A REVIEW OF EMPIRICAL LITERATURE IN INFORMATION SECURITY

D. DANIEL SOKOL* & TAWEI WANG†

INTRODUCTION

Information security breaches have hit the headlines frequently in recent years because of their potential impact on organizations and the public. For example, Equifax announced a data breach in September 2017, which affected about 147 million people.[1] Its business value, estimated by stock prices, dropped four billion dollars in the first week of the breach. The cost associated with the breach was already $439 million[2] before a $425 million settlement was announced in 2020.[3] The trend of data breaches does not show an optimistic future. According to IBM, the average total cost of a data breach was about $4.24 million, but it took, on average, 287 days to identify and contain a data breach.[4]

The seriousness of information security breaches has also attracted attention from the regulators. For example, the U.S. Securities and Exchange Commission ("SEC") has issued guidance and interpretive guidance in 2011 and 2018, respectively, regarding the disclosures of cybersecurity related risks, which has led to more enforcement actions.[5] The Public Company

* Carolyn Craig Franklin Chair in Law and Professor of Law and Business, USC Gould School of Law; Senior Advisor, White & Case LLP.

† Associate Professor and Associate Dean, Operational Effectiveness, School of Accountancy & MIS, DePaul University.

1. John McCrank & Jim Finkle, *Equifax Breach Could Be Most Costly in Corporate History*, REUTERS (Mar. 2, 2018, 7:05 A.M.), https://www.reuters.com/article/us-equifax-cyber/equifax-breach-could-be-most-costly-in-corporate-history-idUSKCN1GE257 [https://perma.cc/4DJH-SAQL].

2. Ryan Erskine, *Protecting Your Reputation from Cyberattacks Isn't Impossible If You Do These 3 Things*, FORBES (Nov. 28, 2018, 7:40 A.M.), https://www.forbes.com/sites/ryanerskine/2018/11/28/protecting-your-reputation-from-cyberattacks-isnt-impossible-if-you-do-these-3-things/?sh=20056dc224a6 [https://perma.cc/NYU9-DFDT].

3. *Equifax Data Breach Settlement*, FED. TRADE COMM'N (Feb. 2022), https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement [https://perma.cc/FJ83-DZTD].

4. IBM, COST OF A DATA BREACH REPORT 2021, at 4, 6 (2021).

5. Kenneth M. Breen, Phara A. Guberman & Sachin Bansal, *SEC Actions Up the Ante for*

Accounting Oversight Board included an assessment and understanding of cyber and information security risks in its 2020–2024 strategic plan.[6] The Federal Trade Commission ("FTC") has also started to propose changes to its Safeguards Rule and the Privacy Rule under the Gramm-Leach-Bliley Act.[7]

Given the huge impact of data breaches on organizations and individuals, the business research community has attempted to better understand information security from various angles, from threat and disclosures to impact and responses.[8] In this study, we will provide a review of prior empirical studies to help readers better understand this stream of literature. The review will be organized based on a summary of the terminologies discussed in International Organization for Standardization ("ISO")/International Electrotechnical Commission ("IEC") 27032:2012 as illustrated in Figure 1.[9] This framework captures the components that are commonly discussed in assessing information security risks as mentioned in the ISO/IEC 27000 series. Specifically, in the framework, threat agents give rise to threats to specific assets in an organization. The threat may exploit the vulnerabilities that can lead to risks. The shareholders would like to reduce the risks by imposing various governance mechanisms (for example, controls) that can also reduce the vulnerabilities. When the risk is realized, it becomes a breach event, which can affect the breached organization. Actions may be taken in response to the security breaches. Accordingly, Figure 1 provides a structure for us to understand information security, from identification of threats and vulnerabilities; risk assessment and management strategies; and potential consequences and responses.

Cybersecurity Disclosures, BLOOMBERG LAW (Sept. 14, 2021, 1:01 A.M.), https://news.bloomberglaw.com/securities-law/sec-actions-up-the-ante-for-cybersecurity-disclosures [https://perma.cc/9PMQ-HYZS]; *see* Robert J. Jackson, Jr., Commissioner, SEC, Speech: Corporate Governance: On the Front Lines of America's Cyber War (Mar. 15, 2018).

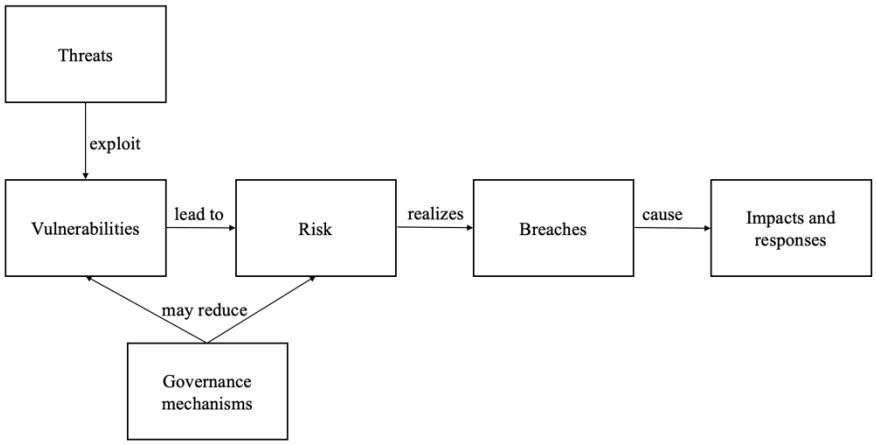
6. *See generally* PUB. CO. ACCT. OVERSIGHT BD., STRATEGIC PLAN 2020–2024 (2020).

