Spring 2023

Board Gender Diversity and Cybersecurity Disclosure Characteristics

Katie Remeis
University of New Hampshire

Board Gender Diversity and Cybersecurity Disclosure Characteristics

By: Katie Remeis

Advisor:
Dr. Jonathan Nash
Assistant Professor of Accounting

Peter T. Paul College of Business and Economics
University of New Hampshire

Introduction

This study explores how board gender diversity impacts the cybersecurity disclosures of publicly traded companies. Cybersecurity is a growing concern for business executives and investors. The PwC 2022 Global Investor survey found that 43% of investors are concerned about cyber risk and 51% of investors think ensuring data security and privacy should be a top five priority for businesses. 49% of investors think ensuring effective corporate governance should be a top five priority. Additionally, 89% of investors use the financial statements and note disclosures to assess how companies manage opportunities and risks (PwC 2022).

Extensive prior literature has studied both cybersecurity disclosures and the impact of board gender diversity separately. There is a gap in the current research studying the impact of board gender diversity on cybersecurity disclosures. This study helps to close that gap by examining how board gender diversity affects cybersecurity related disclosures of breached firms. Cybersecurity disclosures were hand collected for 180 publicly traded companies that had a reported cyber breach. Disclosures were collected for the year before the breach occurred (*t-1*) and the year after (*t+1*). Analysis of the differences in the disclosures indicates that companies with a significant number of women on the board of directors are more likely to publish cybersecurity disclosures.

Literature Review

Cyber Risk

IBM's 2022 Cost of a Data Breach Report studied 550 organizations that were impacted by data breaches that occurred between March 2021 and March 2022. The organizations were from

17 different industries and located in 17 different countries/regions. 83% of the organizations had more than one data breach. 60% of breaches caused price increases for consumers. The average cost of a data breach in the United States was 9.44 million dollars, the highest average cost out of all the countries in the study. The United States has had the highest average cost of a data breach for 12 years in a row. The average cost of a data breach across the globe is 4.35 million dollars, an increase of 2.6% since 2021 and a 12.7% increase since 2020 (IBM, 2022).

Various studies have looked at the factors that increase and decrease the risk of cybersecurity breaches. Internal control weaknesses and noncompliance issues are indicators of future cybersecurity incidents (Steinbart et al., 2012). The presence of an IT executive in the top management team has been associated with a reduced risk of cybersecurity breaches (Kwon, et al., 2013). External auditors perceive firms with prior cybersecurity breach incidents as being higher risk and respond by performing additional audit procedures. Consistent with this conclusion, research finds that audit fees increase for companies after they have a cybersecurity incident (Li et al., 2020).

SEC Guidance

In 2011, the SEC issued guidance regarding cybersecurity disclosures. The guidance was aimed at helping companies decide what disclosures related to cybersecurity, if any, should be included in the financial statements (SEC, 2011). The SEC has issued comment letters to companies with inadequate cybersecurity disclosures. To respond to a SEC comment letter, companies must clarify their existing disclosure and amend their filing. They often agree to change their disclosure practices going forward as well. If a company does not resolve the issues by the time of their following year's 10-K, they need to disclose the matter in Item IB of the 10-K (Brown

et al., 2018). The SEC is encouraging firms to make these disclosures without using unnecessarily complex language, so that the disclosures are easier to read and understand.

More recently, the SEC has proposed standardized cybersecurity disclosure rule with the objective of ensuring the market has adequate information about companies' cybersecurity breaches. The SEC has expressed concern that some cybersecurity incidents are covered in the media but not disclosed in the periodic filings by the affected company. Disclosures are not always consistent or complete. If the proposed rules are approved, companies will have to disclose information about material breaches. After determining whether a breach meets the materiality threshold, firms will have four days to disclose information about the breach to regulators and investors. Companies will have to disclose when the breach took place, whether or not the breach is ongoing and the nature and scope of the breach. They will also have to disclose information about what data was stolen or accessed, the overall effect of the breach on the company, and whether or not the company has remediated the breach (Harrington, 2022).

