Online appendix for

Inexpert Supervision:

Field Evidence on Boards' Oversight of Cybersecurity

Michelle R. Lowry
Virginia Tech
michellel@vt.edu

Anthony Vance
Virginia Tech
anthony@vance.name

Marshall D. Vance
Virginia Tech
mdvance@vt.edu

Appendix A: Sample of Questions from Semi-Structured Interviews

Note: *Below are sample questions from our semi-structured interviews. Given the semi-structured nature of the interviews, these questions represent starting points for discussion. The interview script was customized according to the interviewee's role (i.e., director, executive, or consultant) and relevant background.*

What does "cybersecurity risk" mean to you?

- Do you think that it would be defined in the same way by the directors on your boards?
- [If mentions challenges of cybersecurity] Can you speak to how the unique challenges related to cybersecurity cause your board to approach this risk differently from other enterprise risks?

Outside of the board, who are the other major players with respect to cybersecurity risk management?

- Who provides oversight over these individuals and/or departments that are responsible for cybersecurity risk?
- Within the board, is oversight shared between committees or between the main board and committees?
- For those not on the audit/enterprise risk committee, do they also have responsibility for cybersecurity oversight? If so, what does cybersecurity oversight entail for them?

We would like you to think about the last four board meetings. How was cybersecurity covered, if at all?

Overall, how would you characterize the board's level of experience with cybersecurity issues?

- Can you describe how an individual board member's level of experience impacts how they provide cybersecurity oversight? [Can you give us any examples?]
- How does a given board member's experience with cybersecurity impact the priority they place on cybersecurity oversight?
- How do board members educate themselves about cybersecurity?
- Do you think the board has enough expertise in cybersecurity to provide effective oversight for this risk? Why (why not)?
- Can you describe any challenges from overseeing management (e.g., CISO, CIO) with relatively more experience in cybersecurity?

Can you briefly talk about any cybersecurity consulting engagements [in the case of a consultant interviewee: your practice provides] that involve oversight at the board level?

Overall, how would you rate the board's effectiveness in cybersecurity risk oversight?

Does management have any incentive to filter the reports they give to the board?

Is there any advice you would give to another board on how to effectively oversee cybersecurity?

Is there anything you thought we would ask but we didn't, or is there anything else you would like to tell us?

Appendix B: SEC Cybersecurity Proposed Rule on Expertise Disclosure

Release Nos. 33-11038; 34-94382; IC-34529; File No. S7-09-22]

This table presents a summary of 191 SEC comment letters regarding the SEC's 2022 proposed cybersecurity rules. Two research assistants performed the initial coding under the guidance of one of the authors, then any differences were reconciled by one the authors. Another coauthor was brought in for consultation for any cases where there was ambiguity. We find that 43% of all comment letters discussed the proposed rule of board expertise disclosure, and that the comment letters present similar variations in views as our participants regarding director cybersecurity expertise. About one-third of such discussions were in favor of the disclosure. Objections included a concern that requiring disclosure would create a de facto expectation for director cybersecurity expertise, that such cybersecurity expert directors may not be able to contribute to the board for the wide range of board duties, that there is a scarcity of expertise in the director pool and in particular that small firms could not compete for skilled directors. Comment letters also cited that directors could lean on management and outside experts. The comment letters also raised concerns regarding how to define cybersecurity expertise. Thus, objections focused on the costs and logistical issues for firms who may want to secure cybersecurity expertise. Our findings that director expertise in cybersecurity leads to more substantive oversight provides insight into the benefits of obtaining expertise.

Table B1: SEC Cybersecurity Proposed Rules

Panel A: Summary of comment letter categorization

Total Comment Letters	191	
Comment Letters that discuss disclosure of director expertise	83	
Comments in favor of disclosure of director expertise	27	32.5%
Comments against disclosure of director expertise	48	57.8%
Other comment on disclosure of director expertise	8	9.6%
Total	83	100.0%

Table B1: SEC Cybersecurity Proposed Rules (cont.)

