compustat	0.73	2.17	0.00	123.72
<i>Historical aspiration performance < 0 (absolute)</i>	Absolute value of firm's EPS in the focal year minus its average EPS for the past three years; 0, if difference is positive	Compustat	0.77	3.24	0.00	133.73
<i>Social aspiration performance > 0</i>	Firm's EPS minus the industry average EPS in the same year; 0, if difference is negative	Compustat	111.47	562.33	0.00	4,869.00
<i>Social aspiration performance < 0 (absolute)</i>	Absolute value of firm's EPS minus the industry average EPS in the same year; 0, if difference is positive	Compustat	200.58	1,337.40	0.00	11,195.58
<i>Industry security incidents</i>	Natural logarithm of the sum of security incidents of all companies operating in focal firm's two-digit primary industry	Data Breach Incident Report	4.35	2.52	0.00	9.57
Control variables						
<i>Prior breach experience</i>	1, if focal firm experienced a breach in the three-year period prior to the current year; 0, otherwise	PrivacyRights Clearinghouse	0.04	0.19	0.00	1.00
<i>Industry breach experience</i>	Sum of breaches experienced by focal firm's industry peers in the three-year period prior to the focal year	PrivacyRights Clearinghouse	8.83	11.08	0.00	45.00
<i>Firm size</i>	Natural logarithm of total assets	Compustat	8.06	1.65	4.02	14.63
<i>Earnings per share (EPS)</i>	EPS net of extraordinary items	Compustat	1.82	4.67	-136.86	139.44
<i>Return on assets (ROA)</i>	Net income divided by total assets	Compustat	0.04	0.11	-3.06	0.78
<i>CEO duality</i>	1, if CEO and chair positions combined in focal year; 0, otherwise	Execucomp	0.53	0.50	0.00	1.00
<i>CEO stock ownership</i>	1, if % of firm's outstanding shares held by CEO is more than 1 standard deviation above the mean level; 0, otherwise	Execucomp	0.25	0.43	0.00	1.00
<i>Board size</i>	Number of board of directors members	ISS Director's database	9.34	2.33	3.00	34.00
<i>Outside director percentage</i>	Proportion of external directors on the board	ISS Director's database	0.79	0.11	0.00	1.00
<i>Outside director stock ownership</i>	1, if % of firm's outstanding shares held by external directors more than 1 standard deviation above the mean level; 0, otherwise	ISS Director's database	0.06	0.23	0.00	1.00
<i>Audit committee size</i>	Number of members in the audit committee	ISS Director's database	3.83	1.03	0.00	9.00
<i>CTO turnover experience</i>	Number of CTO replacements in the five-year period prior to the focal year	10-K and DEF 14A Filings in SEC (EDGAR)	0.23	0.56	0.00	5.00

Table 3. Correlations for Divestiture Sample ($N = 46,182$)

Variable	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
1 Unrelated divestiture	1																		
2 Data breach	0.06	1																	
3 Historical aspiration performance > 0	-4.0E-04	-3.0E-04	1																
4 Historical aspiration performance < 0 (absolute)	-1.4E-03	-5.0E-04	-3.0E-04	1															
5 Social aspiration performance > 0	3.0E-03	-0.01	0.18	0.01	1														
6 Social aspiration performance < 0 (absolute)	-2.7E-03	-3.8E-03	-4.0E-04	2.8E-03	-0.01	1													
7 Industry security incidents (log)	2.7E-03	0.05	-0.01	-0.01	-0.05	0.02	1												
8 Inverse Mills' ratio	-0.10	-0.08	0.01	0.01	0.03	2.7E-03	-0.19	1											
9 Prior breach experience	0.08	0.17	-3.0E-04	-1.3E-03	-0.01	-3.6E-03	0.07	-0.15	1										
10 Industry breach experience	-0.01	0.07	-1.2E-03	-2.6E-03	-0.04	-0.04	0.52	-0.22	0.11	1									
11 Firm size	0.15	0.10	-4.0E-04	0.01	-0.04	-0.01	0.12	-0.50	0.15	0.13	1								
12 Diversification	0.1037	0.03	2.9E-03	2.5E-03	0.01	-1.0E-03	-0.04	-0.16	0.04	-0.03	0.25	1							
13 Earnings per share	6.0E-04	7.0E-04	0.48	-0.08	0.18	-1.6E-03	-2.7E-03	3.1E-03	1.2E-03	1.0E-03	0.01	0.01	1						
14 Return on assets	2.3E-03	1.0E-03	2.0E-04	-1.7E-03	1.3E-03	4.0E-04	1.0E-03	-0.12	1.6E-03	0.01	0.03	0.01	1.6E-03	1					
15 Proportion of segments with negative cashflow	-0.05	-0.02	-1.6E-03	-4.7E-03	-0.01	0.01	0.01	0.18	-0.03	-2.9E-03	-0.24	-0.16	-0.01	-0.01	1				
16 Leverage	-1.9E-03	-9.0E-04	0.01	0.03	1.4E-03	-3.0E-04	-2.4E-03	0.08	-1.4E-03	-2.0E-03	1.4E-03	-3.6E-03	-5.0E-04	-1.0E-04	-1.6E-03	1			
17 Current ratio	-0.01	-3.9E-03	-4.0E-04	0.01	-2.0E-04	-4.0E-04	-0.02	0.25	-0.01	-8.0E-04	-0.04	-0.02	4.1E-03	1.1E-03	0.02	-8.0E-04	1		
18 Industry sales growth	-1.7E-03	-0.01	-1.7E-03	-1.9E-03	0.01	-2.0E-03	-0.03	0.11	-0.01	-0.08	-0.05	-0.03	-1.8E-03	-8.0E-04	0.03	-2.4E-03	1.3E-03	1	
19 Divestiture experience	0.22	0.07	0.01	0.01	0.01	-0.01	-3.6E-03	-0.24	0.10	-0.01	0.26	0.18	0.01	0.01	-0.11	-0.01	-0.02	-0.01	1

Note. $p < 0.05$ for correlations in bold.

Table 4. Correlations for CTO Turnover Sample ($N = 10,553$)

Variable	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1 CTO turnover	1																			
2 Data breach	2.6E-03	1																		
3 Historical aspiration performance > 0	-0.01	0.02	1																	
4 Historical aspiration performance < 0 (absolute)	-0.01	-1.6E-03	-0.08	1																
5 Social aspiration performance > 0	-0.01	-0.01	6.0E-04	-3.8E-03	1															
6 Social aspiration performance < 0 (absolute)	1.3E-03	-0.02	0.01	-8.0E-04	-0.03	1														
7 Industry security incidents (log)	0.01	0.09	-0.01	-0.04	-0.07	0.08	1													
8 Inverse Mills' ratio	6.0E-04	-0.17	-0.05	0.17	0.03	3.1E-03	-0.27	1												
9 Prior breach experience	0.01	0.19	0.01	0.00	-0.02	-0.02	0.10	-0.36	1											
10 Industry breaches	-0.01	0.12	0.01	-0.05	-0.03	-0.09	0.44	-0.36	0.15	1										
11 Firm size	-0.03	0.15	0.06	0.04	-0.02	1.5E-03	0.05	-0.36	0.23	0.07	1									
12 Earnings per share	-2.9E-03	0.03	0.48	-0.38	-0.01	0.01	0.03	-0.25	0.04	-2.3E-03	0.16	1								
13 Return on assets	3.6E-03	0.02	0.15	-0.43	-0.01	0.02	0.02	-0.11	0.02	0.01	0.02	0.48	1							
14 CEO duality	-0.02	2.0E-03	0.01	-3.4E-03	0.04	0.01	-0.02	-0.09	-0.01	-0.01	0.16	0.06	0.04	1						
15 CEO stock ownership	-0.02	-0.01	-0.03	0.06	-0.02	4.6E-03	-0.05	0.17	-0.03	-2.6E-03	-0.19	-0.08	-0.06	0.14	1					
16 Board size	-0.01	0.08	0.03	0.04	-0.01	0.02	0.08	-0.42	0.13	0.09	0.60	0.11	0.01	0.07	-0.14	1				
17 Outside director percentage	0.05	0.02	0.01	4.7E-03	0.01	0.02	-0.02	-0.15	0.03	-0.06	0.22	0.05	-0.01	0.08	-0.20	0.15	1			
18 Outside director stock ownership	-4.7E-03	-0.02	-0.01	0.01	-0.02	-0.01	0.05	0.02	-0.02	-0.01	-0.04	-0.02	-0.02	-0.05	0.02	3.0E-03	0.04	1		
19 Audit committee size	-5.9E-03	0.03	0.02	0.02	0.01	1.2E-03	-0.03	-0.21	0.02	-0.03	0.34	0.08	0.02	0.09	-0.10	0.44	0.26	-0.01	1	
20 CTO turnover experience	0.19	0.02	0.02	-0.03	-0.01	-0.01	0.02	-0.04	4.6E-03	0.03	-0.01	0.01	0.02	-0.03	-0.07	0.03	0.08	-0.02	1.3E-03	1