Cybersecurity Disclosures

There is some concern that cybersecurity disclosures could benefit hackers and increase the risk of future cybersecurity breaches. Li et al. (2018) found that firms with prior cybersecurity disclosures were more likely to experience future cybersecurity incidents. This risk of future incidents increased as the length of the prior cybersecurity disclosure increased. Additionally, firms mentioning the existence of trade secrets in their disclosures have a higher risk of being breached (Ettredge et al., 2018). However, there is also evidence that when companies disclose information about their preventative measures against cybersecurity breaches, they are less likely to have a subsequent cybersecurity incident (Wang et al., 2013).

Regulators have the ability to influence cybersecurity disclosures. The Sarbanes-Oxley Act of 2002 (SOX) requires the CEO's and CFO's of publicly traded companies to accept responsibility for adequate financial reporting and appropriate internal control systems within their company. SOX does not require companies to disclose their information security activities. After the passage of SOX, the number of companies who voluntarily disclosed information on information security increased (Gordon et al., 2006). There is also evidence that SEC comment letters have a spillover effect and can increase the quality of cybersecurity disclosures. Even if a company did not receive a SEC comment letter, they are more likely to modify the following year's cybersecurity disclosure if an industry leader, close rival, or other industry peers received comment letters from the SEC (Brown et al., 2018).

Gender Diversity in Corporate Governance

Several studies have concluded that greater gender diversity on a board of directors leads to a more effective board. Gender diverse boards are more likely to discuss sensitive and tough issues than boards consisting of all men (Clarke, 2005). Other studies have found that women directors are more likely to question board processes and ask awkward questions (Herring, 2009). Females have been found to be less self-interest oriented than men, therefore improving the board's decision-making process and increasing the board's effectiveness (Coffey and Wang, 1998). Women have been found to be more committed and more diligent than their male peers (Huse and Solberg, 2006). Evidence has proven that women directors prepare for meetings more than men and have better attendance records. Additionally, women are more likely to join monitoring activities (Adams and Ferreira, 2009), and board gender diversity is associated with increased board strategic control and a reduction in conflict within the board (Nielsen and Huse, 2010).

There is also evidence suggesting that women are more risk averse than men (Beckmann and Menkhoff, 2008). One study found that female executives issue less debt than males and place wider bounds on their earnings forecasts. This suggests that women are more risk averse than their male counterparts (Huang and Kisgen, 2013). Eaton et al. (2019) found that this higher risk aversion contributed to an increase in risk disclosure.

Other research has looked at board gender diversity and disclosures. Liao et al. (2015) found that a greater proportion of female directors on a board increases the propensity and extensiveness of greenhouse gas disclosure. Another study found that a greater percentage of women on the board increases the likelihood of voluntary disclosure of climate change related risks (Ben-Amar et al., 2017). Board diversity has also been associated with more transparent disclosures (Upadhyay and Zeng 2014).

Greater gender diversity on boards has also been shown to reduce fraud. A study with data from 128 publicly listed companies in Australia found that more women on boards was associated with lower occurrences of fraud. More specifically, the study found that a 10% increase in women on the board reduced the probability of fraud by 0.1 percentage points (Capezio and Mavisakalyan, 2016). In an experiment, female participants were more likely to report fraud (Kaplan et al., 2009). Gender diverse boards have also been found to commit less financial reporting mistakes and engage in less fraud schemes (Wahid 2019). Additionally, females on the board of directors have been found to reduce the likelihood of internal control weaknesses. Even having one female board member improved the Internal Controls over Financial Reporting quality (Chen et al., 2016).

Several studies have investigated the number of women needed on a board of directors in order to make a meaningful difference. If there are not enough women on the board, the women may simply be tokens of diversity and the benefits of greater diversity may not be obtained. Several

studies have supported the critical mass theory, the idea that a minimum of three women need to be on a board in order to make a noticeable impact (Konrad et al., 2008; Radu and Smaili, 2022). However, other studies do not support the critical mass of three women. Ben-Amar et al. (2017) found that boards need to have at least two women in order to influence climate change strategy disclosures. Chen et al (2016) found that having even one female board member improves the quality of internal controls over financial reporting.