7. *FTC Seeks Comment on Proposed Amendments to Safeguards and Privacy Rules*, FED. TRADE COMM'N (Mar. 5, 2019), https://www.ftc.gov/news-events/press-releases/2019/03/ftc-seeks-comment-proposed-amendments-safeguards-privacy-rules [https://perma.cc/AE82-WTVY].

8. *See generally* Chirantan Chatterjee & D. Daniel Sokol, *Data Security, Data Breaches, and Compliance*, *in* THE CAMBRIDGE HANDBOOK OF COMPLIANCE (2021); Diane J. Janvrin & Tawei Wang, *Implications of Cybersecurity on Accounting Information*, 33 J. INFO. SYS. A1 (2019).

9. INT'L ORG. FOR STANDARDIZATION, ISO/IEC 27032:2012 INFORMATION TECHNOLOGY—SECURITY TECHNIQUES— GUIDELINES FOR CYBERSECURITY (2012).

FIGURE 1. Framework for the Review



Based on the framework illustrated in Figure 1, the following literature review is organized into three major groups: (1) threats and vulnerabilities; (2) risks and governance mechanisms; and (3) impacts and responses.

II. EMPIRICAL STUDIES IN INFORMATION SECURITY

A. STUDIES ABOUT THREATS OR VULNERABILITIES

When discussing information security risks, threats and vulnerabilities cannot be ignored. However, empirical studies around these two topics are quite limited, with several exceptions. For instance, Telang and Wattal[10] investigated the market reactions to the announcement of software vulnerabilities and found significant negative market reactions. Ransbotham, Mitra, and Ramsey built on the innovation diffusion theory to investigate how effective the market-based disclosures of vulnerabilities are.[11] Using data from a proprietary database of intrusion detection systems and vulnerability markets as well as the national vulnerability database, the authors found that such disclosures limit the diffusion of vulnerability exploitations and reduce the risk of exploitation.[12] Also focusing on the vulnerability disclosing mechanisms, Mitra and Ransbotham compared

10. Rahul Telang & Sunil Wattal, *An Empirical Analysis of the Impact of Software Vulnerability Announcements on Firm Stock Price*, 33 IEEE TRANSACTIONS ON SOFTWARE ENG'G 544–57 (2007).

11. Sam Ransbotham, Sabyaschi Mitra & Jon Ramsey, *Are Markets for Vulnerabilities Effective?*, 36 MIS Q. 43, 45 (2012).

12. *Id.* at 53–59.

attacks based on software vulnerabilities disclosed through full disclosure and limited disclosure mechanisms and demonstrated that full disclosure accelerates the diffusion of attacks.[13] Another study by Wang, Gupta, and Rao, relied on the routine activity theory to investigate the risk of insider threats related to different applications of a financial institution.[14] The authors used the analysis of an enterprise system's log data to understand users' behaviors: the interarrival times of two consecutive unauthorized access attempts and the daily number of unauthorized attempts.[15] The empirical analysis and the additional simulation showed that the value, inertia, visibility, accessibility, and data security measures of an application can be used to predict an application's exposure to unauthorized access risks.[16]

Recently, we started to see studies focusing on vulnerabilities based on external data. For example, Cheong, Huang, Chis, and Wang[17] and Cheong, Wang, and No[18] considered that the vulnerability might not come from the organization itself. Instead, they found that vulnerability was caused by the sharing activities between firms and data brokers as well as among data brokers themselves. Cheong, Huang, Chis, and Wang attempted to build a network of sharing activities between firms and data brokers to illustrate how the information has been shared through third-party cookies.[19] Cheong and Wang used the information of registered data brokers and their competitors, and the breached posts on the dark web to show that the sharing activities among data brokers might result in a systemic security breach across firms due to the "co-opetitive" (where rivals may sometimes work together) nature of data brokers.[20] That is, given that data brokers share valuable information with each other, such activity may increase the likelihood of security breaches. Differently, Wang, Wang, and Zhou attempted to capture firms' potential exposures to security risks on social media.[21] The authors used

13. Sabyasachi Mitra & Sam Ransbotham, *Information Disclosure and the Diffusion of Information Security Attacks*, 26 INFO. SYS. RSCH. 565, 566, 568–69 (2015).

14. Jingguo Wang, Manish Gupta & H. Raghav Rao, *Insider Threats in a Financial Institution: Analysis of Attack-Proneness of Information Systems Applications*, 39 MIS Q. 91, 92 (2015).