Note. $p < 0.05$ for correlations in bold.

Table 5. Stratified Hazard Model Estimates of Unrelated Divestiture and CTO Turnover Failure Responses to Data Breaches

	Model 1	Model 2	Model 3	Model 4	Model 5	Model 6	Model 7	Model 8
	Dependent variable							
	Data breach		Unrelated divestiture		CTO turnover		Related divestiture	
Variable	First-stage probit ^a	Controls	Controls	Main effect	Full model	Controls	Main effect	Full model
Industry security incidents (instrument)	0.05* (0.02)							
Data breach				5.06*** (2.37)	4.09** (1.97)		10.44*** (6.98)	0.22 (0.20)
Historical aspiration performance > 0				1.00 (0.01)	1.01 (0.01)		1.11 (0.16)	1.10 (0.17)
Historical aspiration performance < 0				0.96 (0.03)	0.93* (0.03)		0.88 (0.16)	0.88 (0.16)
Social aspiration performance > 0				1.00*** (0.00)	1.00*** (0.00)		1.00*** (0.00)	1.00*** (0.00)
Social aspiration performance < 0				1.00*** (0.00)	1.00*** (0.00)		1.00*** (0.00)	1.00*** (0.00)
Data breach × Historical aspiration performance > 0					0.90 (0.11)			5.11*** (1.97)
Data breach × Historical aspiration performance < 0					1.08* (0.04)			4.98 (5.91)
Data breach × Social aspiration performance > 0					1.01 (0.01)			1.02* (0.01)
Data breach × Social aspiration performance < 0					1.00 (0.00)			0.80 (0.21)
Inverse Mills' ratio		1.57 (0.68)	1.85 (0.84)		2.01 (0.90)	1.77 (1.42)	2.09 (1.68)	2.11 (1.70)
Prior breach experience	0.56*** (0.07)	1.76 (0.83)	3.10* (1.44)		3.81** (1.81)	4.72 (7.38)	10.77** (9.45)	29.30*** (27.75)
Industry breach experience	0.01*** (0.00)	1.11*** (0.02)	1.11*** (0.01)		1.11*** (0.01)	1.19*** (0.03)	1.20*** (0.03)	1.20*** (0.03)
Firm size	0.18*** (0.01)	0.35** (0.11)	0.34** (0.11)		0.34** (0.11)	0.01*** (0.02)	0.02*** (0.02)	0.02*** (0.02)
Diversification	0.02 [†] (0.01)	0.98 (0.11)	1.00 (0.10)		1.03 (0.10)			1.10 (0.09)
Earnings per share	−0.01* (0.00)	1.00 [†] (0.00)	0.99 (0.01)		0.98 [†] (0.01)	0.96 (0.07)	0.87 (0.17)	0.99 (0.02)

Table 5. (Continued)

Variable	Model 1	Model 2	Model 3	Model 4	Model 5	Model 6	Model 7	Model 8
	Dependent variable				CTO turnover			
	Data breach		Unrelated divestiture		Controls		Full model	
	First-stage probit ^a	Controls	Main effect	Full model	Controls	Main effect	Full model	Main effect
<i>Return on assets</i>	0.01*** (0.00)	1.00 (0.02)	1.00 (0.02)	1.00 (0.02)	10.99* (11.41)	7.16 (8.61)	7.24 (8.72)	1.00 (0.00)
<i>Proportion of segments with negative cashflow</i>	−0.15* (0.06)	0.45 (0.26)	0.43 (0.26)	0.42 (0.26)				0.40* (0.15)
<i>Leverage</i>	−0.07** (0.02)	0.97 (0.03)	0.96 (0.03)	0.96 (0.03)				2.72 (0.00)
<i>Current ratio</i>	−0.01 (0.01)	1.00 (0.02)	1.00 (0.02)	1.00 (0.02)				1.00 (0.02)
<i>Industry sales growth</i>	−0.02 (0.02)	0.98 (0.01)	0.98 [†] (0.01)	0.98 [†] (0.01)				0.99 (0.01)
<i>Divestiture experience</i>	0.35*** (0.05)	0.03*** (0.01)	0.03*** (0.01)	0.03*** (0.01)				0.02*** (0.00)
<i>CEO duality</i>					1.56 (0.72)	1.54 (0.72)	1.54 (0.73)	
<i>CEO stock ownership</i>					7.10*** (3.65)	7.36*** (3.82)	7.39*** (3.82)	
<i>Board size</i>					1.15 (0.18)	1.16 (0.18)	1.15 (0.18)	
<i>Outside director percentage</i>					0.00* (0.01)	0.00* (0.01)	0.00* (0.01)	
<i>Outside director stock ownership</i>					0.72 (0.57)	0.76 (0.63)	0.76 (0.63)	
<i>Audit committee size</i>					0.85 (0.17)	0.91 (0.18)	0.93 (0.18)	
<i>CTO turnover experience</i>					0.04*** (0.01)	0.03*** (0.01)	0.03*** (0.01)	
<i>Wald Chi-square</i>	684.5	365.83	452.47	494.95	243.02	276.42	7,987.24	856.21
<i>Log-likelihood (L)</i>		−1,194.23	−1,161.81	−1,155.58	−191.06	−185.61	−183.5	−2,284.65
$-2[L(\beta \text{ baseline}) - L(\beta_i)] \sim \chi^2$		64.8, $p < 0.001^b$	12.46, $p < 0.001^c$		10.9, $p < 0.001^b$	4.22, $p < 0.05^c$		
<i>Number of firms</i>	11,708	8,760	8,760	8,760	1,818	1,818	1,818	8,760
<i>Observations</i>	76,389	46,182	46,182	46,182	10,553	10,553	10,553	46,182
<i>Number of events</i>	333	1,455	1,455	1,455	503	503	503	2,752

Notes. Two-tailed test; clustered standard errors by firm in parentheses. Breslow method for ties. Hazard ratios displayed across Models 2–8 with values greater (less) than 1 indicating positive (negative) relationship).

^aConstant value of −5.16, $p < 0.001$; industry and year fixed effects, R^2 of 0.24; correlation between dependent variable and inverse Mills' ratio of 0.17.

^bCompared against main effects model.

^cCompared against full model.

