All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

So you're looking for a cyber security board member for your public company...

Good luck finding someone qualified…

The SEC is apparently about to make it a requirement for public companies to report on "the board of directors' cybersecurity expertise, if any, and its oversight of cybersecurity risk".[1]

Some details:

Quoting from those proposed regulations:

> *If any member of the board has cybersecurity expertise, the registrant would have to disclose the name(s) of any such director(s), and provide such detail as necessary to fully describe the nature of the expertise. … the following non-exclusive list of criteria that a registrant should consider in reaching a determination on whether a director has expertise in cybersecurity:*
>
> - *Whether the director has prior work experience in cybersecurity, including, for example, prior experience as an information security officer, security policy analyst, security auditor, security architect or engineer, security operations or incident response manager, or business continuity planner;*
> - *Whether the director has obtained a certification or degree in cybersecurity; and*
> - *Whether the director has knowledge, skills, or other background in cybersecurity, including, for example, in the areas of security policy and governance, risk management, security assessment, control evaluation, security architecture and engineering, security operations, incident handling, or business continuity planning.*

Why would it be hard to find someone like this?

There are about 7,000 public companies in the US, and lots more that do business in the US.[2] Likely there are some that don't have any real need for such expertise because of the nature of their business, but likely at least 6,000 do. And of course the qualifications for aboard member are not just this. But let's slice the loaf here.

There are about 120,000 CISSPs in the world, the vast majority of whom have no executive experience. There are fewer CISMs, most of whom have steady jobs, and most of whom have no top-level executive experience. And there are lots of executives out there, but very few of them understand much about cybersecurity.

So the big problem here is getting enough well qualified people. Just from a numbers perspective, it's almost certain that more than one board will have to share each cybersecurity expert if the companies are serious about proper representation. So here are you going to go to find such people and how willing are you to share them and what about the potentially competing fiduciary duties associated with multiple companies for these board members?

1 https://www.sec.gov/rules/proposed/2022/33-11038.pdf
2 Based on the number listed in the NYSE and NASDAQ

But here's the rub

Somebody that actually has expertise and is in a board position has a fiduciary duty to the shareholders to apply that expertise to the company. And likely the first question they will ask is something like, "What do you have in place for cybersecurity governance?"

If they are actual experts with executive experience, they will likely have to be part of the audit committee so they can have clarity around the situation, and they will want to know the answers to about 120 high level questions about cybersecurity. Examples are the questions from the Standards of Practice.[3] When they ask these questions, the answer to most of them will be something like "we don't know". At that point the board member will have to say that the next company report will have to state something like "At this point, the board does not have enough information to determine whether cybersecurity is reasonable and prudent.."

However, before the next quarterly report, that will likely have to be addressed which means that there will be about 10 days of meetings with the new board member and lots of folks from the company and a realignment of the situation and resourcing. At that point, the board member might be able to upgrade the opinion to something less stark.

And there are some other problems as well

So now we have to face another major limitation. If as a board member I have to spend 10 days per quarter with each company, that's 2 out of 13 weeks, or 6 companies per board member at maximum load. And that means we need 1,000 such qualified executive cybersecurity experts at a minimum to prevent public companies from the required response something to the effect of "We have no substantial cybersecurity expertise on our board."

Of course these companies could elevate their CISO position to also be a board member, but somehow I have problems believing that the CEO and CIO and whoever else is in the management hierarchy above them would want them to be on the board. So all that would do is hollow out the expertise within the company, and worse yet, the person on the board would be someone who has been under the thumb of the folks who are now under their thumb. Somehow this is averse to the corporate culture of most public companies.

You could also poll the board members to see if you have any that qualify and then try to make their expertise publicly available for scrutiny. Of course it's likely that most will not qualify, and those that do will, in most cases, look pretty lame once this is exposed.

Of course public companies could just not worry about it…

Nothing in the regulation says you have to have any such expertise on the board. It just says you have to tell the public about it if you have it. So remain silent and let it become a competitive issue becomes a likely initial strategy. Until everyone else comes out and some of your major competitors look a lot better. The media will yell about it and your stock price may take a hit. But it's likely to come back soon enough… we hope… until the next major incident.

Conclusions

Here is when I am supposed to solve all your problems with my brilliant solution. Sorry. I cannot help you there. Yes you could hire me... the first 6 of you that come along. And I have some long-time expert friends for another 100 or so of you… First come first served.

3 http://all.net/Arch/index.html

