THE UNIVERSITY OF ARIZONA
ELLER COLLEGE OF MANAGEMENT
Dhaliwal-Reidy
School of Accountancy

DHALIWAL-REIDY
SCHOOL OF ACCOUNTANCY

McClelland Hall, Room 301
P.O. Box 210108
Tucson, AZ 85721-0108

Tel: 520-621-2620
Fax: 520-621-3742

accounting.eller.arizona.edu

May 3, 2022

Honorable Chairman Gary Gensler
Honorable Commissioners Allison Herren Lee, Caroline A. Crenshaw and Hester M. Peirce
U.S. Securities and Exchange Commission
100 F Street NE 100 F Street NE
Washington, DC 20549

Re: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, File number S7-09-22

Dear SEC Commissioners:

I am writing to provide support from academic evidence regarding the SEC's recent proposal on enhancing disclosure requirements related to cyber security events, file number S7-09-22. Cybersecurity is an increasingly important risk as nearly 50% of 4,446 CEOs surveyed across 89 countries view it as a top threat (PWC 2022). The Depository Trust and Clearing Corporation (2018, p.16) argues cybersecurity "may have become the most important near-term threat to financial stability [of the economy]." Further, shareholders perceive it as a significant risk to a firm's growth prospects (PwC 2018).

Not only is cyber risk important and eminent, but data breaches can also be costly. Survey evidence suggests that data breaches can be costly to the firm in terms of loss of revenue, customers, and/or business opportunities (Cisco 2017). Ponemon Institute (2017a) provides evidence that, on average, firms incur $225 in total costs *per record* exposed in a data breach. Recent research suggests data breaches have costly valuation implications such as an undiversifiable priced risk factor, higher cost of debt, lower sales growth, and lower financial reporting quality (Florakis et al. 2020; Jiang et al. 2020; Cisco 2017; Ponemon Institute 2017b; Sheneman 2017; Lawrence et al. 2018; Janakiraman, Lim, and Rishika 2018; Smith, Higgs, and Pinsker 2018; Huang and Wang 2020; Kamiya et al. 2021; Ashraf and Sunder 2021). Ponemon Institute (2017b) finds that the average breached firm experiences a five % drop in stock price after disclosing a breach.

Collectively, this evidence suggests that investors generally find cyber incident disclosures are value relevant.[1] Much academic research suggests there is an important link between information

[1] Ashraf (2021) findings suggest such information may also be relevant to peer firms is assessing and evaluating their cyber exposure, even in the absence of a successful attack.

technology and internal controls (e.g., Messier, Eilifsen and Austen 2004; Li, Peters, Richardson, and Watson 2012), with valuation implications when there are deficiencies. We believe the academic evidence generally suggests there is value and importance in disclosing data breach incidents for many reasons. Below we provide more detail regarding specific points raised in the SEC's proposal and the related academic findings.

1. Costs and benefits of mandating cyber disclosures

Generally speaking, academic research finds that mandating disclosure reduces strategic behavior. More specifically, in the context of cyber disclosures, Ashraf, Jiang, and Wang (2022) conduct a study where they contrast firms headquartered in states that mandate deadlines for disclosing cyber incidents with those that do not have such requirements. Not surprisingly, they find that firms in states that mandate cyber incident disclosure deadlines disclose 90% more quickly than those without mandated deadlines, highlighting the ability to improve disclosure timeliness with laws that mandate timing. Mandated disclosure may increase media coverage of breaches (Romanosky, Telang, and Acquisiti 2011), highlighting additional spillover that improves awareness for investors and potentially impacted customers. Customers with compromised data may better be able to protect themselves from the negative implications of the breach with enhanced disclosure, as disclosure may enhance the ability of affected individuals to seek recourse from breached firms through litigation (e.g., Jones Day 2003). Finally, mandated disclosure may inform peers about potential cyber risks and motivate firms to take real actions to prioritize mitigating cyber risk exposure, reducing the occurrence and financial impact (Ashraf and Sunder 2021). This is consistent with research in other contexts that finds people take real actions to reduce bad outcomes on behalf of stakeholders in response to mandatory disclosure (e.g., Jin and Leslie 2003; Cutler et al. 2004; Lu 2012; Kolstad 2013). The ability of mandated disclosure to reduce the risk of bad outcomes is important because Accenture (2014) reports that 45% of chief information officers perceive they have underinvested in cybersecurity. Further, research evidence supports that mandated disclosure is more effective at reducing the cost of capital relative to voluntary disclosure as it makes non-disclosure more informative. Mandated disclosure laws may also increase the likelihood of retaining cybersecurity expertise in the top management team (Ashraf and Sunder 2021).