[†] $p < 0.1$; * $p < 0.05$; ** $p < 0.01$; *** $p < 0.001$.

Table 6. Stratified Hazard Model Estimates of the Effect of Firm Failure Responses on Data Breach Reoccurrence

	Model 9	Model 10	Model 11	Model 12	Model 13	Model 14	Model 15
	Dependent variable						
	Data breach reoccurrence		CTO turnover		Data breach reoccurrence		
Variable	Unrelated divestiture	Without unrelated divestiture response	Unrelated divestiture response	First-stage probit ^b	Without CTO turnover response	CTO turnover response	Unrelated divestiture and CTO turnover response
Firm age	0.04*** (0.00)			0.94*** (0.26)			
Outside director percentage							
Data breach							
Unrelated divestiture			0.42 ⁺ (0.20)				0.30 ⁺ (0.22)
CTO turnover						1.32 (1.15)	1.18 (0.85)
Historical aspiration performance > 0	0.01 (0.04)			−0.03 (0.02)			
Historical aspiration performance < 0	0.02 (0.02)			−0.02 (0.01)			
Social aspiration performance > 0	0.12 (0.44)			−0.00 (0.01)			
Social aspiration performance < 0	−0.22 (0.32)			0.04 (0.11)			
Inverse Mills' ratio		0.00* (0.00)	0.01 (0.00)		0.10 ⁺ (0.13)	0.09 ⁺ (0.11)	0.00** (0.00)
Prior breach experience		0.35* (0.16)	0.38* (0.18)		0.47 (0.25)	0.48 (0.25)	0.44 (0.27)
Industry breach experience		1.04 ⁺ (0.03)	1.04 (0.03)		1.05 ⁺ (0.03)	1.05 ⁺ (0.03)	1.04 (0.21)
Firm size	0.10*** (0.01)	0.01** (0.01)	0.01** (0.01)	−0.05** (0.02)	0.01 (0.02)	0.01 (0.03)	0.01** (0.02)
Diversification	0.04*** (0.01)	0.80 (0.28)	0.81 (0.29)		0.91 (0.28)	0.92 (0.29)	0.79 (0.26)
Earnings per share	0.01 ⁺ (0.00)	1.03 (0.04)	1.03 (0.04)	0.00 (0.01)	1.03 (0.04)	1.03 (0.04)	1.02 (0.04)
Return on assets	−0.01 (0.00)	0.01 (0.07)	0.01 (0.06)	0.02 (0.29)	0.68 (3.54)	0.70 (3.62)	1.76 (9.75)

Table 6. (Continued)

	Model 9	Model 10	Model 11	Model 12	Model 13	Model 14	Model 15
	Dependent variable						
	Unrelated divestiture		Data breach reoccurrence		Data breach reoccurrence		
		Without unrelated divestiture response	Unrelated divestiture response	CTO turnover	Without CTO turnover response	CTO turnover response	Unrelated divestiture and CTO turnover response
Variable	First-stage probit ^a			First-stage probit ^b			
Proportion of segments with negative cashflow	−0.12* (0.06)	4.82 (16.68)	10.43 (39.13)		0.21 (0.76)	0.20 (0.72)	2.07 (9.17)
Leverage	−0.01 (0.00)	1.26*** (0.08)	1.27*** (0.07)		1.36*** (0.11)	1.36*** (0.11)	1.33*** (0.09)
Current ratio	−0.02 (0.02)	0.89 (0.29)	0.89 (0.29)		0.73 (0.37)	0.74 (0.36)	0.92 (0.33)
Industry sales growth	0.01 (0.02)	0.79 (0.20)	0.77 (0.21)		0.90** (0.03)	0.90*** (0.03)	0.84 (0.12)
Divestiture experience	0.81*** (0.03)	0.01** (0.02)	0.01** (0.02)		0.39 (0.52)	0.38 (0.51)	0.02* (0.04)
CEO duality				−0.06 (0.05)			
CEO stock ownership				−0.08 (0.06)			
Board size				0.00 (0.01)			
Outside director stock ownership				−0.09 (0.09)			
Audit committee size				−0.02 (0.02)			
CTO turnover experience				0.47*** (0.03)			
Wald Chi-square	1,142.82	64.3 −65.99	68.17 −63.78	435.42	54.54 −62.28	54.51 −59.19	57.68 −58.11
Log-likelihood (L)							
−2[L(β baseline) − L(β i)] ~ X ²			4.42, <i>p</i> < 0.05			6.18, <i>p</i> < 0.05	11.34, <i>p</i> < 0.001 ^c
Number of firms	7,134	217	217	1818	140	140	138
Observations	39,552	941	941	10,553	595	595	588
Number of events	1,489	89	89	503	66	66	66

Notes. Two-tailed test; clustered standard errors by firm in parentheses. Breslow method for ties. Hazard ratios displayed in Models 10, 11, 13, 14, 15 with values greater (less) than 1 indicate positive (negative relationship).

^aConstant value of −2.94, *p* < 0.001; industry and year fixed effects, *R*² of 0.17; correlation between dependent variable and inverse Mills' ratio of 0.24.

^bConstant value of 1.90, *p* < 0.001; industry and year fixed effects, *R*² of 0.08; correlation between dependent variable and inverse Mills' ratio of 0.19.

^cCompared against Model 11.

p* < 0.1; *p* < 0.05; ****p* < 0.001.

unrelated divestiture, suggesting that even after controlling for a firm's prior data breach experience and industry-wide data breach events (Dahlin et al. 2018), divesting an unrelated subsidiary reduces the hazard of a future data breach by 58%. Hypothesis 1(b) is therefore supported ($p < 0.1$). Hypothesis 2(b) states that replacing the CTO after a data breach reduces the likelihood of subsequent breaches. The nonsignificant 1.32 hazard ratio for CTO turnover in Model 14 does not provide support for Hypothesis 2(b). This positive hazard ratio suggests disruptive effects of CTO turnover leading to future breaches.

Hypothesis 3 tests the aspiration-performance feedback mechanism underlying data breach and firms' unrelated divestiture and CTO turnover responses. Hypothesis 3(a) posits that a firm's unrelated divestiture response to a data breach is contingent on the discrepancy between its performance and aspiration levels. Model 4 in Table 5 reveals a positive and significant interaction between *Data breach* and *Historical aspiration performance* < 0 . With all other variables held at their mean values, when a breached firm underperforms its historical aspiration by 0.37 (the 75th percentile of *Historical aspiration performance* < 0), the hazard of unrelated divestiture increases by 4.08 times relative to a firm that did not experience a data breach. Hypothesis 3(a) is therefore supported ($p < 0.05$). Hypothesis 3(b) states that the effect of a data breach on a firm's CTO turnover will be moderated by the gap between its performance and aspiration levels. Model 7 in Table 5 shows positive and significant interactions with both *Historical aspiration performance* > 0 and *Social aspiration performance* > 0 ($p < 0.001$ and $p < 0.05$, respectively). When a breached firm outperforms its historical aspiration by 0.81 (the 75th percentile of *Historical aspiration performance* > 0), the hazard of CTO turnover increases 4.07 fold relative to a firm that did not experience a data breach. Similarly, a breached firm outperforming its social aspiration by 14 units (the 75th percentile of *Social aspiration performance* > 0) increases the hazard of CTO turnover by 1.4 fold compared with a firm that did not experience a data breach, lending support for Hypothesis 3(b).

