TrustMAPP®

CISO'S STARTER PACK

Frequently Asked Questions

Jason Lish, CSO at Lumen Technologies, and Allan Alford, CISO at TrustMAPP, answer the most frequently asked questions from first-time CISOs.

1. In your experience, is it more difficult to get the board to budget and pay for the security improvements that need to be done, or is it getting IT and end-users to accept and implement those changes?

Jason: With the board, it is around continued education. I'm not going to the board requesting a budget. Typically, I would do that with my internal leadership team based on ROI's or things we need to do to enable the business. For the board, it's just awareness, education, making sure they understand the risk and the challenges as we continue to progress the business model. From an internal standpoint, getting users and our IT partners to adopt certain capabilities, have the understanding they are control owners in a lot of cases and that security doesn't necessarily just own security, it's everyone's responsibility. As CISOs, we have a responsibility to continue to instill that we all play a part in this and again, a lot of that goes back to relationships and education. Oftentimes, when I talk to up-and-coming leaders, the biggest feedback I get is, "We aren't getting the support we need for our IT partners" or they're just not doing the things they need to protect the company. I always ask, "How are you affecting that and inserting yourself to make sure that you have the right seat at the table? How are you providing that awareness and that education? Do you have one-on-ones with your IT leadership partners?" We all play a part in that and can't sit back and say they're not playing along.

Allan: It's all relationships regardless of which half of the question you answer. I will echo this idea that you don't go to the board for money, historically it's never been the board that I ask for money from. In my experience as a CISO, one time have I been in front of the board having a money conversation and that was when a priority we established the previous quarter became a secondary priority because of a critical security shift we needed to make. It was more of a tell than an ask. Budgeting conversations take place with the CEO or CIO depending on where you report.

2. Are there any tips and tricks or tactics that can be done to make cybersecurity more interesting to end-user so that they are willing to be a part of the program you are trying to implement?

Jason: One of the things we understand is that all of us are the weakest link and when attackers try to target organizations or entities, they're going after the end users because they know that they are sometimes the least equipped or educated. Our role is to continuously educate our end users and there are several ways to do that but one of the biggest things is on phishing simulations. I know this has been

around for many years, one of the things we've just rolled out here is the ability to click a button so users can report a particular email. The more we can make it easier for the end-users, the better it is for us. Oftentimes for us, we have to say take that email, copy it as an attachment, send it to this generic email box and it goes off into an abyss. If there's some sort of follow-up communication back to the user to say thank you for the response and give them information on if it was a phishing email. This kind of follow-up goes a long way, and we should do it more and more from this perspective.

3. Allan, I know you have some fun gamifying cybersecurity. Can you tell us a little about how you've done that and how it's engaged everyone from the bottom to the top in your security program?

Allan: People naturally like to compete and team up with one another and compete with the other guys. You want to reward the people that report, you don't want to punish the people that click. But if you can get the reporting statistics and say, "Oh look marketing caught more fake phish than HR did" and start having these kinds of public competitions around them, I think that's one great way to do it. Another trick for adoption that I've always found is to try and go for what I call the "two-fors." This is something that improves the security posture of the organization but also achieves somebody's business goals. For example, when you got SAML and MFA and everything going, enabling SSO. You've centralized your identity which is a good thing for security but you've also made it easier for people to log into things so they can get their jobs done quicker and they see security there as a coat of Teflon on the frying pan rather than a frying pan to the face.

Jason: Security as we all program, try not to make it a one-size-fits-all. There are different personas and if we can tailor to those various personas and if there's also the ability to reward users. For example, don't just roll annual training and have folks sit through an hour or so of training each year. Have a test-out option so that if they take the test and pass it, they can bypass the recorded side of the training. Those who have stayed diligent and paid attention, if they test out, that's another tactic as well.

4. What was the biggest threat of 2021? Do you anticipate that it'll be a threat in 2022? What was the greatest obstacle in addressing that threat?