15. *Id.* at 100.

16. *Id.* at 106–07.

17. Arion Cheong, R. Huang, J. Chis & Tawei Wang, *The Ring of Fire: A Data Flow Map of Data Sharing Activities Between Data Brokers and U.S. Public Firms* (2021) (unpublished manuscript) (on file with authors).

18. Arion Cheong, Tawei Wang & Won Gyun No, *The Invisible Risk: The Data-Sharing Activities of Data Brokers and Information Leakage* (2021) (unpublished manuscript) (on file with authors).

19. Cheong et al., *supra* note 17, at 1–3.

20. Cheong et al., *supra* note 18, at 2–4. On co-opetition, see generally ADAM M. BRANDENBURGER & BARRY NALEBUFF, COOPETITION (1996).

21. Tawei Wang, Y. Wang & M. Zhou, *Great Profile? The Exposure of Information Security*

LinkedIn profiles to form a risk index based on the information disclosed by employees of an organization and the potential vulnerabilities brought by the disclosed information.[22] They demonstrated that the exposures (that is, risk index) are positively related to security breaches.[23]

B. RISKS AND GOVERNANCE MECHANISMS

1. Disclosures of Information Security Risks and Breaches

Following along the line of understanding vulnerabilities and the potential risks, many studies have focused on how organizations disclose information security risks, which may or may not include breaches that the organizations have experienced. These studies mainly build on the voluntary disclosure literature and prior studies in information security when developing their hypotheses or expectations. For example, Gordon, Loeb, Lucyshyn, and Sohail found that the Sarbanes-Oxley Act ("SOX") has a positive impact on the voluntary disclosure of information security activities.[24] Gordon, Loeb, and Sohail focused on the disclosed information security–related risk factors (Item 1A) in 10-K filings and demonstrated that the market responded positively to the disclosures of such risks.[25] That is, the transparency in disclosing information security–related risk factors is valued by the capital market. Also focusing on the disclosure of information security–related risk factors (Item 1A) in 10-K filings, Wang, Kannan, and Ulmer demonstrated that organizations disclosed such risk factors in general or with action-oriented information.[26] They also showed that the disclosures of generic risk factors can be used to predict future security breaches.[27] In addition, the market punished the organizations that disclosed security-related risk factors but experienced security breaches in later periods. Li, No, and Wang[28] demonstrated that the relationship found in Wang, Kannan, and

Vulnerabilities Through LinkedIn Profile Information (2020) (unpublished manuscript) (on file with authors).

22. *Id.* at 3.

23. *Id.*

24. Lawrence A. Gordon, Martin P. Loeb, William Lucyshyn & Tashfeen Sohail*, The Impact of the Sarbanes-Oxley Act on the Corporate Disclosures of Information Security Activities*, 25 J. ACCT. & PUB. POL'Y 503, 504 (2006).

25. Lawrence A. Gordon, Martin P. Loeb & Tashfeen Sohail, *Market Value of Voluntary Disclosures Concerning Information Security*, 34 MIS Q. 567, 590 (2010).

26. Tawei Wang, Karthik N. Kannan & Jackie Rees Ulmer, *The Association Between the Disclosure and the Realization of Information Security Risk Factors*, 24 INFO. SYS. RSCH 201, 204, 213 (2013).

27. *Id.* at 215.

28. He Li, Won Gyun No & Tawei Wang, *SEC's Cybersecurity Disclosure Guidance and Disclosed Cybersecurity Risk Factors*, 30 INT'L J. ACCT. INFO. SYS. 40, 41 (2018).

Ulmer[29] became insignificant after the issuance of the SEC's cybersecurity disclosure guidance in order to show the effect of the SEC's guidance on organizations' information security risk factor disclosure strategies.[30]

Other studies examine different types of disclosures and how they may affect a firm's business value based on stock price reactions. Amir, Levi, and Livne[31] found that the market responded negatively to the withholding of cyberattack information while Berkman, Jona, Lee, and Soderstrom[32] used disclosures to form a measure of cybersecurity awareness based on the length of the disclosures and the relevance of the language used. The authors showed that the market responded positively to disclosures with higher cybersecurity awareness measure.[33] Ettredge, Guo, and Li suggested that when the disclosures in 10-K filings involved trade secrets, the probability of being breached is higher.[34] Wang, Yen, and Yoon went through all SEC comment letters related to information security risk factor disclosures starting from 2011 and demonstrated that (1) organizations did not always respond to the comment letters and (2) the stock market reacted negatively to organizations' responses to SEC comment letters.[35]

2. Governance-Related Issues

In this stream of literature, boards and top management teams are often discussed. Given that information security risks are not observable from the perspective of empirical research design, researchers often use the consequence—security breaches (that is, the realization of the security risks)—to serve as a proxy for the management of information security risks.