Ashraf, Jiang, and Wang (2022) find a negative market response in general to delaying cyber disclosures, suggesting investors value timely cyber incident disclosures. Their analysis also points to a potential cost of increased timeliness. Specifically, nearly 60% of the firms subject to mandated disclosure deadlines provide less detailed disclosures. Further, investors do not have a negative response to disclosure delays motivated by increasing the informativeness of such disclosures. This response points to a trade-off between timeliness and more informative disclosures. The SEC may want to keep this trade-off in mind and consider ways to combat it. More specifically, delayed disclosures that have enhanced detail are not penalized. This suggests the SEC may also want to mandate what information must be disclosed along with the timing, allowing for updated disclosures that omit full details (if unavailable by the deadline) to achieve the improved timeliness and maintain informativeness of the disclosures.

Ashraf (2021) points to a potential unintended cost of mandating disclosures. He finds evidence that more unique and informative cyber risk factor disclosure is present in the absence of mandated requirements by the SEC to make such disclosures. In other words, mandating such cyber risk factor disclosures is associated with more generic and less informative disclosure. However, we note that this evidence is specific to disclosing anticipated bad news in the form of risk disclosures, rather than reporting news of a negative event that occurred, which the current SEC proposal covers. Overall, we still believe investors would benefit from clarity about the timing of such required disclosure and more prescription regarding the content of the disclosure.

2. Strategic Disclosure Concerns

We believe there is value to mandating such disclosures as many cyber incidents may be unreported. Separation of ownership and control, and the existence of externalities, gives rise to opportunistic behavior on behalf of managers (e.g., Jensen and Meckling 1976). Mandating disclosure of cyber events can reduce strategic disclosure, but likely not eliminate it completely.

Choudhary, Sigler, and Ramadas (2021) find a correlation between cyber incidents and the complexity of a company's information technology system related to financial reporting. Companies with the most complex IT financial reporting system (highest complexity across locations, number of customized, purchased, and in-house applications, end-user access, IT modifications, and number of servers) have cyber incidents about 6.4% of the time.[2] Unfortunately, details of IT complexity and, therefore, cyber exposure are typically not provided to investors, highlighting even more value of disclosing cyber incidents as it can provide a signal regarding a company's IT complexity and related controls, which they show have implications for financial reporting reliability.

The current proposal may subject the disclosure decision to an unstated materiality threshold, introducing the possibility of strategic behavior. Specifically, companies are not required to provide investors with quantitative or qualitative materiality disclosures applied in filing financial reporting or related disclosures. Therefore, companies can strategically use such judgment discretion when establishing materiality (e.g., Thompson 2020; Black, Choudhary, and Goodman 2022). Hence, we encourage the SEC to consider requiring companies to disclose the qualitative and quantitative materiality applied in determining this and other financial disclosures to reduce the possibility of such behavior as part of the periodic filings already required.

3. Value of disclosing board expertise related to cybersecurity

Finally, research generally supports the value of IT-related expertise. Survey evidence indicates that audit committees do not easily understand emerging technology risks (KPMG global survey,

[2] In our revised paper we intend to disclose how many cyber incidents in our sample were not publicly disclosed in an SEC filing or new release, subject to PCAOB board approval. However, it is unclear if they unreported incidents are not disclosed because management views the incident as immaterial or if they were unreported for other reasons such as unsuccessful attack.

2014). Ashraf, Michas, and Russomanno (2020) find that information technology expertise on audit committees is associated with a reduction in the propensity of material restatements, a reduction in the propensity of information technology material weaknesses, and more timely earnings announcements highlighting important benefits from this type of expertise and value to disclosing it. They define an IT expert as someone who has worked as a chief information officer or in an IT management role. Their evidence indicates that firms with audit committee IT expertise are 32 % less likely to have a material restatement, 32.6 % less likely to have an IT-related material weakness and announce earnings two days earlier (or about 4 % faster relative to the sample mean). Overall, this suggests an important link between IT expertise and financial reporting reliability and disclosure timeliness and generally supports the SEC's initiative to promote such expertise. Finally, disclosure requirements about cyber expertise may lead companies to focus on recruiting this expertise more frequently, leading to better outcomes.

Thank you for considering what we learn from academic evidence. We hope the Commission is able to consider this and other evidence in support of mandated disclosures of cyber incidents. Enclosed is a list of references that may be useful.

Sincerely,

Preeti Choudhary

Preeti Choudhary
Associate Professor of Accounting
Dhaliwal-Reidy School of Accountancy
University of Arizona

References

Accenture. 2014. High Performers in IT: Defined by Digital. https://www.accenture.com/in-en/~/media/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Technology_4/Accenture-HPIT-Research-Report-Defined-by-Digital.pdf.

Ashraf, M. 2021. Potentially Unintended Consequences of the SEC Restricting Managerial Discretion: Evidence from Cyber Risk Factors. Working paper Michigan State University.

Ashraf, M., and J. Sunder. 2021. Can shareholder benefit from consumer protection disclosure mandates. Working paper Michigan State University and University of Arizona.

Ashraf, M., J. Jiang, and I.Y. Wang. 2022. Are there trade-offs with mandating timely disclosure of cybersecurity incidents? Evidence from state-level Data Breach Disclosure Laws.

