CISO Track

RSA 2020 Event

Session 5: Board Communications

Problem Domain SME: David Johnson

Courtesy of Glilot Capital

Date: February 25th, 2020
Staff: Iftach Ian Amit and Chris Nickerson
Transcribed and Prepared by: Scott Lyons, MS.

Executive Session Summary

Note: This discussion was another carry-over from the initial CISOTrack at BsidesLV. In that discussion, much like this one, a great emphasis was placed on how CISOs communicate with the board and what that interaction looks like. A portion of this discussion also included a cyber insurance Q&A.

The speaker for this session was Dave Johnson, who has an extensive background in investment, M&A integration, and corporate development for companies operating in China, India, Europe and the United States. He has served on nine Boards of Directors, four of which he is currently serving on (i.e., Cloudreach, IntSights, Mphasis, and Mercy College), including as a member of at least one Risk subcommittee.

Any CISO's first step in preparing a presentation for the board is to know their audience. Dave has a better understanding of cybersecurity issues than most board members with a financial background, so he recognized that many CISOs will likely have to give their board members a baseline of education about information security and cyber risk (e.g., industry best practices, top priorities, security controls) to ensure that everyone is on the same page; otherwise, board members won't be able to evaluate the CISO's arguments appropriately. Once they have the basics, CISOs can address:

(1) "What's unique about your company, from a cyber risk perspective?"

This is all about the nature of your business and how that affects the level and types of risks you face: What industry are you in? What geographies do you cover? What types of data do you have? What are you trying to protect (e.g., intellectual property, financial assets)? This is where you highlight which things are most critical and relevant to the risks your company faces.

(2) "What's the architecture of your cyber defense? How are you thinking about it?"

Describe the decision-making process in selecting your current controls, given the landscape of the company and its complexity (e.g., are you in the cloud or not, how many vendors do you have, how many locations do you have?). Because it isn't possible to protect against 100% of the possible risks, CISOs have to make judgements to prioritize, differentiate by where the risks are, dedicate resources, and select appropriate tools to address those various risks. Explain to the board, pragmatically, why you're focusing on certain risks over others.

(3) "What's your perspective on the [organization's] use of technology?"

The specific responses here are not as crucial; this is intended to show that the CISO is knowledgeable. Dave noted that "the depth of insights they have gives me a lot of perspective on if I'm comfortable about the leaders in the company that are responsible for cyber protection."

(4) "Where are you today vs. where were you before?"

Dave finds that trends are more informative than point-in-time, absolute scores, especially since everyone can score things differently. Board members will look for input from legitimate, well-regarded third parties (e.g., external penetration testing, consultants' findings) to corroborate findings from internal assessments. This doesn't mean that the board members don't trust the CISO's recommendations but rather that they want to make sure their bases are covered. If an incident occurs and people turn to the board asking whether they did everything possible, Dave noted that "one thing that [the board] can do is try to look to third parties to validate that [the board members], along with a company, didn't rely just on one sort of source of truth; they had multiple sources of truth."

(5) "Exactly what level of risk are we taking?" Are we exceeding our threshold?

Most board members will know that there's a trade-off between having a fairly cheap cyber insurance policy with fairly limited coverage (i.e., the insurance company wrote in a lot of "outs" so they won't have to pay unless very specific conditions are met) or having tighter language in the contracts and paying substantially more for that additional coverage. The CISO isn't usually the one who "owns" the company's policy (including the budget, selecting the specific terms/conditions, etc.), but knowing the amount, key terms, and built-in benefits can put the CISO in a good light (and stay in the CEO's good graces by not putting them on the spot). This is also important because those terms can have a major effect during response/recovery activities (e.g., if the insurance provider dictates that specific vendors must be used following a breach or ransomware attack).

A large portion of this panel discussion revolved around what types of assessments and data to use to present cyber risk information and trend lines (#4). For example, many of the CISOs agreed that there's been a lot of industry consolidation on board reporting around the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), but how should you develop your scorecard? Should you use third-party tools for internal assessments (e.g., the Expel's free NIST CSF self-scoring spreadsheet, CISA's Cyber Resilience Review [CRR] tool and its crosswalk to NIST CSF, the Capability Maturity Model Integration [CMMI] Cybermaturity Platform aligned with NIST CSF), add to existing external frameworks (e.g., to incorporate cloud security controls into NIST CSF), or is it okay to develop with your own resources? Whichever method is selected, Dave suggested that CISOs should ensure that they use the same method over time and that all data collected are stored in a cloud repository, which will allow for the automation of trend lines (e.g., year-to-date, the last 12 months, the past six months).

Visuals (e.g., trend lines, pie charts, spider graphs) are a great way to present information to the board because sharing data (including those from third parties' reports) can help establish credibility, and visuals are easier for the brain to absorb, even if it's in an area that board members might feel they don't know enough about. In general, Dave prefers separating the discussion of the problem from the discussion of the solution, which gives the other party time to absorb the information, think about it, and accept the problem without getting overwhelmed, leaving them more amenable to hearing your solution later on. However, CISOs often only present to the board once a year, "so you're stuck trying to both educate/share the problem *and* tell them what you're doing. It's almost an impossible task for the board member to absorb all that and execute because it's just how…people work."