Research related to gender diversity and cybersecurity disclosures is limited. A recent study was conducted with data from companies listed on the TSX 60 index from 2014 to 2018. The index is made up of 60 large companies, from nine different industries, listed on the Toronto Stock Exchange. The study concluded that the presence of cybersecurity disclosures is positively associated with gender diversity in corporate governance. The study also supports the critical mass theory, finding that three women need to be on the board of directors in order to notice a change in the cybersecurity disclosures (Radu and Smaili, 2022).

Gender Diversity Legislation

Given the benefits of greater gender diversity in the workforce, both for business and for society, many governments have added gender diversity legislation to reduce the gender gap. Many of these laws have been effective. One study found that the level of gender gap in a country is associated with the proportion of companies with at least 3 women on the board of directors (Fernandez-Feijoo et al., 2014). Having a minimum of 3 women on the board is important, due to the vast number of studies that support the critical mass theory.

Countries have gone about adding gender diversity legislation in different ways. Norway, Spain, France and Italy have all introduced mandatory quotas for female representation on

corporate boards. Countries with legislated quotas have much higher percentages of women on their boards (De Anca, 2008). In Canada, the Ontario Securities Commission introduced a Comply or Explain rule in 2014. Prior to 2014, companies did not have to report the proportion of women directors or their gender diversity policies. Companies listed on the Toronto Stock Exchange are required to report the number of women on their board and in senior management annually. They also need to report whether they have internal targets for gender diversity.

Since 1966, the Equal Employment Opportunity Commission has required any company with over 100 employees in the United States to report on their diversity. This is called the EEO-1 reporting mandate. The mandatory report requires information on racial, ethnic, and gender for each employee. In 2018, close to 75,000 employers filed these reports (Rubin). The data from the reports can be found on the US Equal Employment Opportunity Commission website.

While the United States federal government has not passed any gender diversity mandate legislation, some states have passed laws regarding gender diversity. California passed bill SB 826 in 2018. The bill required that any publicly listed companies headquartered in California have a minimum of two female directors if the board has five or less members. If the board has six or more members, the board needs to have at least three female directors. Fines for noncompliance were set at $100,000 for the first violation and $300,000 for each subsequent violation. Failing to provide the required information to the state would also result in a fine of $100,000 (Shepherd). A Los Angeles Superior Court Judge found the law unconstitutional, so the law has been blocked (Muñoz). The case is expected to go to appeal (Shepherd).

In March 2020, the governor of Washington state, signed Senate Bill 6037 into law. The law went into effect January 1st, 2022. The bill requires public companies incorporated in the state of Washington to have boards of directors consisting of at least 25% women. The law does not

apply to companies that are headquartered in Washington, if they are incorporated in a different state. The law has exceptions for emerging growth companies and smaller reporting companies. Emerging growth companies generally have less than $1 billion in revenue and have recently gone public. If a company does not comply with the 25% threshold, no fines will be imposed. Rather, the company must disclose the measures taken to address the lack of diversity. If the company also fails to disclose their diversity practices, shareholders can go to court and get a court order requiring the company to give the disclosure (Guevara).

Some stock exchanges in the United States have taken measures to try to increase diversity on boards. Nasdaq enacted a board diversity rule that went into effect in August 2022. Corporations listed on Nasdaq are required to disclose the gender and ethic makeup of their boards. If corporations do not currently have at least two diverse board members, they will need to provide an explanation. There is no plan in place to encourage companies to increase the number of diverse board members beyond two (Muñoz).

The New York Stock Exchange has not implemented any board diversity requirements, but they did launch the NYSE Board Advisory Council in 2019. The New York Stock Exchange is taking a market-based approach to increasing board diversity. The council identifies board ready candidates from underrepresented groups and provides them with educational and networking opportunities. The council hosts live events to connect the candidates with companies listed on the exchange that are looking to add more diverse members to their boards. The council hosts an annual networking summit each year. Since 2019, the council has led to over 500 meetings between board leaders and diverse candidates. Over 30 of the council's candidates have joined boards and the candidate pool has grown to about 300 individuals (King).