Turning to the control variables, smaller firms that are cash constrained with lower EPS, as well as firms that have less divestiture experience, operate in shrinking industries, and have prior direct or vicarious experience with data breaches are more likely to engage in unrelated divestitures. These findings are consistent with the divestiture literature (Brauer 2006). Smaller firms, those with greater ownership by CEOs, a lower proportion of independent directors board, and with greater direct and vicarious experience with data breaches are also more likely to replace their CTO. All other control variables, although largely with coefficients in

the expected direction, were not statistically significant. Concordance statistics for the full models ranged from 0.78 and 0.93 (maximum of 1), suggesting that our model predictions are highly consistent with the actual data.

Supplemental Tests

If unrelated divestitures and CTO turnover constitute learning responses to failures, they should mediate the relationship between a firm's own and industry peers' prior experiences with data breaches and the hazard of a reoccurring data breach. We test for this mediation effect by incorporating instruments to strengthen our conclusions (Shaver 2005). A comparison of Models 10 and 11 reveals that the negative effect of a firm's prior data breach experience diminishes after accounting for unrelated divestiture ($p < 0.01$), consistent with a partial mediation pattern. In these models, the effect of industry peers' data breach experience has a marginally significant positive effect, suggesting increased risk of a data breach. However, the positive effect of prior industry breaches loses significance when firms divest unrelated subsidiaries, suggestive of failure learning. Models 13 and 14 do not provide evidence for a direct effect of a firm's own prior data breach experience, but are indicative of industry peers' breach experience as marginally significant for increasing the hazard of a data breach event. However, these models do not provide support for a mediating role of CTO turnover. Together, these findings suggest that while unrelated divestitures mediate failure learning effects, CTO turnover may not convey such failure learning.

To examine the joint effects of unrelated divestiture and CTO turnover responses and their possible substitution effects, we estimate their simultaneous effect on the reoccurrence of a data breach. Model 11 shows a significant negative effect of unrelated divestiture on data breach recurrence and a nonsignificant effect of CTO turnover, confirming that only unrelated divestiture has corrective effects.

A comparison of Models 4 and 8 show that a data breach only increases the hazard of unrelated divestitures but not related divestitures. The bootstrapped difference in coefficients on data breach across these models is statistically significant ($p < 0.001$). Although 28% of unrelated divestitures co-occur with related divestitures, in analyses not reported, we examined the possibility that related divestitures could preclude unrelated divestitures (i.e., constitute competing events). However, even after accounting for the hazard of related divestitures, a data breach significantly increased the hazard of unrelated divestitures. These findings strengthen the idea that the motivation for divestiture in the event of a data

breach is to improve standardization by reducing firm scope.

Discussion

Although digital technologies confer new sources of competitive advantage on firms, they also make them more vulnerable to losing proprietary information about customers and employees that are vital for capturing value from these technologies. Against this backdrop, we examine how firms respond to technological failures in the form of data breaches and whether they learn from these failures based on the effectiveness of their organizational response strategies. We construe technological failures as problems of organizing reflecting structural bottlenecks and dysfunctional routines, which firms seek to remedy via unrelated divestitures and top management turnover. Findings from our empirical analyses support our claim that data breaches accelerate the likelihood of divesting unrelated subsidiaries, which in turn lowers the hazard of a subsequent data breach. Although data breaches increase the likelihood of CTO turnover, in contrast to unrelated divestiture, this failure response does not lower the likelihood of subsequent data breaches significantly. In addition, although the hazard of divesting unrelated subsidiaries is accentuated in the presence of negative historical performance feedback, the likelihood of CTO turnover increases with positive historical and social performance feedback.

Failure Learning and Firms' Responses

Our study extends the literature on failure learning by examining the effectiveness of firms' organizational responses to mitigate the risk of future technological failures. The extant failure learning literature pertaining to product defects and industrial accidents relies mostly on the presumption of continuous adaptive approaches as firms accumulate failure experiences (e.g., Baum and Dahlin 2007, Madsen and Desai 2010). As Madsen and Desai (2010, p. 453) observe in their study of global orbital launch failure, "Given the difficulty of observing changes in organizational knowledge itself, the assumption in much of the empirical organizational learning literature is that changes in observable organizational performance reflect changes in organizational knowledge (see Argote 1999, Baum and Ingram 1998)." Our framework presents a refinement over these prior studies of failure learning by accounting for organizational actions that mediate the effect of failure experience on subsequent failure outcomes. Moreover, when the risk environment evolves rapidly, gradual approaches may be ill-suited to keep up with failure threats (Agarwal and Helfat 2009), necessitating drastic measures such as divestitures and

management turnover for organizational transformation. At the same time, organizational restructuring and top management turnover can create discontinuities of other types that may have adverse effects. This dilemma pervades our context of cyberhacking and the resulting data breaches that compels firms to respond, while also making it difficult to evaluate the evolving risk threats from adversaries.

As our study demonstrates, unrelated divestitures and CTO turnover resonate with the idea that in the context of technological failures, existing capabilities may become viewed as liabilities and hence need to be removed before building new capabilities. Multiple media and industry reports corroborate our findings. A recent global divestiture study conducted by Ernst & Young (2019, p. 3),¹¹ for instance, states that, "divesting is helping streamline operating models to keep pace with technological innovation and improve agility." The report also points out that "many companies have become increasingly complex by operating in several disparate, yet intertwined, businesses" and that divestitures are often intended for streamlining operations and redeploying resources to "support the capital requirements to fund new technology investments." (Ernst & Young 2019, p. 5)

Our finding that unrelated divestitures and top management turnover affect the rate of failure reoccurrence in different ways suggests that not all organizational responses constitute failure learning. Given its effectiveness in reducing reoccurrence of data breaches, unrelated divestments may be regarded as a more substantive form of failure learning. In contrast, CTO dismissal does not generate the desired benefits by way of reducing the rate of a data breach reoccurrence. This finding is corroborated by a quote from a personal interview with a senior executive, suggesting the possibility that CTO turnover can be disruptive, and may constitute scapegoating to appease investors, or to prioritize reputation repair efforts as visible signals to external audiences (Rhee and Valdez 2009, Dahlin et al. 2018).

After the [data breach] incident, we changed our CTO. The new person made a bunch of company-wide changes and left after nine months. Following that, we had two other CTOs who did not stay long either. Nobody has any idea what is going on! We know that there are 'cybersecurity ninjas' appointed in the company, but we don't know who they are and what they do. Not sure if anything really changed around here. (Anonymous 2018)

Thus, as our study reveals, organizations seek to balance multiple and potentially conflicting goals (Gaba and Greve 2019), such that in the absence of profitability concerns, top executive turnovers may

constitute a socio-political response, which is less effective in addressing the safety concerns. Industry analysts also point out that although a CTO's leadership skills matter, the quality of talent that can be attracted and retained is key to managing cybersecurity risks (Andriotis and Ensign 2019). So even though firms tend to change their CTO after a breach incident, the turnover can create other types of discontinuities with adverse effects. Accordingly, our interviews revealed that in more recent years, firms have learned from their failure responses and begun to promote a "blameless culture with more psychological safety" to counteract the tendency for scapegoating. In this sense, failure learning could be viewed as a cumulative adaptive process that proceeds through experimentation and trial and error (Cyert and March 1963, Levitt and March 1988, Argote 1999).

Our finding that unrelated divestitures are accelerated by their negative historical performance feedback suggests that in poorly performing firms, failures are taken more seriously as cybersecurity compliance is increasingly incorporated into firms' audit processes (Agnew 2014). In contrast, managerial assessment of failures in high-performing firms may be sympathetically viewed as a cost of doing business, resulting in a more symbolic response in the form of CTO turnover. Our analyses also raises the question of how external audiences shape firms' failure learning and associated responses (Baum and Dahlin 2007, Dahlin et al. 2018). Failure-stricken firms tend to rely more on their historical rather than social performance feedback for formulating substantive responses such as unrelated divestitures that reduce the risk of subsequent failure. Thus, consistent with prior studies (e.g., Kim et al. 2015), social performance feedback may render incomplete information about the causes underlying others' performance, thereby rendering such feedback less effective. Although failures can attract negative stakeholder evaluations, our analyses (not reported) reveal that failure responses in the form of unrelated divestitures and CTO turnovers are not sensitive to negative stock market reactions, or regulatory scrutiny that could activate firms' attention (Zuckerman 2000, Hoffman and Ocasio 2001).