Another example of human nature at work is how many CISOs can probably agree with this statement:

> "I've made a lot of recommendations to the corporations that [have] been ignored, and then they hire a consulting firm who recommends the same thing, and all of a sudden, it gets adopted. There's something about senior executives and something about boards that likes the validation from external as well as internal."

This doesn't mean that the third parties are more accurate or more comprehensive. One CISO noted how third-party tools and assessment providers "all suck, and the only difference…between [them] is how less they suck from one another… The quality of those [Big Four assessments, in his experience,] is very, very low - like, sub-suboptimal." Another noted that

> "consultants are very easy to influence, so, when they come in, if you have an approach and they like it…get them to write about how this is a very good approach… [If] the company's going to spend money on a consultant, and I think I already know the answer, I'm going to spend the time to try to influence that consultant, and most of the time they're all too happy because you're doing half the work for them… So it's kind of a win-win scenario, other than…the shareholders spent money that maybe they didn't need to spend, but, again, most boards don't know that these third-party sources are not that credible… You can tell them that [the sources aren't credible] but then they don't know if you're just using it as a justification" and they'll be wary since the buck will stop with them, the board members, if an attack happens and they can't show that they did everything possible.

This might also partially be because "most boards look at cyber risk as sort of an extension of financial risk, so [board members] have a lot of experience in using third-party auditors to theoretically validate the financials," even if CFOs' opinions about those financial auditors are probably pretty close to what CISOs think about third-party security assessors.

One CISO pitched a creative potential alternative: creating a security advisory board composed of peer CISOs who would assess the company's security program and provide an objective third-party perspective. This could be the information security equivalent to what is used in the pharmaceutical industry, in which a manufacturing advisory board (which is separate from the corporate board) gives the company direct advice on how to actually make the drugs. While some companies do maintain enterprise risk subcommittees to keep board meetings to a more manageable timetable, Dave noted that he hasn't seen anyone create a panel of security experts like this before. This might be feasible for a few companies, such as Wall Street banks spending millions annually on security, but may not be something that most boards would be likely to do now.

Smaller companies face a different set of challenges; they might be investing in building up their technology (and not the security controls to manage the corresponding risks) so that they can grow, leaving them exposed. If they hold key personal data, this could have major legal implications that could land them in trouble (e.g., under the General Data Protection Regulation in the E.U., or the California Consumer Protection Act). Some companies don't have any third-party validation measures at all. If the Chief Information Officer is also the CISO, they might be so focused on the technology that they haven't implemented appropriate detection mechanisms yet. This is why, when Dave joins the board of a small-to-midsize company, he immediately asks when the cyber review will be (e.g., "what's our schedule? What's our governance around that?").

If there doesn't appear to be any expectation for the CISO to brief the board, and neither the board nor the CEO have asked for a cyber review at all, the head of security should be proactive and take it upon themselves to emphasize to the CEO why this is an important component of the company's risk management strategy. One CISO said that they stated, as part of their findings and recommendations to the executives during a presentation after their first 90 days, "I will be presenting to the board," which made his expectations clear. If there's a security incident and the CISO hadn't briefed the board, it isn't just on the board and the CEO; the CISO's accountable too. The window for initiating a board presentation could close if a new CISO lets it slide for too long after starting a new job. This would not only expose the company and leave the board in the dark about those risks, but could also affect the CISO's career trajectory in the long term. If the head of security isn't following reasonable practices and it's discovered during an audit, that could have career implications that would absolutely hurt the individual's subsequent employment opportunities.

In Dave's experience as a board member, he knows he can't evaluate the cyber risk as well as the CISO, so a large part of his critique is based on his evaluation of the CISO themselves:

> "I'm saying, 'Do I trust you? Are you going to tell me the truth? Are you really on top of this?' So, the way that you carry yourself, the breadth of what you share, the trust that you establish, the credibility and the honesty is what I look for… The one that really scares me is somebody who comes in and says, 'We're under control.' …My defense mechanisms immediately go up because I don't know what that means; I don't know how that could be. Tell me the context…they're going to get the questions like, 'Well, how many events did you have? And how many false positives? …How many of those events did you really assess?' …You just open yourself up for all kinds of horrible questions. So, you know, I would just try to establish credibility, right… Yes, the charts help. Yes, the contents… All this stuff is about building trust; anything you can do to build trust, that you've got it…you're on top of it… you're doing a good job."

Organizations of all sizes face cyber risk, yet board members will not typically be cybersecurity experts. CISOs have to know their board, be able to explain the basics of information security and industry best practices in a way that's easy to understand, break down that organization's unique risk profile and corresponding risk management efforts, and use human nature to their advantage - bring in third-party validation to show off how awesome you are, use visuals wherever you can, and explain your decisions in context. Your risk might be increasing over time while your technology resources age, but if you want the board to understand what you're doing, why you're doing it, and what your budget is used for, then you need to explain that to them regularly.