Hypotheses

Given the growing concern among investors about cybersecurity incidents and the increase in SEC comment letters regarding cybersecurity risk disclosures, an increasing number of companies are publishing cybersecurity risk disclosures. Close to 90% of investors use financial statements to evaluate how a company is managing their risks (PwC 2022). After a cyber breach has occurred, investors will likely expect to see more information regarding cybersecurity risk, especially if the company did not disclose any information about the risk previously. I expect that after a cybersecurity breach, companies will be more likely to publish a cybersecurity risk disclosure. Therefore hypothesis 1 is as follows:

H1: Firms will be more likely to include a disclosure about cybersecurity risk in their 10-k after a breach has occurred

Prior literature shows that women are more risk averse than men ((Beckmann and Menkhoff, 2008). Prior research also shows that having females on the board of directors increases voluntary disclosures related to climate change risks (Ben-Amar et al., 2017). Based on this prior research, I think having women on the board of directors will result in better cybersecurity risk disclosures for a given company. If that is that case, companies with a significant number of women on the board will be more likely to publish cybersecurity risk disclosures. Hypothesis 2 is as follows:

H2: Firms with a significant number of women on the board of directors will be less likely to be missing a cybersecurity risk disclosure than firms without a significant number of women directors.

Methodology

Sample Selection

Audit Analytics was used to identify 180 publicly traded companies that disclosed a cybersecurity breach in SEC filings. Then, two cybersecurity risk disclosures were hand collected for each of the 180 companies that had experienced and reported a breach, one from the 10-k filed the year preceding the breach (*t-1*) and one from the 10-k the year after (*t+1*). This yielded a sample of 360 cybersecurity risk disclosures.

Variables

Three variables related to the characteristics of the disclosures were examined. The first variable tested was *MISSING*, which was coded 1 if the company had a cybersecurity risk disclosure, and 0 otherwise. The second variable, *LENGTH*, was defined as the number of characters in each cybersecurity risk disclosure. The third variable, *COMPLEXITY*, was defined as the Flesch Reading Ease Score for each cybersecurity risk disclosure. To test the second hypothesis, the variable *FEM* was coded 1 if 25% or more of the board of directors were women, and 0 otherwise.[1] The data on board gender diversity was taken from the BoardEx database.

Results

Table 1 presents statistics related to the first hypothesis. The three variables of interest are presented separately for years *t-1* and *t+1*. The prior year disclosures are shown in the NY = 0

[1] A percentage was used because prior literature suggests gender diversity has an effect when a critical mass of women are on the board, typically three women. If not enough women are on the board, they may simply be tokens of diversity and have no effect on cybersecurity risk disclosures (Konrad et al., 2008; Radu and Smaili, 2022)

column and subsequent year disclosures are shown in the NY = 1 column. Differences across the two periods for the variables *MISSING* and *LENGTH* are statistically significant. 10% of companies did not publish a cybersecurity risk disclosure before a breach. After a breach, less than 4% of companies had a missing cybersecurity risk disclosure. The difference is significant ($p = 0.02$). The average number of characters in prior year risk disclosures was 2,085. This number increases to 3,554 characters for risk disclosures published after the cybersecurity breach. Again, the difference is statistically significant ($p < 0.01$). Risk disclosures were slightly more complex in the year following a breach, but the difference is not significant.

TABLE 1

Disclosure Means

Variable	***PY = 0***	***NY = 1***	***P-Val***	
MISSING	0.100	0.039	0.022	**
LENGTH	2,085	3,554	0.001	***
COMPLEXITY	27.827	27.929	0.974	

Table 1 presents the mean values of the variables *MISSING*, *LENGTH*, and *COMPLEXITY*. *MISSING* is defined 1 if the firm did not include a disclosure indicative of cybersecurity risk, and 0 otherwise. *LENGTH* is defined as the number of characters in the cybersecurity risk disclosure, if available. *COMPLEXITY* is defined as the Flesch Reading Ease Score for the cybsersecurity risk disclosure, if available. The sample include observations associated with 180 firms that disclosed a cybersecurity breach in an SEC filing (year *t*). The variable *NY* is coded 1 for observations from the year after the cybersecurity breach (*t+1*), and 0 for observations from the year before the cybersecurity breach (*t-1*). ***, **, and * indicate statistical significance at the 0.01, 0.05, and 0.10 levels, respectively, using a 2-tailed test.