Limitations and Future Research

At the time of this study, state regulations mandate only the disclosure of PII-related data breaches. Although this may limit the generalizability of our study vis-à-vis the broader phenomenon of cyber intrusion (e.g., ransomware attacks and service disruptions), multiple interviews with technology executives highlight the concomitant loss of PII data. In other words, our findings provide a conservative estimate of firms' responsiveness to data breaches.

Apart from relying on the disclosure of data breaches, which are relatively infrequent and often downplayed (Gephart 1993), our work leverages measurable intermediate outcomes, such as the number of network attacks or security incidents a firm faces to assess whether firms' strategic responses are conditioned on their ability to defend against such attacks.

Owing to incomplete availability of data on the precise geographical location of the breached event, we were not able to pinpoint whether the divested unit was also the one where the data breach occurred. Although such a test of collocation may provide deeper insights into firms' efforts to eliminate the weak link within the organization, our interviews highlight that breached units may in fact hold valuable data, and thus, contribute strategic value to the firm. Viewed differently, divestiture of the breached unit may not be financially advisable, as exemplified by Yahoo's sale of its breached Internet business to Verizon in 2016 whereby the discovery of the data breach resulted in a valuation discount of approximately \$500 million. Similarly, the absence of sufficient financial accounting information about the divested and breached unit preclude a direct assessment of the tradeoffs between financial costs and digital safety benefits. It is plausible that firms do not divest the breached unit, but instead choose alternative less profitable units to address coordination problems and improved harmonization of routines. Resolving these aforementioned data limitations could be worthwhile pursuits for future work.

Extensions to our study could also examine how collaborative organizational forms, such as meta-organizations and platform-based ecosystems (Gulati et al. 2012), manage to leverage the data and informational benefits generated by their partners, while protecting themselves from the vulnerability to cybersecurity risks. Cybersecurity risks within the system resulting in the breach of a single partner can cascade into series of breaches within the system (Clinton and Perera 2016, Verizon 2016). Relatedly, failures originating from third-party contractors or complementors could shape the business portfolios of digitally-enabled platforms and collaborative organizations. In response to such evolving failure threats, firms may preemptively build internal software and hardware capabilities to reduce organizational exposure to technical bottlenecks and external sources of vulnerabilities. Future research could examine the effectiveness of acquiring such technological capabilities. In addition, studies could examine the microprocesses underlying digital failures, and examine the effectiveness of employee training for failure learning, which, as our interviewees emphasized, has received increased attention in recent years.

Conclusion

In sum, much of the exciting possibilities surrounding digitalization rest on technologies that promise reduced costs, increased scalability, and greater interconnectivity. This study provides a cautionary tale by drawing attention to the organizational underpinnings of technological failures and how firms may leverage existing corporate strategy tools to learn from failures and minimize risk.

Acknowledgments

The authors are grateful for editorial comments and feedback from Ron Adner, Phanish Puranam, Feng Zhu, and two anonymous reviewers. They thank Daniel Forbes; Christopher Uggen; Shaker Zahra; and participants at the PhD workshop at the Carlson School of Management, University of Minnesota; research seminar at the Lee Kong Chian School of Business, Singapore Management University; Annual Meeting of the Academy of Management in Chicago; and Annual Meeting of the Strategic Management Society in Minneapolis. They also acknowledge executives at Target Corporation for the opportunity to present an earlier version of this study at their corporate headquarters in Minneapolis. All errors remain the authors'.

Endnotes

¹ See <https://www.privacyrights.org/data-breaches>, accessed April 28, 2020.

² See <https://www.un.org/pga/71/2016/09/21/press-release-hl-meeting-on-antimicrobial-resistance/>, accessed April 28, 2020.

³ The CTO is generally the most senior technical officer in a firm (Adler and Ferdows 1990). Larger firms may anoint a separate CIO who oversees information security directly and reports to the CTO. For smaller firms, the responsibilities of a CIO overlaps significantly with the CTO.

⁴ In 2013, the U.S. President directed the National Institute for Standards and Technology to develop a framework that would serve as the authoritative source of information for information security best practices.

⁵ Organizations experiencing PII breaches are required to notify government agencies, such as the Federal Trade Commission, attorney general offices, and departments of consumer affairs and public health.

⁶ For firms that experienced data breaches, company announcements and media reports surrounding the rationale for divestitures generally focused on unlocking value of the divested asset rather than relating the divestiture explicitly to the data breach incident. This is expected since doing so would negatively affect the value of the divested asset. Divestitures are often enshrouded with the notion of failure and the admission of past mistakes (e.g., divestiture of prior acquisitions that do not meet expectations) such that scholars have noted firms' reluctance to disclose their divestiture patterns (Hamilton and Chow 1993, Brauer 2006).

⁷ These parent firms were identified using the following four-digit NAICS code: 5240 (Other Financial Investment Activities), 5242 (Agencies, Brokerages, and Other Insurance Related Activities), 5259 (Other Investment Pools and Funds).

⁸ We attempted to control for a firm's technological infrastructure (number of computers, servers, network points) by collecting data from Harte Hanks Technology Database. The short period (2006–2009)

of coverage severely limited our sample. A subsample analysis revealed that a firm's technological infrastructure was strongly correlated with Firm size ($\rho = 0.58$, $p < 0.01$).

⁹ Results from Cox models without stratification are consistent, albeit with weaker statistical significance. Although the fixed effects (stratified) model estimates the hazard rate for each firm as a function of its characteristics across time, the standard Cox model estimates the hazard rate between firms. Thus, the fixed effects specification estimates the effect of a data breach on a firm's hazard of unrelated divestiture and CTO dismissal after accounting for time-varying changes in that firm's characteristics that could influence this hazard. Within-firm changes may reflect a firm's learning over time measured by variables such as a firm's prior breach experience and industry breach experience (which we include as controls) that could increase the hazard of a unrelated divestiture and CTO turnover following a data breach occurrence. Although stratified Cox models can suffer from limitations, failure to account for the nonindependence of observations could lead to severely biased coefficient estimates and standard errors (Allison 2009).

¹⁰ A strong exclusion restriction is characterized by a higher R^2 value (low R^2 : 0.02, high R^2 : 0.24) and a lower correlation between the endogenous variable and the inverse Mills' ratio (low correlation: 0.31, high correlation: 1.00).

¹¹ See https://www.ey.com/en_us/divestment-study/2019/why-so-many-companies-are-divesting, accessed April 28, 2020.

