CISO TRACK

RSA 2020 Event

Session 6: “Un-conference” & Closing

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

Executive Session Summary

This was the final session in a long day and was intended as a way to wrap up spinoff conversations from previous sessions, discuss unanswered questions/topics, and close out the event. The three main topics that arose in this session covered cyber insurance, organizational culture, and further developing a community of peer CISOs.

Cyber Liability Insurance

Cyber insurance was brought up in a previous session as well as in the context of a joke: “Do you need insurance if your security tools use AI [artificial intelligence]?” There are a lot of factors that can affect cyber liability insurance: Do you want an inexpensive policy that may have a lot of “gotcha” provisions (e.g., not covering attacks they deem as “acts of war,” like some companies faced following NotPetya)? Is your risk acceptance so high that insurers will raise your rates? Will the plan you’re getting cover just the parent company, or also any subsidiaries (e.g., where the holding company has more than 80% vested interest)? Do you have vendors pushing your consulting firm to have tens of millions of dollars’ worth of coverage because one of your responses to their questionnaire suggested that you *might* have access to their sensitive data *if* that vendor has vulnerabilities? Ultimately, how do you figure out how much coverage you actually need?

One CISO found that using risk modeling companies to identify coverage needs would be prohibitively expensive, so he asked other CISOs what methods they used. One response was to set up time to talk to the underwriters themselves and explain your security program to them, because “it turns out that the underwriters, who still don't fully understand the risk that they're facing (for instance, with everyone using the same cloud providers), are actually really interested in these conversations” and sometimes you can get a better deal out of having those relatively informal discussions. Another CISO commented that they’ve also engaged directly with their broker and proactively presented far more information than the broker would’ve received in a questionnaire, which explained the CISO’s rationale for the coverage amount they proposed.

Another response was to conduct internal exercises to model your risk: he worked with his team to come up with eight different breach scenarios of varying impact levels (e.g., a few compromised laptops versus finding out all data from the last five years have been compromised versus the whole service going down for multiple days), then brought in other stakeholders to model how those scenarios would play out. For example, he’d consult with the revenue team to guesstimate the costs associated with breach response in terms of staff (e.g., more customer support advocates), tooling, third-party support (e.g., forensics vendor), etc. He then compared the results of that exercise to the findings of an IBM report on the cost of breaches to benchmark their estimates, which were then used as the average when calculating what their maximum coverage limits should be.

It's important for CISOs to know what's actually included in their cyber liability insurance plan and what isn't. One CISO noted that they found out, in the middle of responding to an incident, that they didn't have some of the services they thought were bundled into their cyber insurance coverage. A CISO who used to work for a value-added reseller found that a lot of his clients at the time thought they had a great deal on services like digital forensics, eDiscovery, and litigation support because their insurer had a personal relationship with the service provider, but the "special deal" they were led to believe they were getting was actually more expensive than if they'd contracted directly with the service provider, and "it was referenced in the policy, not that it was *mandatory*, but that you *should* use them." Any of these factors could easily influence the CISO's security budget, and no one wants to be caught off-guard by "gotcha" terms.

Organizational Culture

The next topic of discussion was about the CISO's role, as a leader, in consciously building a culture in the security organization that influences their teams beneficially, and how the CISO can stay on top of that. One CISO interpreted his role as approaching problems with empathy, asking for feedback, paying attention to how a team members respond to a communication, and addressing potentially problematic dynamics within or between teams quickly. This included having "a scheduled meeting just for people to share experiences - not only of sort of negative interactions, or less than ideal interactions, but also the positive as well," which he found worked out well over time and led to progress.

Another CISO focuses on making sure his team's responses to any type of communication ("upwards, downwards…laterally within the same team") come across with the right kind of message: "We're not the team of police. We're not the team [that's]…watching everything you do. We're not Big Brother; we're here to help, we're an enabler of the organization." To avoid coming across as adversarial, this CISO felt that the team should rephrase "no" into "yes, but…here's a better alternative," which in turn encouraged teams to reach out more often for advice and solutions because they knew "we're all here together…trying to actually get us to [the] company objectives." To make sure that information security team is informed about what's important for the business and can pass that intelligence on, this CISO requires his team members go through the company's training program for non-technologists that's designed to help participants understand how the company makes money, because "if you don't know how we make money, then you just throw in risks, right?"

Two other CISOs described using physical cues, posters on the wall or desk toys with cards, to emphasize the organization's vision, mission, and/or values, both of which described seeing/hearing that content in their employees' responses later (i.e., incorporated into their annual review goals for 2020, and hearing key phrases - such as "prioritize the basics" or "think risks, not controls" - in conversations between team members).