Table 2 provides statistics related to the second hypothesis. Panel A shows means for the variables *MISSING*, *LENGTH* and *COMPLEXITY* separately for firms where *FEM* = 0 and *FEM*

= 1 for the prior year risk disclosures. Panel B shows the *LENGTH* and *COMPLEXITY* variables for the breach disclosure. Panel C shows the *MISSING*, *LENGTH* and *COMPLEXITY* variables for the next year cybersecurity risk disclosures based on the *FEM* values.

Panels A and C show companies with boards of directors consisting of at least 25% women were less likely to have a missing cybersecurity risk disclosure, both year *t-1* and *t+1*. The difference is significant in year *t+1* ($p < 0.01$). None of the firms with a significant number of women on the board omitted a cybersecurity disclosure in the year after a cybersecurity breach. This provides some support for the second hypothesis.

Panels A and B also show that firms with a significant number of women on the board are likely to publish shorter, based on the number of characters, cybersecurity risk disclosures. Differences in the variable *LENGTH* are significant in the year following a cybersecurity breach ($p = 0.08$). This result provides weak evidence that the cybersecurity breach disclosures are shorter and less complex for companies with more than 25% women directors.[2]

[2] One potential explanation for the differences being insignificant is the small sample size. Future researchers might consider expanding the sample to determine whether or not the documented relation exists.

TABLE 2

Disclosure Means By Board Characteristics

Panel A: Prior Year (PY) Disclosures

Variable	*FEM = 0*	*FEM = 1*	*P-Val*	
MISSING	0.094	0.077	0.570	
LENGTH	2,039	1,852	0.507	
COMPLEXITY	28.191	21.830	0.928	

Panel B: Breach Disclosures

Variable	*FEM = 0*	*FEM = 1*	*P-Val*	
LENGTH	1,473	1,211	0.408	
COMPLEXITY	64.153	53.501	0.241	

Panel C: Subsequent (NY) Disclosures

Variable	*FEM = 0*	*FEM = 1*	*P-Val*	
MISSING	0.057	0.000	0.000	***
LENGTH	3,343	1,811	0.085	*
COMPLEXITY	26.569	30.751	0.528	

Table 2 presents the mean values of the variables *MISSING*, *LENGTH*, and *COMPLEXITY* separately for firms with a significant number of female directors (*FEM* = 1) and without (*FEM* = 0). *FEM* is defined 1 if at least 25 percent of a firm's directors, and 0 otherwise. *MISSING* is defined 1 if the firm did not include a disclosure indicative of cybersecurity risk, and 0 otherwise. *LENGTH* is defined as the number of characters in the disclosure. *COMPLEXITY* is defined as the Flesch Reading Ease Score for the cybersecurity risk disclosure, if available. The sample include observations associated with 92 firms that disclosed a cybersecurity breach in an SEC filing (year t) and had director data available in BoardEx. There are 39 firms where *FEM* = 1 and 53 firms where *FEM* = 0. ***, **, and * indicate statistical significance at the 0.01, 0.05, and 0.10 levels, respectively, using a 2-tailed test.

Conclusion

This study provides evidence that having a significant number of female directors can be beneficial for a company's cybersecurity risk disclosures. Companies are more likely to publish a cybersecurity risk disclosure after a cyber breach has occurred. Companies are significantly more likely to publish a cybersecurity risk disclosure in the year following a breach if at least 25% of

the directors on the board are women. This is extremely important given the growing risk of cybersecurity breaches. Investors' concern regarding cybersecurity is growing and they will be looking at the risk disclosures to learn more.

This study further supports prior literature that shows that more than one women director is needed to make a noticeable impact. This study split companies based on whether or not 25% of their board members were women. This is important for companies to understand when putting together their board of directors. In order to gain the benefits of a gender diverse board, they need to have more than one woman director.

