MICHIGAN STATE UNIVERSITY

THE UNIVERSITY OF ARIZONA

May 8, 2022

**The Eli Broad College of Business**

Accounting and Information Systems

Michigan State University
North Business Complex
632 Bogue Street, Rm N270
East Lansing, MI 48824

Phone: 517-355-7486
Fax: 517-432-1101
Accounting.broad.msu.edu

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

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

Dear SEC Commissioners,

We are business professors at Michigan State University and The University of Arizona. We write to you to share research-backed insights on the potential effects of the SEC's recently proposed cybersecurity disclosure rule (file number S7-09-22). We organize our comments in six parts:

- Trade-offs of requiring firms to disclose cyber incidents within an explicit deadline
- Cybersecurity benefits of requiring firms to disclose cyber incidents
- Unintended consequences of providing firms with more structure when disclosing cybersecurity risk factors
- Benefits of having a board member with information technology or cybersecurity expertise
- Spillover benefits of cyber incident disclosures
- Concluding remarks

**Trade-offs of requiring firms to disclose cyber incidents within an explicit deadline**

Findings in Academic Research

Data breach notification laws are U.S. state-level laws that require firms to disclose the occurrence of a data breach to people whose personal information is leaked in the breach. Some of these data breach notification laws require firms to disclose the occurrence of a data breach within a certain deadline while other data breach notification laws do not mandate an explicit deadline. Ashraf, Jiang, and Wang (2022)[1] examine how having an explicit deadline to disclose the occurrence of a data breach impacts the timing and information content of that data breach disclosure. They find that:

- firms facing an explicit deadline disclose the occurrence of a data breach 89.82 percent faster than firms without such a deadline;
- firms facing an explicit deadline are 57.71 percent less likely to include details about how the breach happened and what data was leaked; and

[1] Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4068575.

**The Eli Broad College of Business**

Accounting and Information Systems

Michigan State University
North Business Complex
632 Bogue Street, Rm N270
East Lansing, MI 48824

Phone: 517-355-7486
Fax: 517-432-1101
Accounting.broad.msu.edu

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

- investors respond more negatively to the occurrence of a data breach when firms delay disclosure, but investors are more forgiving (i.e., less of a negative reaction) when the delay is used to gather and report breach details.

Implications for New Proposed Rule

Ashraf et al. (2022)'s findings suggest that there is a trade-off when mandating an explicit short deadline to disclose the occurrence of a cyber incident: requiring firms to disclose a cyber incident within four days of discovery – as the new SEC rule proposes – will likely result in faster disclosure that contain less information content about the cyber incident.

Given the findings of Ashraf et al. (2022), there are two potential paths forward – a single disclosure regime or a two-step disclosure regime.

Under a single disclosure regime, the proposed four days deadline likely needs to be extended to a longer deadline, to allow for enough time to include important details in the disclosure. While it is difficult to say what the "optimal" deadline should be, a longer time frame would be required if the new rule's intention is to increase the informativeness of the disclosure.

An alternative to the single disclosure regime is to mandate a two-step disclosure regime. Step one is to require firms to issue a skeleton disclosure to inform investors, via 8-K, about the occurrence of a cyber incident within four days of discovery. Step two is to require the initial disclosure to be followed up with a second comprehensive disclosure detailing the cyber incident at some point after the initial skeleton disclosure (e.g., 30 or 60 days after). The two-step disclosure regime may even allow the SEC to reduce the four days disclosure deadline to something as short as 24 hours, if firms are only making a skeleton disclosure initially.

**Cybersecurity benefits of requiring firms to disclose cyber incidents**

Findings in Academic Research

Ashraf and Sunder (2022)[2] study the effects of data breach notification laws on firms' cybersecurity investments and oversight. They document that firms increase their investments in cybersecurity after these laws have been passed, because firms desire to avoid disclosing bad news (i.e., firms want to avoid having to incur a data breach that firms would now need to disclose). Overall, this enhanced focus on cybersecurity ultimately benefits shareholders through a decreased cost of equity capital and higher firm value.