Many studies have discussed the role played by the board on information security management. This can be traced back to the time when information security risks were not considered a strategic risk. For example, Hsu and Wang argued from the perspective of communication and coordination among directors and found that board size, average age and tenure, and the heterogeneity of age could reduce the possibility of security

29. Wang et al., *supra* note 26.

30. Li et al., *supra* note 28, at 41.

31. Eli Amir, Shai Levi & Tsafir Livne, *Do Firms Underreport Information on Cyber-Attacks? Evidence from Capital Markets*, 23 REV. ACCT. STUDS. 1177, 1177–78 (2018).

32. Henk Berkman, Jonathan Jona, Gladys Lee & Naomi Soderstrom, *Cybersecurity Awareness and Market Valuations*, 37 J. ACCT. & PUB. POL'Y 508, 510 (2018).

33. *Id.*

34. Michael Ettredge, Feng Guo & Yijun Li, *Trade Secrets and Cybersecurity Breaches*, 37 J. ACCT. & PUB. POL'Y 564, 565 (2018).

35. Tawei Wang, Ju-Chun Yen & Kyunghee Yoon, *Responses to SEC Comment Letters on Cybersecurity Disclosures*, 46 INT'L J. ACCT. INFO. SYS., Sept. 2022, at 1–2.

breaches.[36] However, the proportion of independent directors and the heterogeneity of tenure could increase it.[37] Higgs, Pinsker, Smith, and Young focused on the board-level technology committee.[38] Building on the signaling theory and voluntary disclosure theory, they demonstrated that firms with board-level technology committees are more likely to have reported security breaches.[39] One recent study by Hsu and Wang suggested that due to the idiosyncratic nature of information security risks, when the board members were busier (that is, with multiple appointments in different organizations), though they can bring more industry-level knowledge to the firm, they do not have enough attention for the firm-specific issues, which can lead to an increase in the likelihood of security breaches.[40]

Many other studies pay attention to the top management team, or the role played by the Chief Information Officer ("CIO") in managing information security risks. Kwon, Ulmer, and Wang used the role of CIO as a proxy when considering security risks at the strategic level and the CIO's compensation composition to measure their risk preferences.[41] The authors demonstrated that the amount of behavior-based compensation and the pay differences of outcome-based compensation between IT and non-IT executives are negatively associated with the likelihood of information security breaches.[42] Similarly, Feng and Wang used compensation to capture the CIO's risk appetite and demonstrated that the level of CIO risk aversion is negatively associated with the likelihood of security breaches.[43] The association is stronger when the CEO is also risk averse. Banker and Feng turned their attention to CIO turnover and showed that security breaches caused by system issues can increase the CIO turnover by seventy-two percent.[44] However, this is not the case when the breaches were caused by human errors or frauds.[45] From a different perspective, Smith, Tadesse, and

36. Carol Hsu & Tawei Wang, *Exploring the Association Between Board Structure and Information Security Breaches*, 24 ASIA PAC. J. INFO. SYS. 531, 533 (2014).

37. *Id.*

38. Julia L. Higgs, Robert E. Pinsker, Thomas J. Smith & George R. Young, *The Relationship Between Board-Level Technology Committees and Reported Security Breaches*, 30 J. INFO. SYS. 79, 79–80 (2016).

39. *Id.* at 80, 83, 92.

40. Carol Hsu & Tawei (David) Wang, *Too Busy to Monitor? Board Busyness and the Occurrence of Reported Information Security Incidents*, 54 HAW. INT'L CONF. ON SYS. SCIS., Jan. 4–8, 2021, at 6232.

41. Juhee Kwon, Jackie Rees Ulmer & Tawei Wang, *The Association Between Top Management Involvement and Compensation and Information Security Breaches*, 27 J. INFO. SYS. 219, 224–31 (2013).

42. *Id.* at 221–23, 227–29.

43. Cecilia (Qian) Feng & Tawei Wang, *Does CIO Risk Appetite Matter? Evidence from Information Security Breach Incidents*, 32 INT'L J. ACCT. INFO. SYS. 59, 73 (2019).

44. Rajiv D. Banker & Cecilia (Qian) Feng, *The Impact of Information Security Breach Incidents on CIO Turnover*, 33 J. INFO. SYS. 309, 310 (2019).

45. *Id.* at 313.

Vincent emphasized the human capital (for example, technological experience and prior board experience) and structural capital (for example, multiple responsibilities) brought by the CIO and demonstrated that these capitals can all be considered as predictors for future breaches.[46]

One recent paper by Islam, Wang, Frah, and Stafford considered the CIO's role as a shielding effect for competitors to reduce the spillover effect after the announcement of the focal firms' security breaches.[47] Instead of emphasizing the role of the CIO, Hsu and Wang discussed the characteristics of the composition of the top management team (for example, age and tenure) and argued that such characteristics can affect investment and management decisions regarding information security and the corresponding policy initiatives.[48] They showed that the average length and heterogeneity of tenure increase the possibility of breaches.[49] Haislip, Lim, and Pinsker built on the upper echelon theory to argue and demonstrate that the management of cybersecurity risks relies on multiple executives.[50] They showed that CEOs and CFOs with technical backgrounds are less likely to be related to security breaches.[51]