This study contributes to the existing literature because is the first study that uses hand collected data to look at cybersecurity risk disclosures of companies that have experienced a cybersecurity incident. Future opportunities for research include examining the impact of gender diversity on the board of directors and the complexity of cybersecurity risk disclosures, as the results from this study for the *COMPLEXITY* variable were not statistically significant. Other opportunities include examining impact of gender diversity on the length and complexity of cybersecurity breach disclosures, as the *LENGTH* and *COMPLEXITY* variables for breach disclosures were not statistically significant in this study.

Work Cited

Adams, R. B., & Ferreira, D. (2009). Women in the boardroom and their impact on governance and performance. *Journal of Financial Economics*, *94*(2), 291-309.

Beckmann, D., & Menkhoff, L. (2008). Will women be women? Analyzing the gender difference among financial experts. *Kyklos*, *61*(3), 364-384.

Ben-Amar, W., Chang, M., & McIlkenny, P. (2017). Board gender diversity and corporate response to sustainability initiatives: Evidence from the carbon disclosure project. *Journal of Business Ethics*, *142*(2), 369-383.

Brown, S. V., Tian, X., & Wu Tucker, J. (2018). The spillover effect of SEC comment letters on qualitative corporate disclosure: Evidence from the risk factor disclosure. *Contemporary Accounting Research*, *35*(2), 622-656.

Capezio, A., & Mavisakalyan, A. (2016). Women in the boardroom and fraud: Evidence from Australia. *Australian Journal of Management*, *41*(4), 719-734.

Chen, Y., Eshleman, J. D., & Soileau, J. S. (2016). Board gender diversity and internal control weaknesses. *Advances in Accounting*, *33*, 11-19.

Clarke, C. J. (2005). The XX factor in the boardroom: why women make better directors. *Directors Monthly*, *24*(47), 8-10.

Coffey, B. S., & Wang, J. (1998). Board diversity and managerial control as predictors of corporate social performance. *Journal of Business Ethics*, *17*(14), 1595-1603.

De Anca, C. (2008). Women on corporate boards of directors in Spanish listed companies. *Women on Corporate Boards of Directors: International Research and Practice*, 96-107.

Eaton, T. V., Grenier, J. H., & Layman, D. (2019). Accounting and cybersecurity risk management. *Current Issues in Auditing*, *13*(2), C1-C9.

Ettredge, M., Guo, F., & Li, Y. (2018). Trade secrets and cyber security breaches. *Journal of Accounting and Public Policy*, *37*(6), 564-585.

Fernandez-Feijoo, B., Romero, S., & Ruiz-Blanco, S. (2014). Women on boards: do they affect sustainability reporting?. *Corporate Social Responsibility and Environmental Management*, *21*(6), 351-364.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Sohail, T. (2006). The impact of the Sarbanes-Oxley Act on the corporate disclosures of information security activities. *Journal of Accounting and Public Policy*, *25*(5), 503-530.

Guevara, N. (2021, February 28). *What to Know About Washington's New Rules for Boardroom Diversity*. Puget Sound Business Journal. Retrieved December 13, 2022, from https://www.bizjournals.com/seattle/news/2021/02/28/washington-state-aims-to-make-boards-more-diverse.html

Harrington, D. (2022, June 1). *SEC Cybersecurity Disclosure Requirements' Impact on Your Business*. Varonis. Retrieved December 13, 2022, from https://www.varonis.com/blog/sec-cybersecurity-disclosure-requirements#:~:text=Disclose%20when%20the%20breach%20took,incident%20on%20the%20company's%20operations

Herring, C. (2009). Does diversity Pay?: Race, gender, and the business case for diversity. *American Sociological Review*, *74*(2), 208-224.

Huang, J., & Kisgen, D. J. (2013). Gender and corporate finance: Are male executives overconfident relative to female executives?. *Journal of Financial Economics*, *108*(3), 822-839.

Huse, M., & Solberg, A. G. (2006). Gender-related boardroom dynamics: How Scandinavian women make and can make contributions on corporate boards. *Women in Management Review*.