Allan: I'm going to say ransomware for 2021. Yes, it will continue in 2022. It's only going to get worse. It's still growing. Peak ransomware has not happened yet. And the biggest obstacle to overcoming it, there are two facets to how ransomware gets in your door. It used to be that it was largely through phishing emails and a little bit through exploited vulnerabilities and the more recent stats I've seen, in some cases the vulnerability exploitation hires so it's 40/60 60/40 split now depending on whom you talk to and which study you look at. And what that means is you've got two challenges as the CISO that you go to the deal with. The first one is getting MFA rolled out for all your users so

that the phishing and the login credential harvesting is blocked by that strategy and the second one is vulnerability management which has the precursor of asset management which I'm going to declare to be the biggest hurdle for anyone to overcome. You can have all the best intentions and all the right tooling in the world, but if you don't know where all the servers and workstations to go deploy those solutions, then you're always going to have a kink in your armor.

Jason: Part of it is being ready and having the visibility, but a big part of it is also the resiliency. So, if something does happen, how do you recover from that? There are two recommendations there: One is even if it's out of our purview, but our backups and restoration are a key part of our security program and sometimes we don't think about that because that's in the IT area, but that can play a big role in if something does happen. A part of that is doing regular exercises. The concept of these tabletop drills where everybody across the organization that plays a key role understands their role if ransomware does happen. Part of the key decisions come from the top as well like whether to pay or not to pay, when do we notify our regulators and investors. There are lots of key decisions that need to be made where it involves leadership as well so as we go through this journey, it's important that they're on board as well and understand their role. For me, it's two things: one is the supply chain. That continues to be a big area of concern for all of us as we look at more reliance on third parties, so how do we understand what those ramifications are upstream and downstream. Understanding inventory is our key third-party providers and what they do from a business enablement standpoint and how do we identify when there is an impact. Lastly, talent is a big issue. As COVID has continued to persist, we've realized that people can work from anywhere so we're all competing for the same talent and that will continue next year as well.

5. Why do you think asset management is such a challenge?

Allan: In a smaller company, it's not a big deal. Generally speaking, you know what servers deployed, you know what laptops you've issued and what VMs you have spun up in the cloud. As you grow, any organization with more than a hundred people, you're going to start finding there are things you don't about. You're going to find that you have in every category of asset you might have there are things you were unaware of. It's not just size, it's also time. Over time any organization, even if on January 1 you truly know every single asset you have, by December 31 you don't. There's a time factor too. That can be a variety of things like more people adding more things to the mix without going through the proper process. But it's not uncommon at all for a company that's been around for a long time to have assets that have gone forgotten and are still around. It could be that people who use to manage them are no longer with the company and anything else. I think it's both time and size and scope that make it incredibly difficult and as cyber practitioners, you're not the ones who own these assets in the first place. You're reliant upon IT and engineering or other people who may or may not follow the process and so you're forced to do an after-the-fact assessment using various sundry

tools that aren't going to give you a complete and comprehensive picture. You'll find that you have to triangulate data. You may have agents that tell you you've got 10,000 endpoints and then you do a network scan and discover you actually have 11,000 but then this other thing says you have 9,000 and something else says you have 8,000. It's not something you can easily get ahold of once the sprawl has begun.

6. The Log4j problem is dominating the cybersphere. How has responding to this threat been any different than responding to any other? How does it differ from past threats and what are you doing to ensure/limit the scope of the damage?

Jason: The reality is we've had many of these types of events in the past. While this one is more pervasive because more organizations and vendors utilize APACHE and the open-source components that are embedded in a lot of the applications and products that we use as opposed to previous ones may have just affected certain product lines or vendors that many of us use. But if you think back to Heartbleed and others that created an industry response, I think the difference as we've matured as CISOs is that we're collaborating a lot more not only with each other but with our vendors, with their IT partners. We've realized that in cases like this we're all in this together. As an example, I have a couple of Slack channels or signal groups that we are sending constant updates on what we see happening in the cyber community now. My recommendation for up-and-coming CISOs is to get out there. I know it's more difficult with COVID, but wherever you can interject into local or national forums, do periodic dinners when it's possible to continue to grow that network and relationships because in times like this you'll need it. There's so much sharing and collaboration going on at this point. My tangible recommendations are that you have good relationships with your vendors, and you have good relationships with your peers in the community.