References

- Acquisti A, Friedman A, Telang R (2006) Is there a cost to privacy breaches? An event study. *Proc. 27th Internat. Conf. Inform. Systems (ICIS)*, Milwaukee (Association for Information Systems, Atlanta), 1563–1580.
- Adler PS, Ferdows K (1990) The chief technology officer. *California Management Rev.* 32(3):55–62.
- Adner R (2017) Ecosystem as structure: An actionable construct for strategy. *J. Management* 43(1):39–58.
- Agarwal R, Helfat CE (2009) Strategic renewal of organizations. *Organ. Sci.* 20(2):281–293.
- Agnew H (2014) Big Four get serious on cyber security. *Financial Times* (June 8), <https://www.ft.com/content/270d2894-ecb5-11e3-a754-00144feabdc0>.
- Allison PD (2009) Fixed effects models for events history data. *Quantitative Applications in the Social Sciences: Fixed Effects Regression Models* (Sage Publications, Thousand Oaks, CA), 70–86.
- Allison PD (2014) *Event History and Survival Analysis: Regression for Longitudinal Event Data*, volume 46 (Sage Publications, Thousand Oaks, CA).
- Andriotis AM, Ensign RL (2019) Capital One cyber staff raised concerns before hack. *Wall Street Journal* (January 17), <https://www.wsj.com/articles/capital-one-cyber-staff-raised-concerns-before-hack-11565906781>.
- Anonymous (2017) Personal communication with the chief executive officer of an investment banking firm, April 3.
- Anonymous (2018) Personal communication with a senior marketing executive of a major discount retailer, October 25.
- Argote L (1993) Group and organizational learning curves: Individual, system and environmental components. *British J. Soc. Psych.* 32(1):31–51.
- Argote L (1999) *Organizational Learning: Creating, Retaining, and Transferring Knowledge* (Kluwer Academic, Boston).
- Argote L, Beckman SL, Eppler D (1990) The persistence and transfer of learning in industrial settings. *Management Sci.* 36(2):140–154.
- Baum JA, Dahlin KB (2007) Aspiration performance and railroads' patterns of learning from train wrecks and crashes. *Organ. Sci.* 18(3):368–385.

- Baum JA, Ingram P (1998) Survival-enhancing learning in the Manhattan hotel industry, 1898–1980. *Management Sci.* 44(7): 879–1020.
- Benaroch M, Chernobai A (2017) Operational IT failures, IT value-destruction, and board-level IT governance changes. *MIS Quart.* 41(3):729–762.
- Bennett VM, Snyder J (2017) The empirics of learning from failure. *Strategy Sci.* 2(1):1–12.
- Berger PG, Ofek E (1999) Causes and effects of corporate refocusing programs. *Rev. Financial Stud.* 12(2):311–345.
- Bergh DD (1995) Size and relatedness of units sold: An agency theory and resource-based perspective. *Strategic Management J.* 16(3): 221–239.
- Bernstein ES (2012) The transparency paradox: A role for privacy in organizational learning and operational control. *Admin. Sci. Quart.* 57(2):181–216.
- Berry H (2010) Why do firms divest? *Organ. Sci.* 21(2):380–396.
- Berry H (2013) When do firms divest foreign operations? *Organ. Sci.* 24(1):246–261.
- Blau A (2017) The behavioral economics of why executives underinvest in cybersecurity. *Harvard Bus. Rev.* (June 7), <https://hbr.org/2017/06/the-behavioral-economics-of-why-executives-underinvest-in-cybersecurity>.
- Brauer M (2006) What have we acquired and what should we acquire in divestiture research? A review and research agenda. *J. Management* 32(6):751–785.
- Bromiley P, Harris JD (2014) A comparison of alternative measures of organizational aspirations. *Strategic Management J.* 35(3):338–357.
- Bundy J, Pfarrer MD, Short CE, Coombs WT (2017) Crises and crisis management: Integration, interpretation, and research development. *J. Management* 43(6):1661–1692.
- Campanelli M (2006) ChoicePoint to divest three units. *DMNews* (July 12), <https://www.dnnews.com/data/news/13070929/choicepoint-to-divest-three-units>.
- Capron L, Mitchell W (2009) Selection capability: How capability gaps and internal social frictions affect internal and external strategic renewal. *Organ. Sci.* 20(2):294–312.
- Carmeli A, Tishler A, Edmondson AC (2012) CEO relational leadership and strategic decision quality in top management teams: The role of team trust and learning from failure. *Strategic Organ.* 10(1):31–54.
- Cavusoglu H, Mishra B, Raghunathan S (2004) The effect of Internet security breach announcements on market value: Capital market reactions for breached firms and Internet security developers. *Internat. J. Electronic Commerce* 9(1):70–104.
- Certo ST, Busenbark JR, Woo HS, Semadeni M (2016) Sample selection bias and Heckman models in strategic management research. *Strategic Management J.* 37(13):2639–2657.
- Chatterjee S, Wernerfelt B (1991) The link between resources and type of diversification: Theory and evidence. *Strategic Management J.* 12(1):33–48.
- Chemmanur TJ, Yan A (2004) A theory of corporate spin-offs. *J. Financial Econom.* 72(2):259–290.
- Chen H, Chiang RH, Storey VC (2012) Business intelligence and analytics: From big data to big impact. *Management Inform. Systems Quart.* 36(4):1165–1188.
- Clay-Williams R, Colligan L (2015) Back to basics: Checklists in aviation and healthcare. *BMJ Quality Safety* 24(7):428–431.
- Cyert RM, March JG (1963) *A Behavioral Theory of the Firm* (Prentice Hall, Englewood Cliffs, NJ).
- Dahlin KB, Chuang YT, Roulet TJ (2018) Opportunity, motivation, and ability to learn from failures and errors: Review, synthesis, and ways to move forward. *Acad. Management Ann.* 12(1): 252–277.
- Desai VM (2011) Mass media and massive failures: Determining organizational efforts to defend field legitimacy following crises. *Acad. Management J.* 54(2):263–278.
- Desai VM (2015) Learning through the distribution of failures within an organization: Evidence from heart bypass surgery performance. *Acad. Management J.* 58(4):1032–1050.
- Diwas KC, Staats BR, Gino F (2013) Learning from my success and from others' failure: Evidence from minimally invasive cardiac surgery. *Management Sci.* 59(11):2435–2449.
- Duhaime I, Grant J (1984) Factors influencing divestment decision-making: Evidence from a field study. *Strategic Management J.* 5(4):301–318.
- Eesley C, Lenox MJ (2006) Firm responses to secondary stakeholder action. *Strategic Management J.* 27(8):765–781.
- Eggers JP, Kaplan S (2009) Cognition and renewal: Comparing CEO and organizational effects on incumbent adaptation to technical change. *Organ. Sci.* 20(2):461–477.
- Ernst & Young (2019) Global corporate divestment study. Accessed April 28, 2020, https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/divestment/2019/global_divestment_study_report.pdf.
- Farrell KA, Whidbee DA (2003) Impact of firm performance expectations on CEO turnover and replacement decisions. *J. Accounting Econom.* 36(1–3):165–196.
- Feldman ER (2016) Managerial compensation and corporate spinoffs. *Strategic Management J.* 37(10):2011–2030.
- Feldman ER, Amit R, Villalonga B (2016) Corporate divestitures and family control. *Strategic Management J.* 37(3):429–446.
- Fisher SR, White MA (2000) Downsizing in a learning organization: Are there hidden costs? *Acad. Management Rev.* 25(1):244–251.
- Fischbacher-Smith D (2010) Beyond the worst-case scenario: 'Managing' the risks of extreme events. *Risk Management* 12(1):1–8.
- Gaba V, Greve HR (2019) Safe or profitable? The pursuit of conflicting goals. *Organ. Sci.* 30(4):647–667.
- Gaba V, Joseph J (2013) Corporate structure and performance feedback: Aspirations and adaptation in M-form firms. *Organ. Sci.* 24(4):1102–1119.
- George G, Howard-Grenville J, Joshi A, Tihanyi L (2016) Understanding and tackling societal grand challenges through management research. *Acad. Management J.* 59(6):1880–1895.
- Gephart P (1993) The textual approach: Risk and blame in disaster sensemaking. *Acad. Management J.* 36(6):1465–1514.
- Gerth T, Peppard J (2014) How newly appointed CIOs take charge. *MIS Quart. Executive* 13(3):159–173.
- Goldstein J, Chernobai A, Benaroch M (2011) An event study analysis of the economic impact of IT operational risk and its subcategories. *J. Assoc. Inform. Systems* 12(9):606–631.
- Greve HR (1998) Performance, aspirations and risky organizational change. *Admin. Sci. Quart.* 43(1):58–86.
- Greve H (2003) A behavioral theory of R&D expenditures and innovations: Evidence from shipbuilding. *Acad. Management J.* 46(6):685–702.
- Gulati R, Puranam P (2009) Renewal through reorganization: The value of inconsistencies between formal and informal organization. *Organ. Sci.* 20(2):422–440.
- Gulati R, Puranam P, Tushman M (2012) Meta-organization design: Rethinking design in interorganizational and community contexts. *Strategic Management J.* 33(6):571–586.
- Hamilton RT, Chow YK (1993) Why managers divest—Evidence from New Zealand's largest companies. *Strategic Management J.* 14(6):479–484.
- Harrigan KR (1981) Barriers to entry and competitive strategies. *Strategic Management J.* 2(4):395–412.
- Haunschild PR, Sullivan BN (2002) Learning from complexity: Effects of prior accidents and incidents on airlines' learning. *Admin. Sci. Quart.* 47(4):609–643.
- Haunschild PR, Polidoro F Jr, Chandler D (2015) Organizational oscillation between learning and forgetting: The dual role of serious errors. *Organ. Sci.* 26(6):1682–1701.