IBM. (2022). *Cost of a Data Breach 2022*. IBM. Retrieved December 13, 2022, from https://www.ibm.com/reports/data-breach

Kaplan, S., Pany, K., Samuels, J., & Zhang, J. (2009). An examination of the association between gender and reporting intentions for fraudulent financial reporting. *Journal of Business Ethics*, *87*(1), 15-30.

King, E. (2022, June 16). *The Importance of the NYSE's Market-Driven Approach to Board Diversity*. NYSE. Retrieved December 13, 2022, from https://www.nyse.com/boardadvisory/the-importance-of-the-nyse-s-market-driven-approach-to-board-diversity

Konrad, A. M., Kramer, V., & Erkut, S. (2008). The impact of three or more women on corporate boards. *Organizational Dynamics*, *37*(2), 145-164.

Kwon, J., Ulmer, J. R., & Wang, T. (2013). The association between top management involvement and compensation and information security breaches. *Journal of Information Systems*, *27*(1), 219-236.

Li, H., No, W. G., & Boritz, J. E. (2020). Are external auditors concerned about cyber incidents? Evidence from audit fees. *Auditing: A Journal of Practice & Theory*, *39*(1), 151-171.

Li, H., No, W. G., & Wang, T. (2018). SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. *International Journal of Accounting Information Systems, 30,* 40-55.

Liao, L., Luo, L., & Tang, Q. (2015). Gender diversity, board independence, environmental committee and greenhouse gas disclosure. *The British Accounting Review*, *47*(4), 409-424.

Muñoz, A. (2022, August 8). *Nasdaq's Rule on Board Diversity is a Good First Step, Not a Gold Standard*. Fortune. Retrieved December 13, 2022, from https://fortune.com/2022/08/08/nasdaq-new-rule-board-diversity-sec-aracely-munoz/

Nielsen, S., & Huse, M. (2010). The contribution of women on boards of directors: Going beyond the surface. *Corporate Governance: An International Review*, *18*(2), 136-148.

PwC. (2022). *PwC's Global Investor Survey 2022: ESG Execution Gap*. PwC. Retrieved December 13, 2022, from https://www.pwc.com/gx/en/issues/esg/global-investor-survey-2022.html

Radu, C., & Smaili, N. (2022). Board gender diversity and corporate response to cyber risk: evidence from cybersecurity related disclosure. *Journal of Business Ethics, 177*(2), 351-374.

Rubin, J. (2022, June 13). *Show or Tell: A Road Map for Board Diversity Laws*. Bloomberg Law. Retrieved December 13, 2022, from https://news.bloomberglaw.com/daily-labor-report/show-or-tell-a-road-map-for-board-diversity-laws

SEC. (2011, October 13). *CF Disclosure Guidance: Topic No. 2*. SEC. Retrieved December 13, 2022, from https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

Shepherd, L. (2022, June 1). *Court Overturns California Law Requiring Women on Boards of Directors*. SHRM. Retrieved December 13, 2022, from https://www.shrm.org/resourcesandtools/legal-and-compliance/state-and-local-updates/pages/california-court-overturns-law-requiring-women-on-boards-of-directors.aspx

Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2012). The relationship between internal audit and information security: An exploratory investigation. *International Journal of Accounting Information Systems*, *13*(3), 228-243.

Upadhyay, A., & Zeng, H. (2014). Gender and ethnic diversity on boards and corporate information environment. *Journal of Business Research*, *67*(11), 2456-2463.

Wahid, A. S. (2019). The effects and the mechanisms of board gender diversity: Evidence from financial manipulation. *Journal of Business Ethics*, *159*(3), 705-725.

Walton, S., Wheeler, P. R., Zhang, Y. I., & Zhao, X. R. (2021). An integrative review and analysis of cybersecurity research: Current state and future directions. *Journal of Information Systems*, *35*(1), 155-186.

Wang, T., Kannan, K. N., & Ulmer, J. R. (2013). The association between the disclosure and the realization of information security risk factors. *Information Systems Research*, *24*(2), 201-218.