Ashraf, M., P. Michas, and D. Russomanno. 2020. The Impcat of Audit Committee Information Technology Expertise on the Reliability and Timeliness of Financial Reporting. The Accounting Review, 95(5), pp 23-56.

Black, J., P. Choudhary, and T. Goodman. 2022. Determinants and Consequences of Management Reporting Materiality Discretion, working paper, Purdue University and University of Arizona.

Choudhary, P, V. Ramadas, and J. Sigler. 2021. The Implications of IT Environment on the Audit and Financial Reporting Quality, working paper University of Arizona, Public Company Accounting Oversight Board, and Xavier University.

Cisco. 2017. Annual Cyber Security Report. *2017 Annual Cybersecurity Report*. https://www.cisco.com/c/dam/m/digital/1198689/Cisco_2017_ACR_PDF.pdf.

Cutler, D. M., R. S. Huckman, and M. B. Landrum. 2004. The role of information in medical markets: An analysis of publicly reported outcomes in cardiac surgery. *American Economic Review* 94 (2): 342–346.

Depository Trust and Clearing Corporation. 2018. The Next Crisis Will Be Different. http://www.dtcc.com/~/media/Files/Downloads/WhitePapers/Systemic-Risk-White-Paper-962018.pdf.

Messier, W. F., Jr. A. Eilifsen, and L.A. Austen. 2004 Auditor detected misstatements and the effect of information technology. International Journal of Auditing (8) 223-235.

Florakis, C., C. Louca, R. Michaely, and M. Weber. 2020. *Cybersecurity Risk*. Working Paper.

Huang, H. H., and C. Wang. 2021. Do banks price firms' data breaches? *The Accounting Review* 96 (3): 261–286.

KPMG. 2014. 2014 global audit committee survey. Available at: https://assets.kpmg.com/content/dam/kpmg/pdf/2014/01/global-auditcommittee-survey-2014.pdf

Janakiraman, R., J. H. Lim, and R. Rishika. 2018. The Effect of a Data Breach Announcement on Customer Behavior: Evidence from a Multichannel Retailer. *Journal of Marketing* 82 (2): 85–105.

Jiang, H., N. Khanna, and Q. Yang. 2020. *The Cyber Risk Premium*. Working Paper.

Jin, G. Z., and P. Leslie. 2003. The Effect of Information on Product Quality: Evidence from Restaurant Hygiene Grade Cards. *The Quarterly Journal of Economics* (May): 409–451.

Jones Day. 2003. Technology Commentaries: California Raises the Bar on Data Security and Privacy. https://www.jonesday.com/California-Raises-the-Bar-on-Data-Security-and-Privacy-09-10-2003/.

Kamiya, S., J.-K. Kang, J. Kim, A. Milidonis, and R. M. Stulz. 2021. Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics* 139 (3): 719–749.

Lawrence, A., M. Minutti-Meza, and D. Vyas. 2018. Is operational control risk informative of financial reporting deficiencies? *Auditing* 37 (1): 139–165.

Li, C., G. Peters, V. Richardson, and M. Watson. 2012. The Consequences of Information Technology Internal Control Weaknesses on Management Information Systems: The case of Sarbanes-Oxley Internal Control Reports. MIS Quarterly 36 (1) 179-203.

Lu, S. F. 2012. Multitasking, Information Disclosure, and Product Quality: Evidence from Nursing Homes. *Journal of Economics and Management Strategy* 21 (3): 673–705.

PricewaterhouseCoopers (PwC). 2018. 2018 Global Investor Survey. Available at: https://www.pwc.com/gx/en/ceo-survey/2018/deep-dives/pwc-global-investor-survey-2018.pdf.

PricewaterhouseCoopers (PwC). 2022. 25th Annual Global CEO Survey - PwC. Available at: https://www.pwc.com/gx/en/ceo-agenda/ceosurvey/2022.html.

Ponemon Institute. 2017a. 2017 Cost of Data Breach Study: United States. Available at: http://info.resilientsystems.com/hubfs/IBM_Resilient_Branded_Content/White_Papers/2017_Global_CODB_Report_Final.pdf.

Ponemon Institute. 2017b. The Impact of Data Breaches on Reputation & Share Value. Available at: https://www.centrify.com/media/4737054/ponemon_data_breach_impact_study.pdf.

Romanosky, S., R. Telang, and A. Acquisti. 2011. Do data breach disclosure laws reduce identity theft? *Journal of Policy Analysis and Management* 30 (2): 256–286.

Sheneman, A. G. 2017. *Cybersecurity Risk and the Cost of Debt*. Working Paper.

Smith, T., J. Higgs, and R. Pinsker. 2018. Do Auditors Price Breach Risk in Their Audit Fees? *Journal of Information Systems*.

Thompson, R. 2020. Reporting Misstatements as Revisions: An evaluation of Manager's use of Materiality Discretion.

Walton, S., P. Wheelter, Y. Zhang. 2021. An Integrative Review and Analysis of Cybersecurity Research: Current State and Future Directions 35 (1): 155–186.