Another CISO noted that his team of passionate employees who cared about their colleagues, their work, and the company were hated and no one wanted to meet with them because they "didn't know how to channel [their] energy in positive ways," likely because information security involves doing "really tough jobs and it puts a lot of stress on people." To prevent burnout and encourage people to keep a positive attitude, he opted to hire people just starting out in the field to "create an environment where other people have to step up their game to be mentors and [feel like] leaders, even if they're not a manager," emphasizing that it's really a team effort and everyone needs to know that someone's got their back.

When one CISO "inherited a team that was very cynical and depressed about the amount of tech debt that existed," was "butting heads with Engineering," and "had this kind of feeling of defeat," he reinforced to his team:

> "Your role isn't to get to '100% security.' Your job is to help influence and articulate the risk to the rest of the business…so that the right stakeholders across the organization understand that acceptable level of residual risk, and why we're making decisions, and that we're a partner [in the organization]."

To ease some of the tension when groups are at odds (e.g., between the Security and Engineering teams), one CISO found that a very effective tool was to go to the person with whom you're butting heads and tell them that "you don't want his job, and you don't want his responsibility." His reaction was that,

> "It's astonishing; I found, in this case, how often it was that people were not appreciating how true that was. And when you frame it up like that…they start thinking like, 'Oh, my God, I know… I would *hate* to have to do all the stuff that that person takes care of, when I really think about it.'"

Shaping a team's overall culture into something positive, supportive, and helpful for the rest of the organization can be really difficult; the adversarial stance, negativity, and burnout that's so common can, at least partially, be attributed to the nature of the job, as various CISOs noted:

> [1] "We asked the people that work in security to essentially do the impossible, right? It is literally a no-win situation, right? You *cannot* "win" you can only *"not lose*." And

> that's, emotionally, that is, I think, that is just *draining*. And, and I don't know what to do about that."
>
> [2] "One of the things that I try to do with my team is [to] actually make them part of that [product] delivery, so that way they feel like - even though it's an engineering delivery - it's also a security win as well. [This is] so we don't feel like we're burned out because we didn't get breached; that was the success criteria there."
>
> [3] "I started realizing fairly quickly that people that work in security actually *don't* have that many progression opportunities within the company. Like, some of them can move into software development, but not all… So, that actually means that people join your security team, and their way of growing is either within the security team or they're going to go to another company."

Accounting for career development in a way that allows employees to "feel like there's a trajectory within the team…[and that] also makes them feel like they can actually learn something about how to become the next security leader" can affect retention. One way to do this is to build internal training resources and bring in external speakers. This could include inviting CISOs from other companies whose security teams have a different approach or internal culture. This could also mean pulling stakeholders from other departments to talk about, "'How do we work with each other? What are the immediate tasks? And how can we improve?' And that way the team is aware of, like, the different pockets of the company, and what they do, and what their concerns are."

Building a Community of/for CISOs

Part of CISOTrack's mission is to keep these conversations going by creating a community of peer CISOs who can reach out to one another for mentoring, resources, and ideas about how to tackle difficult situations. One existing group is the Information Security Leadership Forum on Slack, a nonprofit group that consists of CISOs, venture capitalists and investors, and other industry leaders in practitioner roles. Because this group - while invite-only - isn't exclusively for CISOs, the CISOTrack hosts asked for feedback on how best to foster this peer community. Another concern was the built-in retention feature in Slack, which automatically deletes older messages, since it can be a blessing and a curse: people might be more likely to open up about sensitive topics, but you wouldn't be able to reference them later if need be (and Slack might also be data mining conversations on the back end!)

Alternative suggestions for off-line conversations included using the Signal messaging app, setting up an eSIM service (which was less well-received), or another method of secure communication with flair that highlights their particular area. Regardless of whichever solution is ultimately selected, having those open lines of communication can allow CISOs to discuss what their respected peers would do in a certain situation (including technical concerns or even topics like negotiating compensation packages), back-channel issues they've noticed that aren't public yet, and offering oneself as a resource for particular challenges or concerns. This kind of trusted advisory relationship would let CISOs know who they can turn to and that their connections are people they know who are in a similar position in other organizations.

Future CISOTrack events are currently scheduled for Cyber Week, a huge international information security conference hosted in Tel Aviv, as well as next year's BSides Las Vegas event. The hosts asked for feedback to tailor these events to cover the most important topics for participants, but also to determine whether there are other regional areas that are a "hotbed for CISOs" (e.g., San Francisco, Phoenix). Participants are urged to suggest any place(s) with 15-20+ CISOs who would attend a full-day event like this, even if it isn't tied to a conference.