Differently, several studies focus more on the effect of external monitoring and the effect of adoption of security standards. For example, three studies all focus on the effect of audit on security risk management from different angles. Yen, Lim, Wang, and Hsu demonstrated that audit firm industry expertise and audit firm tenure can negatively moderate the positive correlations between security breaches and subsequent audit fees given the expertise and tenure can help auditors better evaluate the idiosyncratic security risks.[52] Smith, Higgs, and Pinsker built on the literature in audit fees to show that board-level risk committees and the active audit committees can reduce the audit fee premium due to security breach

46. Thomas Smith, Amanuel F. Tadesse & Nishani Edirisinghe Vincent, *The Impact of CIO Characteristics on Data Breaches*, 43 INT'L J. ACCT. INFO. SYS., Dec. 2021, at 1–2.

47. Md Shariful Islam, Tawei Wang, Nusrat Frah & Tom Stafford, *The Spillover Effect of Focal Firms' Cybersecurity Breaches on Rivals and the Role of the CIO: Evidence from Stock Trading Volume*, 41 J. ACCT. & PUB. POL'Y, Mar.–Apr. 2021, at 2.

48. Carol Hsu & Tawei Wang, *Composition of the Top Management Team and Information Security Breaches, in* HANDBOOK OF RESEARCH ON DIGITAL CRIME, CYBERSPACE SECURITY, AND INFORMATION ASSURANCE 117, 119 (Maria Manuela Cruz-Cunha & Irene Maria Portela eds., 2014).

49. *Id.* at 126.

50. Jacob Haislip, Jee-Hae Lim & Robert Pinsker, *The Impact of Executives' IT Expertise on Reported Data Security Breaches*, 32 INFO. SYS. RSCH. 318, 318–19 (2021).

51. *See id.* at 326.

52. Ju-Chun Yen, Jee-Hae Lim, Tawei Wang & Carol Hsu, *The Impact of Audit Firms' Characteristics on Audit Fees Following Information Security Breaches*, 37 J. ACCT. & PUB. POL'Y 489, 490 (2018).

risks.[53] Li, No, and Boritz also focused on the relationship between cybersecurity risks and audit fees.[54] The authors demonstrated that audit fees reflect security risks with severe breaches.[55] In addition, the increase in audit fees can reduce the likelihood of future security breaches.[56]

In addition, studies have examined the role played by security or privacy laws. For example, Romanosky, Telang, and Acquisti found that data breach disclosure laws reduce identity theft caused by data breaches by 6.1%.[57] Boroomand, Leiponen, and Vasudeva found that with General Data Protection Regulations ("GDPR") and security breaches in their industries, firms pay more attention to data privacy, which results in a decrease in business value.[58] Klein, Manini, and Shi demonstrated that boards add more directors with IT expertise and more frequently assign cyber risk oversight to the board with the effect of GDPR.[59]

Last, a few studies have investigated the adoption of information security risk management standards on the management of security risks. For instance, Hsu, Wang, and Lu used a list of firms with ISO 27001 certificates and showed that, different from the expected signaling effect and the expected improvement in security risk management, there was no evidence on the relationship between that ISO 27001 certification and firm performance.[60] Garg, Wang, and Wilkin considered ISO 27001 adoption as an indicator of better security risk management of a firm.[61] The adoption of ISO 27001 can mitigate the relationship between financial reporting opacity and stock price crash risk due to security breaches.[62]

53. Thomas J. (Tom) Smith, Julia L. Higgs & Robert E. Pinsker, *Do Auditors Price Breach Risk in Their Audit Fees?*, 33 J. INFO. SYS. 177, 180 (2019).

54. He Li, Won Gyun No & J. Efrim Boritz, *Are External Auditors Concerned About Cyber Incidents? Evidence from Audit Fees*, 39 AUDITING: J. PRAC. & THEORY 151, 152 (2020).

55. *Id.*

56. *Id.* at 165.

57. Sasha Romanosky, Rahul Telang & Alessandro Acquisti, *Do Data Breach Disclosure Laws Reduce Identity Theft?*, 30 J. POL'Y ANALYSIS & MGMT. 256, 274 (2011).

58. Farzam Boroomand, Aija Leiponen, & Gurneeta Vasudeva, Does the Market Value Attention to Data Privacy? Evidence from U.S.-Listed Firms Under the GDPR 26–28 (2021) (unpublished manuscript) (on file with authors).

59. April Klein, Raffaele Manini & Yanting (Crystal) Shi, *Across the Pond: How U.S. Firms' Boards of Directors Adapted to the Passage of the GDPR*, 39 CONTEMP. ACCT. RSCH. 199, 215–22 (2022).

60. Carol Hsu, Tawei Wang & Ang Lu, *The Impact of ISO 27001 Certification on Firm Performance*, 49 HAW. INT'L CONF. ON SYS. SCIS., Jan. 5–8, 2016, at 4842, 4846.