Release Nos. 33-11038; 34-94382; IC-34529; File No. S7-09-22]

Panel B: Representative comment quotes

Comments in favor of disclosure of director expertise
The SANS Institute believes that cyber expertise is needed on the board of public corporations. The expertise should focus on cyber implications with directors who understand these issues. The SANS Institute believes this is possible through proper training and certifications that validate directors' skills, similar to other industries, such as an accountant that has achieved their Certified Public Accountant designation. This will give confidence to the investors and assurance that the board can make smart decisions concerning cyber risk and investments. *The SANS Institute*
We have consistently supported legislative efforts to require publicly traded companies to disclose in their annual reports or annual proxy statements, whether any member of their governing body, such as a board of directors, has expertise or experience in cybersecurity issues. .....Beyond supporting cybersecurity strategies that address internal company-related risks, ensuring board members' understanding of the cybersecurity landscape is also vital to their understanding of external company-related risks. ...The board should be comprised of skilled directors with a balance of broad business experience and extensive industry expertise to understand and question the breadth of risks faced by the company. Risks posed by cybersecurity incidents and threats should be understood by board members, and we have long advocated that board members should develop and have cybersecurity expertise. *CEO of CALPERS*
We are pleased to see that the Proposed Rules address the role of the board in cybersecurity risk management and strategy in a thorough manner, including disclosure of whether any board member has expertise or experience in cybersecurity. ...We believe disclosing the names of board members with cyber expertise is unlikely to deter such members from performing board service. These skills are highly sought after, ...We believe that annual disclosure of cyber expertise among board members, if any, in the annual report and proxy would be helpful to investors, especially in voting decisions. *Council of Institutional Investors*
One effective regulatory approach would be asking public companies to disclose whether a cybersecurity expert is on the board of directors, and if not, why not. We have sponsored bipartisan legislation called the Cybersecurity Disclosure Act to require companies to provide this disclosure to investors. *United States Senators Jack Reed, Mark R. Warner, Catherine Cortez Masto, Kevin Cramer, Susan M. Collins, Angus S. King, Jr., and Ron Wyden*
Comments against disclosure of director expertise
Against de facto mandate, scarcity of talent, disproportionate effect on small firms Although these proposed amendments do not *mandate* that corporate boards include a member with expertise in cybersecurity, they have the implicit suggestion that corporate boards *should* include a member with such qualifications. Failure to have a board member with expertise in cybersecurity, therefore, could result in investors reaching the mistaken conclusion that a company is unconcerned with cybersecurity. While the Exchange agrees with the Commission that cybersecurity is an important area of focus for nearly all public companies, it does not believe that the absence of a cybersecurity expert on a company's board is necessarily the fatal flaw that the required disclosure may implicitly suggest to investors. … In the area of cybersecurity, a corporate board may rely on reporting from an in-house cybersecurity team or external consultants. Relying on non-board member experts should not suggest that a company is unserious about cybersecurity. ...If the Proposal is adopted in its current form, the Exchange believes that many companies will prioritize attracting board members with "cybersecurity expertise" in order to demonstrate their commitment to managing cybersecurity risk. With 7,848 companies filing on domestic forms and 973 FPIs filing on foreign forms during calendar year 2020, the NYSE questions whether there are truly enough individuals with both cybersecurity expertise and other relevant experience to make them suitable candidates for service on a corporate board. If a shortage does exist, the Exchange is also concerned that smaller and medium-sized companies may be disproportionately disadvantaged in attracting these highly sought after individuals for board service. *NYSE Group*