- Hayward ML, Hambrick DC (1997) Explaining the premiums paid for large acquisitions: Evidence of CEO hubris. *Admin. Sci. Quart.* 42(1):103–127.
- Hayward ML, Shimizu K (2006) De-commitment to losing strategic action: Evidence from the divestiture of poorly performing acquisitions. *Strategic Management J.* 27(6):541–557.
- Helfat CE (1994) Evolutionary trajectories in petroleum firm R&D. *Management Sci.* 40(12):1720–1747.
- Helfat CE, Raubitschek RS (2018) Dynamic and integrative capabilities for profiting from innovation in digital platform-based ecosystems. *Res. Policy* 47(8):1391–1399.
- Hoffman AJ, Ocasio W (2001) Not all events are attended equally: Toward a middle-range theory of industry attention to external events. *Organ. Sci.* 12(4):414–434.
- Hofmann DA, Stetzer A (1998) The role of safety climate and communication in accident interpretation: Implications for learning from negative events. *Acad. Management J.* 41(6):644–657.
- Hoskisson R, Johnson RA, Moesel D (1994) Corporate divestiture intensity in restructuring firms: Effects on governance, strategy, and performance. *Acad. Management J.* 37(5):1207–1251.
- Hosoe N, Tanaka M (2012) Divestiture of TEPCO for reparation for the Fukushima nuclear accident—A path to vertical unbundling. *Energy Policy* 51:207–212.
- Clinton L, Perera D, eds. (2016) *The Cybersecurity Social Contract: Implementing a Market-Based Model for Cybersecurity* (Internet Security Alliance, Arlington, VA).
- Jenkins JL, Anderson BB, Vance A, Kirwan CB, Eargle D (2016) More harm than good? How messages that interrupt can make us vulnerable. *Inform. Systems Res.* 27(4):880–896.
- John K, Lang LH, Netter J (1992) The voluntary restructuring of large firms in response to performance decline. *J. Finance* 47(3):891–917.
- Karim S, Mitchell W (2004) Innovating through acquisition and internal development: A quarter-century of boundary evolution at Johnson & Johnson. *Long Range Planning* 37(6):525–547.
- Kashmiri S, Nicol CD, Hsu L (2017) Birds of a feather: Intra-industry spillover of the Target customer data breach and the shielding role of IT, marketing, and CSR. *J. Acad. Marketing Sci.* 45(2):1–21.
- Kelly D, Amburgey TL (1991) Organizational inertia and momentum: A dynamic model of strategic change. *Acad. Management J.* 34(3):591–612.
- Khatri N, Brown GD, Hicks LL (2009) From a blame culture to a just culture in healthcare. *Healthcare Management Rev.* 34(4):312–322.
- Kim JY, Finkelstein S, Halebian J (2015) All aspirations are not created equal: The differential effects of historical and social aspirations on acquisition behavior. *Acad. Management J.* 58(5):1361–1388.
- Knott AM (2003) The organizational routines factor market paradox. *Strategic Management J.* 24(10):929–943.
- Kotlar J, Massis A, Wright M, Frattini F (2018) Organizational goals: Antecedents, formation processes and implications for firm behavior and performance. *Internat. J. Management Rev.* 20(S1):S3–S18.
- Lawton R, Carruthers S, Gardner P, Wright J, McEachan RR (2012) Identifying the latent failures underpinning medication administration errors: An exploratory study. *Health Services Res.* 47(4):1437–1459.
- Lee SH, Mun HJ, Park KM (2015) When is dependence on other organizations burdensome? The effect of asymmetric dependence on Internet firm failure. *Strategic Management J.* 36(13):2058–2074.
- Letzing J (2012) Attack hits Zappos accounts. *Wall Street Journal* (January 17), <https://www.wsj.com/articles/SB10001424052970204468004577164754266555954>.
- Levinthal DA, March JG (1993) The myopia of learning. *Strategic Management J.* 14(S2):95–112.
- Levinthal DA, Wu B (2010) Opportunity costs and non-scale free capabilities: Profit maximization, corporate scope, and profit margins. *Strategic Management J.* 31(7):780–801.
- Levitt B, March JG (1988) Organizational learning. *Annual Rev. Sociol.* 14(1):319–338.
- Lin Z, Zhao X, Ismail KM, Carley KM (2006) Organizational design and restructuring in response to crises: Lessons from computational modeling and real-world cases. *Organ. Sci.* 17(5):598–618.
- Madsen PM, Desai V (2010) Failing to learn? The effects of failure and success on organizational learning in the global orbital launch vehicle industry. *Acad. Management J.* 53(3):451–476.
- March JG, Shapira Z (1987) Managerial perspectives on risk and risk taking. *Management Sci.* 33(11):1404–1418.
- McAfee Labs (2016) McAfee Labs threat reports. Report, McAfee Labs, Santa Clara, CA. Accessed April 28, 2020, <https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-sep-2016.pdf>.
- McAfee A, Brynjolfsson E, Davenport TH (2012) Big data: The management revolution. *Harvard Bus. Rev.* 90(10):60–68.
- McIntyre DP, Srinivasan A (2017) Networks, platforms, and strategy: Emerging views and next steps. *Strategic Management J.* 38(1):141–160.
- Narduzzo A, Rocco E, Warglien M (2001) Talking about routines in the field. Dosi G, Nelson R, Winter S, eds. *The Nature and Dynamics of Organizational Capabilities* (Oxford University Press, New York), 27–50.
- Nelson RR, Winter SG (1982) *An Evolutionary Theory of Economic Change* (Belknap, Cambridge, MA).
- Neter J, Kutner M, Wasserman W, Nachtsheim C, eds. (1996) *Applied Linear Statistical Models* (McGraw-Hill, Chicago).
- Ocasio WC (1995) The enactment of economic adversity: A reconciliation of theories of failure-induced change and threat-rigidity. *Res. Organ. Behav.* 17:287–331.
- Oliver C (1991) Strategic responses to institutional processes. *Acad. Management Rev.* 16(1):145–179.
- Palepu K (1985) Diversification strategy, profit performance and the entropy measure. *Strategic Management J.* 6(3):239–255.
- Pauchant T, Mitroff I (1992) *Transforming the Crisis-Prone Organization* (Jossey-Bass, San Francisco).
- Pearson CM, Clair JA (1998) Reframing crisis management. *Acad. Management Rev.* 23(1):59–76.
- Pearson CM, Mitroff I (1993) From crisis prone to crisis prepared: A framework for crisis management. *Acad. Management Perspect.* 7(1):48–59.
- Perrow C (1984) *Normal Accidents: Living with High Risk Technologies* (Princeton University Press, Princeton, NJ).
- Puffer SM, Weintrop JB (1991) Corporate performance and CEO turnover: The role of performance expectations. *Admin. Sci. Quart.* 36(1):1–19.
- Puranam P, Alexy O, Reitzig M (2014) What’s “new” about new forms of organizing? *Acad. Management Rev.* 39(2):162–180.
- Puranam P, Singh H, Chaudhuri S (2009) Integrating acquired capabilities: When structural integration is (un)necessary. *Organ. Sci.* 20(2):313–328.
- Puranam P, Singh H, Zollo M (2006) Organizing for innovation: Managing the coordination-autonomy dilemma in technology acquisitions. *Acad. Management J.* 49(2):263–280.
- Rahmandad H, Repenning N (2016) Capability erosion dynamics. *Strategic Management J.* 37(4):649–672.
- Ramanujan R (2003) The effects of discontinuous change on latent errors in organizations: The moderating role of risk. *Acad. Management J.* 46(5):608–617.
- Rathert C, May DR (2007) Healthcare work environments, employee satisfaction, and patient safety: Care provider perspectives. *Healthcare Management Rev.* 32(1):2–11.