61. M. Garg, T. Wang & C. Wilkin, The Impact of Information Security Breaches and "Big Bath" on Stock Price Crash Risk 9, 17 (2021) (unpublished manuscript) (on file with authors).

62. *Id.* at 21–23.

3. Security Investment Decisions

Security investment decisions have long been a major focus in academic literature.[63] Many of the papers in this stream were based on research methodologies such as analytical modeling,[64] though with several exceptions that relied on empirical data to perform the analysis.[65] For example, Tanaka, Matsuura, and Sudoh used the data from the government in Japan to empirically test and show that information security investment–level is dependent on vulnerability.[66] Wang, Chaudhury, and Rao introduced the concept of value-at-risk in the context of information security.[67] The authors use value-at-risk to measure the risk of daily losses due to security exploits.[68] Based on a dataset about daily activity data from a large financial institution, the authors simulate its daily losses based on the data and interviews with security managers.[69] Such information about risks and losses can be used for investment decisions. Angst, Block, D'Arcy, and Kelley differently focused on healthcare breaches.[70] The authors demonstrated that there were two types of information technology adopters and showed that more IT security was not directly related to the reduction of security breaches.[71] Instead, institutional factors such as the two types of information technology adoption can be used to determine the effectiveness of IT security investments.[72] Recently, Jeong, Lee, and Lim matched 118 information security breaches and 98 information security investment announcements to demonstrate the positive spillover effect of both security breaches and security investments.[73] That is, competitors of the breached firm can benefit

63. *See, e.g.*, Tyler Moore, Scott Dynes & Frederick R. Chang, Identifying How Firms Manage Cybersecurity Investment (2016) (unpublished manuscript) (on file with authors) (conducting interviews with information security executives and managers about how firms and government agencies make cybersecurity investment decisions).

64. Lawrence A. Gordon & Martin P. Loeb, *The Economics of Information Security Investment*, 5 ASS'N FOR COMPUTING MACH. TRANSACTIONS ON INFO. & SYS. SEC. 438, 439 (2002).

65. Sangmi Chai, Minkyun Kim & H. Raghav Rao, *Firms' Information Security Investment Decisions: Stock Market Evidence of Investors' Behavior*, 50 DECISION SUPPORT SYS. 651, 652, 656 (2011).

66. Hideyuki Tanaka, Kanta Matsuura & Osamu Sudoh, *Vulnerability and Information Security Investment: An Empirical Analysis of E-Local Government in Japan*, 24 J. ACCT. & PUB. POL'Y 37, 38 (2005).

67. Jingguo Wang, Aby Chaudhury & H. Raghav Rao, *A Value-at-Risk Approach to Information Security Investment*, 19 INFO. SYS. RSCH. 106, 106 (2008).

68. *Id.* at 108–09.

69. *Id.* at 107.

70. Corey M. Angst, Emily S. Block, John D'Arcy & Ken Kelley, *When Do IT Security Investments Matter? Accounting for the Influence of Institutional Factors in the Context of Healthcare Data Breaches*, 41 MIS Q. 893, 893–94 (2017).

71. *Id.* at 909–12.

72. *Id.* at 911.

73. Christina Y. Jeong, Sang-Yong Tom Lee & Jee-Hae Lim, *Information Security Breaches and IT Security Investments: Impacts on Competitors*, 56 INFO. & MGMT. 681, 681–82 (2019).

from their competitors' security breaches.[74] In addition, one firm's security investment announcement may be considered an increase of security investment–level through the entire network.[75]

4. Employee Training and Behaviors

When discussing the management of information security risks, employee training and behaviors (for example, policy compliance) are the main considerations.[76] This stream of literature was mainly performed by behavioral research methodologies in order to better capture the subjective perspectives, such as risk perceptions and behavioral decisions. However, there are some exceptions, though limited. For example, Dang-Pham, Pittayachawan, and Bruno focused on the sources of security influence.[77] The authors used social network analysis to examine security influence in a large contractor company in Vietnam.[78] The findings suggested that security influence occurred between employees in the same department, especially those with longer tenure or younger age.[79]

C. IMPACTS AND RESPONSES TO INFORMATION SECURITY BREACHES

1. Impact of Information Security Breaches

Impact of information security breaches is one of the main topics in prior empirical literature. This stream of literature can be traced back to the early 2000s, and the studies mainly rely on publicly reported security breaches instead of company self-reported breaches. Though with the enactment of breach-notification laws in the past two decades, studies have rarely attempted to distinguish the breaches that may lead to compliance issues from others. Last, though it seems that we hear about security breaches every day, information security breach events are still considered a rare sample after excluding firms without publicly accessible information, such as firm characteristics, performance, or trading information.[80]

While a few of these studies attempted to understand the impact of

74. *Id.* at 690.

75. *Id.*

76. Beth Stackpole, *How to Build a Culture of Cybersecurity*, MASS. INST. TECH. SLOAN SCH. MGMT. (Mar. 15, 2022), https://mitsloan.mit.edu/ideas-made-to-matter/how-to-build-a-culture-cybersecurity [https://perma.cc/XJG5-5D4A].