Scarcity of talent [T]he NACD Cyber-risk Oversight handbook 2020 observes "there simply are not enough 'cyber experts' to populate every board." ...The NACD's Governing Digital Transformation: A Practical Guide similarly points out that a common pitfall of recruiting "digital directors" is focusing solely on individuals with technical backgrounds because other skills and backgrounds might be more useful from a governance perspective. Thus, whether a board includes a cybersecurity expert might not be as relevant as the other proposed disclosures related to cybersecurity governance (for example, proposed Item 106(c) of Regulation S-K). The SEC might instead consider revising the Proposal to elicit disclosure of how or whether the board engages with experts to execute its governance role over cybersecurity. Such a disclosure would complement the proposed disclosures in Item 106(c) while providing registrants with the flexibility needed to craft cybersecurity governance appropriate to their organization. *Crowe LLC*
De facto mandate, scarcity of talent, one- trick ponies, director education and relying on management is sufficient The requirement to disclose whether the issuer has a cybersecurity expert on the Board of Directors could evolve into a market expectation that all issuers have an expert on their Board. PPG does not believe that the Commission's disclosure rules should be a "de facto" governance requirement. ... the requirements of proposed Item 407(j) are so specific that there likely is not a large pool of director candidates with this level of expertise who also have the general leadership and business experience to serve as a director of a public company. Directors can gain expertise on cybersecurity (or many other company risks) through educational opportunities, table-top exercises and from the issuer's own cybersecurity team. Issuers would be better served having a cybersecurity expert with the qualifications set forth in proposed Item 407(j) on their management team, rather than on the Board. *PPG Industries, Inc.*
De facto mandate, current rules are sufficient We believe dedicated expertise may be valuable for some companies. In general, however, especially given the limited size of boards, it may not be practical or advisable for a board to recruit dedicated experts in each of its critical oversight areas. While we recognize that neither of the proposals requires designated board experts, we believe that, especially when read together, some may infer that the Commission prefers that issuers identify such experts. We therefore encourage the Commission to consider whether existing proxy rules (which require disclosure of the particular experience, qualifications, attributes, or skills of board nominees), when combined with disclosure regarding board oversight of a company's cybersecurity risk, may be sufficient to inform investors about the role of the board in cyber risk management, without a separate requirement to identify cybersecurity experts. *Deloitte & Touche LLP*

Appendix C: Additional Interview Evidence

Table C1: Additional Interview Evidence of How Expertise Affects Boards' Cybersecurity Oversight

4.2.1. How expertise influences board engagement
Yeah, because your general board members, because they have their day life and whatever is exacting or commanding their attention in the course of any given week, may not have time to dabble in paradigm battles… And to even be positioned to even have the thought or to have it occur to you to even raise the implications of these emergent technologies, is probably not something a board member whose principal interests lie elsewhere, would have had the time to have even become aware that there's a question out there that you might want to pose or ask. (E-7) [T]he board should make sure it's got its governance structure right…. And if they do get that right, it has real world effects. Because then there's somebody on the board who is knowledgeable about cyber, and that means that the CISO has somebody to talk to. And there should be a line of communication between that board member and the CISO. And usually, that also means that the CISO gets out from under the CIO, doesn't report to the CIO directly. So, if you get the governance model right, these issues are going to get better funding and then get more time and attention. (C-3) [Without a director with expertise,] I would predict that there wouldn't have been somebody in the audit and finance committee who would've stepped up, because they're already busy. They got a lot to do. I would bet that somebody else, one of the other board members, would've asked the question …, "So what are you guys doing about cybersecurity?" We would've had to go in and present, but it would've been at a much higher level. [Without the director with expertise] I don't know that we ever would've had this maturity model in place. … [C]ertainly we wouldn't have done that third party review and bring that in.… I think we would be at a very different [level]... I think it took an IT person to be able to really drill in and understand at the level she wanted to. I don't think the others would just have the interest. They would just want to know it's protected, and, "Do you have somebody in charge of it," or, "Do they know what they're doing," kind of thing. (E-2) [T]he audit committee chair said, "I would like to do a benchmark and analysis using the same yardstick, the same measuring stick, to see how one [company] stacks up against the other, where we're strong, where we're weak, where there's synergies, where there's big gaps." And that launched our whole project. …Oftentimes, that is where it comes, is at the request of one board member who is seen as the IT or cybersecurity expert who can ask for those special things that sends the CISO or the CIO, or the chief risk officer, or the chief legal officer off to do these reports or these sorts of analyses. (C-7) I'm the lead on cybersecurity risks. And just by the nature of my background, I work very closely with the other chair on setting cybersecurity goals and what the board should be focusing on. Along with the IT leadership, we have inter-quarter calls …checking on how things are going, whether the board should be specifically looking at things that we were not aware of. And I help to interpret some of the technical language into risks for the board. (D-13 expert)
4.2.2. How expertise influences questioning
But [X, a director with more cyber expertise] just comes up with good ideas, good things to think about, or for management to think about. Not only just where do the ones and zeros go, but how are you structured, your organization? Where are you spending your time in your organization in your information areas? You know, your data processing areas and stuff. (D-1 nonexpert)