Allan: I would not be functional as a CISO without the community I can rely on. It's funny, it's counterintuitive because CISOs by nature are security people and by nature, everyone thinks these are paranoid and secretive people that play everything close to the vest. The amount of cooperation and coordination that goes on between CISOs, it's out there it's available, talk to people on LinkedIn, find out about Slack groups, find out about signal groups, find out about local activities and groups. Make friends, make connections. You'll find that together we hold each other up.

7. Which area of or approach to organizational security do you feel companies are mistakenly not paying enough attention to?

Allan: I hate the phrase, "Shadow IT." What I like is the phrase, "business enabled IT." The idea is as a CISO, you're supposed to move at the speed of business, and you can't always do that. What you'll find is the business will move at its speed and get ahead of you. The stuff we call shadow IT is really the people that are deploying things they need to deploy. If they've got a mission to get done and they need a new service spun up and

don't have time to wait on IT and security, they're going to just go get that server and deploy it and get running with it and tell you after the fact. It's a constant challenge on the CISO and not on the business that CISOs have to move at the speed of business and look at those moments, take them apart and figure out what compelled these people to "break the rules," go with the insecure option, bypass security to do what they need to do and how do we as CISOs focus our program on addressing those problems. It's not so much as what the business neglects but what we ourselves often find that we've neglected which is velocity.

Jason: Two things that come to me is one is as we've made lots of investments in various tools, oftentimes it's challenging to know the effectiveness of those investments so the more we can identify capabilities to test those controls to make sure they're working as intended. The good news is there are more automated capabilities that are coming out to focus on this. For example, if we have ten tools that are in place to identify and alert us to potential threats or anomalies, can we simulate attacks to test those tools that they are working as intended and which of those tools are giving us the biggest bang for the buck. Control effectiveness is something I think we need to continue to keep on the forefront and maximize investments that we've made because oftentimes we'll buy a tool, turn two of the ten switches on, check the box off and call it done when there's a lot of other capabilities that we can leverage out of that. Secondly, the concept of security performance management is another area that continues to evolve in importance so how do we measure our program and be able to model where we make certain investments and how that's going to impact our program and how do we clearly articulate that in a business context? Really why we're here as CISOs is to enable the business. We could talk about tools and quantifying fair models and risk and so on but the more we can translate that into business-speak and show them the progression of the program and how it's enabling the business, I think that's an area we need to continue to focus on.

8. Any other thoughts?

Jason: Oftentimes I get the question of, "Why did I go down the CISO path?" I think the unique thing about this role, or any security leader position is the ability to not only influence the organization that you're protecting and serving but seeing the bigger picture and mission. We're having to evolve to be more business leaders so it's not just about the bits and bytes. I think it's fascinating that we are technically in a technical position, but we really have to understand the business and where it's going and be part of that journey. I think the other big thing is we have an opportunity to impact the entire industry as a whole so as we continue to come together as leaders, how do we influence and change things? It's exciting to be part of an organization and see that bigger picture but also help affect change across an entire industry.

Allan: It's easy to think when you join information security that your job is to secure all

the things and what you're really doing is securing the right things. The right things are the most important things that are also the vulnerable things and when I say the most important things, they're the most important things to the organization. It's not security dictating priorities, it's the business dictating priorities. The reason I think folks might enjoy becoming a CISO is it's this perfect intersection of security and business. It's the intersection of risk and business value. It's a fascinating and interesting place to be and there's something new every day not just from the technology side but from the business side. Getting in that alignment and working with the rest of the organization, I always walk away feeling pretty good at the end of my day.

To watch this webinar, please visit THIS link

To download the complimentary Gartner® report, The CISO's Guide to Your First 100 Days, please click HERE