77. Duy Dang-Pham, Siddhi Pittayachawan & Vince Bruno, *Applying Network Analysis to Investigate Interpersonal Influence of Information Security Behaviours in the Workplace*, 54 INFO. & MGMT. 625, 625–28 (2017).

78. *Id.* at 628.

79. *Id.* at 632–33.

80. Chatterjee & Sokol, *supra* note 8.

security breaches on firm performance, most of them mainly rely on short-term and long-term stock market–related metrics to quantify the impact.[81] In addition, prior studies do not find consistent results in terms of how security breach announcements may affect the breached firm. For example, Campbell, Gordon, Loeb, and Zhou used information security breaches reported in major newspapers and demonstrated that confidentiality-type breaches are associated with significant negative stock market reactions around the days of the announcements.[82] Kannan, Rees, and Sridhar attempted to explain why prior studies did not always find negative stock market reactions to security breaches by focusing on the nature of the breaches, the types of firms, and the time periods of the study.[83] However, no significant negative results were found.[84] Goel and Shawky, differently, used reported security breaches from 2004 to 2008 to show that, on average, the announcement of security breaches was related to negative stock market reactions around the days of the announcements.[85] Gordon, Loeb, and Zhou also used reported security breaches from new articles, but from 1995 to 2007.[86] The authors found a negative association between the announcement of security breaches and stock market reactions. However, the association mainly holds for the availability type breaches. Similar to Kannan, Rees, and Sridhar,[87] Wang, Ulmer, and Kannan also attempted to explain why prior studies did not always find a negative impact of security breaches on business value.[88] The authors found that the information released through the announcement may not be clear enough to trigger a stock price reaction. Recently, Richardson, Smith, and Watson revisited these inconsistent

81. *See, e.g.*, Anat Hovav & John D'Arcy, *The Impact of Denial-of-Service Attack Announcements on the Market Value of Firms*, 6 RISK MGMT. & INS. REV. 97, 97–100 (2003); Sachin B. Modi, Michael A. Wiles & Saurabh Mishra, *Shareholder Value Implications of Service Failures in Triads: The Case of Customer Information Security Breaches*, 35 J. OPERATIONS MGMT. 21, 26 (2015); Georgios Spanos & Lefteris Angelis, *The Impact of Information Security Events to the Stock Market: A Systematic Literature Review*, 58 COMPUTS. & SEC. 216, 217 (2016); Ali Alper Yayla & Qing Hu, *The Impact of Information Security Events on the Stock Value of Firms: The Effect of Contingency Factors*, 26 J. INFO. TECH. 60, 67 (2011).

82. Katherine Campbell, Lawrence A. Gordon, Martin P. Loeb & Lei Zhou, *The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market*, 11 J. COMPUT. SEC. 431, 433, 444 (2003).

83. Karthik Kannan, Jackie Rees & Sanjay Sridhar, *Market Reactions to Information Security Breach Announcements: An Empirical Analysis*, 12 INT'L J. ELEC. COM. 69, 69 (2007).

84. *Id.* at 86–87.

85. Sanjay Goel & Hany A. Shawky, *Estimating the Market Impact of Security Breach Announcements on Firm Values*, 46 INFO. & MGMT. 404, 405–06 (2009).

86. Lawrence A. Gordon, Martin P. Loeb & Lei Zhou, *The Impact of Information Security Breaches: Has There Been a Downward Shift in Costs?*, 19 J. COMPUT. SEC. 33, 35 (2011).

87. Kannan et al., *supra* note 83.

88. Tawei Wang, Jackie Rees Ulmer & Karthik Kannan, *The Textual Contents of Media Reports of Information Security Breaches and Profitable Short-Term Investment Opportunities*, 23 J. ORGANIZATIONAL COMPUTING & ELEC. COM. 200, 200 (2013).

findings documented in prior studies and showed that security breaches were not associated with stock market performance, audit fees, or internal control weaknesses.[89]

In addition to the direct impact of security breaches on the breached firms' business values, studies have also attempted to examine how such effects may be spilled over to other organizations in the same industry or across industries.[90] For instance, Ettredge and Richardson focused on the distributed denial of service ("DDoS") attacks in February 2000 on internet firms.[91] The authors showed that internet firms that were not attacked also faced a negative stock market reaction during that period.[92] Similarly, Hinz, Nofer, Schiereck, and Trillig demonstrated that the announcement of data thefts resulted in decreases in both the breached firms' and similar firms' stock prices.[93] Differently, Cavusoglu, Mishra, and Raghunathan showed that while the announcement of a security breach was related to a negative stock market reaction, the breach could have a positive effect on the market value of security developers during the breach announcement period.[94] Recently, Wang, Wang, and Yen also documented a similar negative spillover effect for the breached firms and other firms who offered similar products.[95] The authors further showed that such spillover effect is weaker when the breach was caused by internal factors or the loss of personally identifiable information.[96] Moving away from stock price reactions suggested that compared with the breached firms, competitors experienced an increase in abnormal trading volume around the breach announcement date.[97] The spillover effect also suggested an increased level of uncertainty towards the non-breached competitors.