[2] Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3308551.

The Eli Broad College of Business

Accounting and Information Systems

Michigan State University
North Business Complex
632 Bogue Street, Rm N270
East Lansing, MI 48824

Phone: 517-355-7486
Fax: 517-432-1101
Accounting.broad.msu.edu

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

Implications for New Proposed Rule

The findings of Ashraf and Sunder (2022) suggest that mandating firms to disclose the occurrence of cyber incidents in 8-K filings will create stronger incentives for firms to enhance their cybersecurity, through greater investments in cybersecurity, in order to decrease the chance of a cyber incident that firms must now disclose to investors.

**Unintended consequences of providing firms with more structure when disclosing cybersecurity risk factors**

Findings in Academic Research

Ashraf (2021)[3] studies how greater SEC guidance on cybersecurity risk factors impacts the structure of these risk factor disclosures. He documents herding behavior: after the SEC's 2011 cyber risk disclosure guidance, firms issued less unique cybersecurity risk factors and started issuing risk factors that more closely match the wording of the SEC's 2011 guidance. He also finds that shareholders find more unique (not boilerplate) cybersecurity risk factor disclosures to be more informative.

Implications for New Proposed Rule

If the SEC issues further guidance on how firms should disclose cybersecurity risk factors, the findings of Ashraf (2021) suggests that firms will herd towards what the firms think the SEC wants them to disclose rather than disclosing risk factors that appropriately represent a firm's cybersecurity risk.

**Benefits of having a board member with information technology or cybersecurity expertise**

Findings in Academic Research

Ashraf, Michas, and Russomanno (2020)[4] study the impact an audit committee information technology expert has on firm's financial reporting quality. They find that firms with such experts have higher quality financial reporting, in part due to the expertise this board member brings to the table about cybersecurity.

Implications for New Proposed Rule

The findings of Ashraf et al. (2020) suggest that requiring a information technology or cybersecurity expert on the board may ultimately benefit shareholders.

[3] Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3807487.
[4] Available at https://meridian.allenpress.com/accounting-review/article/95/5/23/431229/The-Impact-of-Audit-Committee-Information.

The Eli Broad College of Business

Accounting and Information Systems

Michigan State University
North Business Complex
632 Bogue Street, Rm N270
East Lansing, MI 48824

Phone: 517-355-7486
Fax: 517-432-1101
Accounting.broad.msu.edu

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

**Spillover benefits of cyber incident disclosures**

Findings in Academic Research

Ashraf (2022)[5] studies the spillover effects of data breaches. He documents that non-breached firms enhance their cybersecurity after a peer firm has a data breach.

Implications for New Proposed Rule

To the extent that disclosure of a cyber incident via 8-K increases market-wide news dissemination of that incident, the findings of Ashraf (2022) suggest that a spillover benefit of mandating these 8-K disclosures is that unaffected firms will see the negative peer news and enhance their own cybersecurity.

**Concluding remarks**

We hope the above-referenced academic studies are able to provide helpful insights as the SEC debates whether and how to finalize its recent proposal regarding cybersecurity disclosures.

We are all available and happy to discuss these issues further.

Sincerely,

Jayanthi Sunder
Dhaliwal-HSLopez Professor in Accounting at The University of Arizona
[redacted]

Isabel Yanyan Wang
Deloitte/Michael Licata Professor in Accounting at Michigan State University
[redacted]

John Xuefeng Jiang
Plante Moran Professor in Accounting at Michigan State University
[redacted]

Musaib Ashraf
Assistant Professor in Accounting at Michigan State University
[redacted]

[5] Available at https://meridian.allenpress.com/accounting-review/article/97/2/1/463979/The-Role-of-Peer-Events-in-Corporate-Governance.