[Our more expert director] understands the ins and outs, and she's taken a liking to it. So she brings to the table a lot of things that we don't think about, and then she says, "Well, have you thought about this? Have you thought about that?" And that has been a godsend. (D-1 nonexpert)

People are quite diligent I've found on boards. They would typically spend the time and energy to get more knowledgeable and there are a lot of resources. And people on boards, they're smart people. They know how to educate themselves. And what they do is they would do what I did. They would talk to other people, they would take courses, they would do whatever they needed to do to be sufficiently knowledgeable so that they can do the right thing. (D-1 nonexpert)

[Director X] is probably our most versed person in his experience with these kinds of issues…. I know I wasn't brought in because of my cybersecurity expertise…. It's helpful to have someone who's kind of lived in the world on the front edge of things a little bit, and I think boards certainly would benefit by having somebody that has knowledge of what are the questions that need to be asked and the issues that need to be addressed so that you don't just get a kind of a glossy eye, 'we're on top of this and let us show you all the insurance we have to protect against all these different possibilities….' He just might ask more questions and have more insights than the average board member would... he tends to be someone who brings a little bit more to the party for that. (D-8 nonexpert)

I think, because just the nature of our oversight, everyone's participating, asking questions. I don't see [expert director's] questions are different than anybody else's question. I'm just trying to think back on some of the relevant conversations that we've had. Maybe. Maybe it's a little bit more technical than someone else's question, but it doesn't get real technical, if that makes sense. All of that conversation is something any board member would be able to understand the subject matter and the nature of the questions. (D-16 nonexpert)

[in contrast to cybersecurity] from an accounting standpoint, you can read the financial statements, you can see where the cash flows are coming form, you can see where the risks are. [In cybersecurity] you have to ask a bunch of questions and you need the background or knowledge of some of the technology to even be asking the question." D-18 nonexpert)

[In response to: Did they ask you any follow-up questions?] Nope. Which shows the maturity level of the board. They wouldn't be able to ask questions. (E-5)

There's a language barrier here. Boards don't want to be embarrassed. They don't want to sit in a room and say, "What is that acronym," and, "What does that mean?" They're not going to do that. (C-6)

4.2.3. Lack of expertise requires coaching by CISOs

Educating the board	The last presentation was to the full board, and they were just generally asking questions. A lot of them were generally asking questions about more, just trying to seek better understanding around cyber and what have you.... For a lot of the individuals, they were trying to still learn about cybersecurity. There were times where, especially right now with the ... different types of cyberattacks that are occurring, there's a certain level of interest to really understanding more. (E-3) One of the things that we implemented the first year I was here is a discipline, or I should say, a cadence where, at least once a year, we have a board education session. One year it was just security 101 kind of stuff. The anatomy of a program, how it's built, how you evolved to the strategy, how you execute, that kind of stuff. And then we did a tabletop demonstration, how we do our annual cybersecurity, executive tabletop exercises. We had one session on, 'How