89. Vernon J. Richardson, Rodney E. Smith & Marcia Weidenmier Watson, *Much Ado About Nothing: The (Lack of) Economic Impact of Data Privacy Breaches*, 33 J. INFO. SYS. 227, 249 (2019).

90. Jengchung V. Chen, Hung-Chih Li, David C. Yen & Kenneth Vincent Bata, *Did IT Consulting Firms Gain When Their Clients Were Breached?*, 28 COMPUTS. HUM. BEHAV. 456, 462–63 (2012).

91. Michael L. Ettredge & Vernon J. Richardson, *Information Transfer Among Internet Firms: The Case of Hacker Attacks*, 17 J. INFO. SYS. 71, 71 (2003).

92. *Id.* at 78.

93. Oliver Hinz, Michael Nofer, Dirk Schiereck & Julian Trillig, *The Influence of Data Theft on the Share Prices and Systematic Risk of Consumer Electronics Companies*, 52 INFO. & MGMT. 337, 345 (2015).

94. Huseyin Cavusoglu, Birendra Mishra & Srinivasan Raghunathan, *The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers*, 9 INT'L J. ELEC. COM. 69, 95–96 (2004).

95. Wang et al., *supra* note 35, at 19.

96. *Id.* at 29.

97. Islam et al., *supra* note 47, at 3–4, 7.

2. Crisis Management or Responses to Security Breaches

Crisis management and responding strategies have been a major consideration when discussing risk management. However, prior empirical research in this area is still lacking with only a few exceptions. For instance, Goode, Hoehle, Venkatesh, and Brown focused on the Sony PlayStation Network breach and showed that when customers' expectations of compensation following the breach of their data were met, such compensation can effectively influence customers' service quality perceptions.[98] Wang, Qi, Wang, and Jiang, and Gwebu, Wang, and Wang, respectively, examined the response strategies of the breached firm.[99] For example, Gwebu, Wang, and Wang identified four response strategies taken by breached firms and showed that firms with higher reputations were not affected due to different response strategies.[100] Prior studies have also documented that breached firms may leverage the negative news to manage their earnings or take a big bath especially when their financial reporting quality is lower.[101]

CONCLUSION

Information security breaches have attracted a lot of attention from the public, organizations, and regulators. However, our understanding of security risks is still limited due to their rapidly changing nature, advances in information technology, and the development of different business models. In this study, we have reviewed prior empirical studies in this field on threats and vulnerabilities, governance mechanisms, and impacts and responses. Based on the earlier discussions, we would encourage more studies in the following areas.

First, empirical studies focused on threats and vulnerabilities, especially on emerging challenges that were not commonly noticed in the past, are still limited. Studying threats and vulnerabilities becomes increasingly critical due to the sharing activities among business partners or even among data brokers. More studies can better help us understand the implications brought by the complex network of data sharing and usage.

98. Sigi Goode, Hartmut Hoehle, Viswanath Venkatesh & Susan A. Brown, *User Compensation as a Data Breach Recovery Action: An Investigation of the Sony PlayStation Network Breach*, 41 MIS Q. 703, 718 (2017).

99. Y. Wang, K. Qi, T. Wang & W. Jiang, Firm's Response Strategies After Data Breach and Stock Market Reactions 1 (2020) (unpublished manuscript) (on file with authors); Kholekile L. Gwebu, Jing Wang & Li Wang, *The Role of Corporate Reputation and Crisis Response Strategies in Data Breach Management*, 35 J. MGMT. INFO. SYS. 683, 683 (2018).

100. Gwebu et al., *supra* note 99.

101. *See, e.g.*, Garg et al., *supra* note 61, at 21–23.

In addition, though litigation, reputation, and operational costs have often been discussed in prior studies, empirical studies are still lacking when understanding the actual cost implications. Future studies can attempt to separate the security breach announcements that are due to regulated (for example, breach-notification laws) versus non-regulated reasons in order to better understand the impact on businesses and compliance issues. The new privacy and security regulations, such as GDPR, the California Consumer Privacy Act, or the New York Privacy Act of 2021, can also be considered when understanding their potential impact on organizations' responses in security risk management practices.

Furthermore, cybersecurity insurance became popular in recent years due to the increased number of cyber incidents. However, the risk assessment, the pricing strategies, and the effect on the insured's information security risk management program as relating to cyber breach insurance are still unclear. More studies can help us better understand or provide insights on how this risk transfer strategy, through insurance, may work for both the insurer and the insured.

Last, more studies can focus on the crisis management and disaster recovery strategies. It is still unclear how organizations recover from security breaches and how breaches affect organizations' security risk management practices. The crisis management and disaster recovery lessons learned can be valuable for other organizations as they set their policies and processes in the face of potential breaches.