- Rawley E (2010) Diversification, coordination costs, and organizational rigidity: Evidence from microdata. *Strategic Management J.* 31(8):873–891.
- Rerup C (2009) Attentional triangulation: Learning from unexpected rare crises. *Organ. Sci.* 20(5):876–893.
- Rhee M, Valdez ME (2009) Contextual factors surrounding reputation damage with potential implications for reputation repair. *Acad. Management Rev.* 34(1):146–168.
- Romanosky S (2016) Examining the costs and causes of cyber incidents. *J. Cybersecurity* 2(2):1–15.
- Romanosky S, Hoffman D, Acquisti A (2014) Empirical analysis of data breach litigation. *J. Empirical Legal Stud.* 11(1):74–104.
- Roux-Dufort C (2007) Is crisis management (only) a management of exceptions? *J. Contingencies Crisis Management* 15(2):105–114.
- Salvato C (2009) Capabilities unveiled: The role of ordinary activities in the evolution of product development processes. *Organ. Sci.* 20(2):384–409.
- Shaver JM (2005) Testing for mediating variables in management research: Concerns, implications, and alternative strategies. *J. Management* 31(3):330–353.
- Shimizu K, Hitt MA (2005) What constrains or facilitates divestitures of formerly acquired firms? The effects of organizational inertia. *J. Management* 31(1):50–72.
- Shrivastava P (1987) *Bhopal: Anatomy of a Crisis* (Ballinger, New York).
- Sitkin SB (1992) Learning through failure: The strategy of small losses. *Res. Organ. Behav.* 14:231–266.
- Smith RD (2003) The chief technology officer: Strategic responsibilities and relationships. *Res. Tech. Management* 46(4):28–36.
- Smith D, Sipika C (1993) Back from the brink—Post-crisis management. *Long Range Planning* 26(1):28–38.
- Starbuck WH, Milliken FJ (1988) Challenger: Fine-tuning the odds until something breaks. *J. Management Stud.* 25(4):319–340.
- Sydow J, Schreyögg G, Koch J (2009) Organizational path dependence: Opening the black box. *Acad. Management Rev.* 34(4):689–709.
- Tanriverdi H, Du K (2009) Disintegrating information technology in corporate divestitures: Implications for regulatory compliance risks and costs. *Proc. 30th Internat. Conf. Inform. Systems (ICIS)* (Association for Information Systems, Atlanta), 50.
- Tripsas M (2009) Technology, identity, and inertia: Through the lens of “The Digital Photography Company”. *Organ. Sci.* 20(2):441–460.
- Tripsas M, Gavetti G (2000) Capabilities, cognition, and inertia: Evidence from digital imaging. *Strategic Management J.* 21(10–11):1147–1161.
- Tushman ML, Anderson P (1986) Technological discontinuities and organizational environments. *Admin. Sci. Quart.* 31(3):439–465.
- Tyre MJ, Hauptman O (1992) Effectiveness of organizational responses to technological change in the production process. *Organ. Sci.* 3(3):301–320.
- Vaughan D (1990) Autonomy, interdependence, and social control: NASA and the space shuttle Challenger. *Admin. Sci. Quart.* 35(2):225–257.
- Vaughan D (1999) The dark side of organizations: Mistake, misconduct and disaster. *Annual Rev. Sociol.* 25(1):271–305.
- Verizon (2016) Data breach investigations report. Report, Verizon, New York. Accessed April 28, 2020, https://enterprise.verizon.com/resources/reports/DBIR_2016_Report.pdf.
- Verizon (2017) Data breach investigations report. Report, Verizon, New York. Accessed April 28, 2020, https://enterprise.verizon.com/resources/reports/2017_dbir.pdf.
- Vidal E, Mitchell W (2015) Adding by subtracting: The relationship between performance feedback and resource reconfiguration through divestitures. *Organ. Sci.* 26(4):1101–1118.
- Weick KE (1990) The vulnerable system: An analysis of the Tenerife air disaster. *J. Management* 16(3):571–593.
- Weick KE, Quinlan RE (1999) Organization and development. Spence JT, Darley JM, Foss DJ, eds. *Annual Rev. Psych.* 50:361–386.
- White House (2015) Cyber Threat Intelligence Integration Center. Fact sheet, The White House, Office of the Press Secretary, <https://obamawhitehouse.archives.gov/the-press-office/2015/02/25/fact-sheet-cyber-threat-intelligence-integration-center>.
- Wiersema MF, Liebeskind JP (1995) The effects of leveraged buyouts on corporate growth and diversification in large firms. *Strategic Management J.* 16(6):447–460.
- Wiersema MF, Zhang Y (2013) Executive turnover in the stock option backdating wave: The impact of social context. *Strategic Management J.* 34(5):590–609.
- Williams TA, Gruber DA, Sutcliffe KM, Shepherd DA, Zhao EY (2017) Organizational response to adversity: Fusing crisis management and resilience research streams. *Acad. Management Ann.* 11(2):733–769.
- Woo Y, Willard GE, Daellenbach US (1992) Spin-off performance: A case of overstated expectations? *Strategic Management J.* 13(6):433–447.
- Xia J, Li S (2013) The divestiture of acquired subunits: A resource dependence approach. *Strategic Management J.* 34(2):131–148.
- Zuckerman E (2000) Focusing the corporate product: Security analysts and de-diversification. *Admin. Sci. Quart.* 45(3):591–619.

GuiDeng Say is an assistant professor of strategy and organisation at the Lee Kong Chian School of Business, Singapore Management University. His research examines firms’ response to negative risk events, such as data breaches, investors’ socially motivated divestments and antimicrobial resistance, and how health adversities influence rural entrepreneurs’ decisions. He received his PhD in strategic management and entrepreneurship from the Carlson School of Management, University of Minnesota.

Gurmeeta Vasudeva is an associate professor in the Strategic Management and Entrepreneurship Department at the Carlson School of Management, University of Minnesota. Her research focuses on organizational learning, collaborative approaches for technological innovation, and new industry emergence in global settings. She received her PhD in strategic management and public policy from the School of Business, George Washington University.