	do you protect yourself from the criminal?' kind of thing. So every year we have that, and that's really helped in board education. (E-6) [T]he executive committee is essentially attending the audit committee meeting that I update in, which is great for me because it's a super opportunity not just to educate the board but [also] the executive committee and keep them in the loop. (E-9) We're bringing in the CISO to talk about what's going on. Part of that I would say is part of the governance, but also in terms of helping educate the directors. I mean, a lot of the directors are like me that grew up… When I was in [college] we were using punch cards for our computer science classes. (D-14 expert)
Conditioning the board	But we have really hammered that home, and this is the five functions that you align a cybersecurity program to. And this is the framework we're using to manage cybersecurity. So this is what one should look like, these are the things that you should have in place. And then we go through a process saying, "Well, this is the maturity of us against that framework of how we've implemented it." And then the rest of it becomes a little bit of trying to understand what's the best way to help them provide oversight, what are the best kind of reports. (E-3) [speaking as the CISO and their team] "(L)et us tell you what the risks are, let us tell you what we're most concerned about, and for those things we're concerned about we're going to report back to you on the progress we make on remediating that, and then... let me show you how we're protected from an insurance standpoint, too, so if something does go bump in the night, it's not going to harm the company's financial situation." (D-8 nonexpert) I took one of those [articles], "The Top 10 Questions Boards Should Ask CISOs." We took the questions, I filled it out, and then we just gave it to the board members and their repository to pre-answer before they ask. (E-6) Part of it starts with education. Explain to us what the risks are. And then, what are you doing to mitigate those? Probably, finally, how can we help? I mean, is it resources or investment? I think it would be a combination of all of those things. (D-14 expert)
4.2.3. Expertise enables board members to challenge the CISO	
	In asking the CISO these questions, it was pretty clear the CISO was very old fashioned and was much more focused on keeping things out as opposed to assuming that people got in… And we ended up replacing that person. [When asked if the board would have known to replace the CISO without D-11's cybersecurity expertise] I doubt it. Given that I was the one driving questions, I doubt it. (D-11 expert) I think having people now on the boards that have that expertise is a risk mitigator for companies because it really is allowing subject matter expertise on the board to go. "We'll pull out here." [As an example of director feedback] "No, you're not making the right investment," or "You're not making the right level of investment." Or, "It's clear to me that the IT leadership in this company doesn't have the expertise needed to deal with the risks that are facing this company." And I think that's the value of having a board member that understands the cyber space. (E-8) [An expert director] said, "I'd like to see a third party brought in, somebody from the outside, to do an independent assessment of where you are from a cyber maturity perspective and then put together an initiative plan, so we understand where you're going and what things you're doing." So, we said, "All right." We wanted to proactively get in front of that. (E-2)

4.2.4. Expertise enables board members to detect false or withheld information	
	There is always a bit of "protect your house." We know that information is filtered to the board and that's why it's important to get outside sources of information…. [Regarding whether the filtering is unique to cybersecurity] I think it becomes more challenging because the boards may not know enough to ask as many questions. If you have a cyber expert it is probably not as big of an issue. It is more challenging because of the nature of it. …IT is a more dynamic thing that makes it more challenging. (C-2) [A director should be someone] who understands technology, who has done and overseen cybersecurity, so a former CIO, or a former CISO, somebody who has sat in the chair and has asked those questions of a CISO, or been in the operations seat and has done these things before. Otherwise, you run the risk of getting snowed, and you're going to." (C-6) [In response to how oversight is different if there is a board with expertise] Well, I mean, to be crude, to not get [expletive] in a meeting, right? So, if either one of you two are sitting in a meeting, a cyber meeting, and you see a board-level presentation, which is generally going to be fairly high level. But you're going to know the right kind of questions to start asking. You hear something in that presentation where it feels like, "Well, that feels a little weak," or "I'm not seeing something that I would expect to see in a cyber protection program here." …You bring somebody in, who's got real cyber expertise. I think that is a big risk mitigated for the board. (E-8) [In response to our question: Do they (CISOs) have pressure or incentive to provide a rosier picture, to make themselves look better or to make their boss look better?] Yeah, it's a great question. I think there's always the risk of that. This is where educating the board members to ask more piercing or penetrating questions and have their own expertise or having an expert on the board (I mean if you get to that point) helps. … But, I think having the person in front of the board, you generally get a gauge in terms of the person is trying to just tell you a rosy picture or they're actually saying, "Here's a situation." (D-14 nonexpert)

Table C2 Additional Interview Evidence of Whether Cybersecurity Expertise is Needed

Is cybersecurity expertise needed?	
Yes	[S]ome of our best practices in the industry are to add that cyber expert IT professional on the board. And that has been something that's been recent of the last three to five years, but a lot of focus the last two years…[we have] a spot, we don't have anyone who fills that now. I think that is a hole in our governance that we all recognize we need to do something about and put more internal focus on it….We should have cyber expertise I think on our boards …and the audit committee. We have GAAP, obviously, and we have all the rules and regulations around SOX that the financial statements stay true to intent. It seems like the way cyber is developing. It's right there, right behind financial statements right now. The integrity of the financial statements, the integrity of your systems and the reliability of your systems are one and two. (D-15 nonexpert) Having your own board member who is [themselves] an expert, in terms of the issues being discussed or presented, when the presenting CISO goes out of the room or looks away, [board members] can all look to you and say, "thumbs up?," ... [I]t's an extra little piece of validation, separate and independent of what their own personal entities might bring to the table. (E-7) [T]he board's chock full of all sorts of people who have run large businesses and understand governance and understand strategy and financial management systems and supply chains and all

	those things. And they're brought in because they had that experience. Why would you not do the same thing in your digitized space? Why wouldn't you bring somebody in that has that kind of expertise and knowledge, because in most corporations, that is the area where they are potentially the most singularly at risk for catastrophic failure. (E-8) I actually am very much an advocate of having a strong cyber presence on the board.… [T]here's virtually no industry that's untouched by [cybersecurity] anymore, and it's not going to get better in the short term. So, I do support that approach and that regulation moving forward because I think the vast majority of boards are woefully—and this is from talking to peers and others—are inadequate in the space. I do support it. (E-9) It's an area that will be considered best practice today for a board to have expertise on and be a regular part of the communication at board meetings and regular updates. So, it's not just SEC, but it's good business today. There's so many different ways that a company can be damaged. Everything from the stealing of critically important information, not even known as stolen. I think that becomes almost number one for a corporate. But, of course, when you're being held hostage for a major payment and you're running a utility, it's pretty damn important as well. So, the big problem that I see…is a shortage of expertise in the area and with a very high demand. (D-17 nonexpert)
Middle ground	I'd love to have more knowledge. I think having [Director X with expertise] come on the board helped. I think that having these third parties coming in every couple of years give you some validation of what's working and what's not working. I think it's a combination of a lot of things. Personally, I don't think you should get a board member that the only thing he or she brings to the board is cybersecurity. (D-1 nonexpert) There's a lot of debate out there about boards having a designated cyber expert. I'm in the camp of, it depends. It depends on what kind of company it is. But definitely, the board has to have enough knowledge to understand risk presented by cyber risk, and then have confidence that management is executing to mitigate that risk. (E-6) I think when you look at the board and the function of the board, you really want people that are very broad based in knowledge. And not necessarily deep expertise. The most important role of the board is that financial fiduciary responsibility. Certainly, you're going to have accounting and audit practitioners and things like that.... [W]hen you give a board seat that's dedicated to technology, or cyber, or some combination [thereof]..., is that really benefiting the entire company? And for a technology company, it's probably yes. Certainly, in fact, most board members of a technology company ought to be somewhere out of the technology sphere. But we're not a technology company, although we're obviously more and more dependent on technology. (E-6) I'm not opposed to [having a cybersecurity expert on the board], but I think that the board having the ability to directly contract for ancillary support is probably a shorter-term solution. I think in a long-term solution, I think that's a great idea. But again, I wouldn't just put a cybersecurity person in there. I would put somebody in there who understands the holistic environment of security and risk. (C-5) And so I see this debate a lot about do we need a cyber expert, and my personal opinion on that is many of us have dealt with cyber in managing our own companies, and people like [Director X] who've had a variety of military experience and the like, but to get someone who was maybe a former CISO, they may not make the best board member because they don't have the broader experience. And, in fact, I think we should be relying on the company hiring great expertise to manage the risk and us being at more of the oversight role. But, having said that, I think, again,

	that's why it's so high on the list of risk is because just the nature of the subject matter is one that, even if you were an expert five years ago, you might not be so expert today. It's a tough area to manage. (D-16 nonexpert)
No	The shareholders do not expect their board members to be experts in cybersecurity. They expect the company to have experts in cybersecurity and to be effectively deploying those to manage the risks, and I think the boards rely on third parties much like we do in an audit. (D-4 nonexpert) I think that for the level of oversight that they're providing, that just to have a general understanding of awareness is important. I'm not necessarily sure if they have to have a deep level. (E-3)