Unauthorized Access: "Board-er" Patrol in Privacy and Cyberattacks
Recorded December 2022

Kamran Salour:
Hello and welcome to another rousing edition of *Unauthorized Access*. I am Kamran Salour and I am joined by my co-host, or as some would say, the sole host of this podcast, Sadia Mirza. Sadia and I are excited for today's podcast because we are joined today by Violet Sullivan. Now, some of you may know Violet as her normal role of VP of client engagement at Redpoint Cybersecurity, but we of course know Violet much better than that. We know her as a great connector. We know her as a great lover of all things cyber. We know her as a professor at the University of Baylor. We know her as a swag maker and of course a lover of artificial intelligence, which I know is very near and dear to her heart. And today we are going to talk with Violet about something a little bit political, some might say. We're going to talk about border patrol. In actuality, we're going to talk about board level buy-in and how to make people care about cyber privacy and risk. I'm excited for today's episode, Sadia, are you?

Sadia Mirza:
I am very excited, you know that. I usually like to just have our friends on this podcast and waste a bunch of time just talking to one another about these kinds of things. And so Violet, in addition to everything you said, violet is obviously a very good friend. I met her at Net D. We forgot to mention that she's also the creator of the best LinkedIn posts and I'm sure that's how most people know her. Violet, we are so excited to have you on and to talk about this important topic.

Violet Sullivan:
Thank you. I've been waiting to get on this podcast too. I am an avid listener of *Unauthorized Access* and love the team at Troutman Pepper, so thanks for having me on. And, also, can't wait to call your bluff whenever you have someone non friend join the podcast.

Sadia Mirza:
No, they're all friends. But Violet, when we were talking about, essentially, we wanted to know what do you want to talk about? And you raised this as being a really important issue and something that you continue to learn more and more about as you interact with your clients. And so why don't you tell us what you think the problem is? Why can we not get the buy-in that we need from the board even at this point, given all that goes on and the attention on privacy and security.

Violet Sullivan:
I think this topic came to mind because it's one of my biggest pet peeves is that we are seeing this. This is a risk that we're seeing on a global scale in terms of the media and the news. Big tech is all over being vilified through this cyber privacy risk and we're seeing it from the consumer's perspective and privacy. We're seeing it from the business perspective more on the risk side and cybersecurity. I really think the biggest problem has been the message, the communication and how this is presented when it comes to actually doing anything about it. What has traditionally been a cleanup focus and reactive response to risk has been tried for 10, 20 years to be addressed at the organizational level, like let's get out in front of this, let's prepare. But the incentives aren't there and the communication isn't there to explain to everybody how they should work together to solve this problem.

So, I really just think it's because we traditionally see a boring monotone voice coming to the board and explaining cybersecurity as this technical subject with monotone. Just think about how this has been traditionally presented. It is a legalese talk lecture webinar that is communicated without necessarily tying it to something that they can tangibly think about and get worried about and interested in. And so, I think that the board know they have to do this, but there's not teeth in understanding. So, we could talk all day long about fiduciary duty and duty of loyalty, but I don't think that's the issue. I think it's the way it's presented and how we need to shake up the communication around these issues of cyber privacy and risk.

Sadia Mirza:
That reminds me of when we were at Privacy and Security in DC and it was something that Ron had mentioned, and I know one, we know how much you adore Ron. I think everyone listening knows how much I adore Ron as well, but this was something that he had talked about and I think it's really true, because what you're talking about is the messaging and how it's being communicated to the board. And one of the questions that Ron had asked was, "Look, what's the most important characteristic or skill needed in a CISO?"

And I think a lot of people at that time were like, oh, a CISO really needs to be a technical expert and really have a good understanding of the technical issues that you face in cybersecurity. But then you can obviously tell where the discussion was going, is that actually your CISO, the most important skill that the CISO should have is communication. And I think that goes back to your point, you can't just have someone that gets in and just talks text speak to the board. You need to be able to communicate the issues right directly to the board in a way that they can understand it.

Violet Sullivan:
Yes, and I'm going to pull from that same example when that CISO discussion was happening, Ron pointed out something that I love because there has always been the scare tactic that is around cyber and privacy even and even risk. So, all those three topics, the scare tactic we always hear that if's, not if but when, and I'm guilty of it too, just as Ron admitted that he was guilty of it. You have done that to your clients to try to shake them and say, this is a real issue. But I think what I've realized once you get past the scare tactic, your approach is that all of these teams who are asking to collaborate on a problem have never worked together before. So, you have in a cyber incident or privacy issue, take pixels, take anything that's on AI, anything that's on the horizon that could cost a company money, whether because of disaster or regulators or litigation.

It's going to bring together technical subject matter areas. It's going to bring together HR communications, legal risk, it's privacy compliance audit. It's going to bring together so many different groups that have no idea how to align their interests. And those goals have never been set side by side and figured out. So not only is the CISO primarily not required to be only technical, but they're also required to be able to see a little bit of all sides of the business to be able to get their message across. I think that's where we're actually failing at a CISO only being technical because how in the world are they going to be able to think about the privacy concerns when they're actually conflicting?

Sadia Mirza:
I think Violet, what we're talking about is still really the communication and I guess another problem is the isolation where everyone is operating in their own worlds. What else, just you being on the front lines and talking to clients about this and dealing with this issue, what other problems are you seeing with the way that we're approaching it now?

Violet Sullivan:
Well, I promise we'll get to how to fix it, but I see the biggest problems besides communication and this isolation of different departments working together in a cross-functional way that they never have is the other common one, which is lack of preparation and they have not seen the issues. And so then lack of preparation, you also see a lack of efficiency or like duplicative behavior. You'll see two people doing the same thing. And the biggest example is communicating to third parties. Someone calls law enforcement even though that's not in plan to call law enforcement and it's the wrong people to call law enforcement. I did a tabletop yesterday where Compliance said that they were going to reach out to Breach Council and Legal said "No, that's our job to reach out to Breach Council". I mean this is a very specific example, but when you take a step back and look at the problem, these are the things that can happen when there's not a cohesive pushing towards a solution.

The other problems just to rattle them off is problem practicing difficult decisions. And I see that without getting forced out of the “it depends” mode, it's going to stay in “it depends.” It's going to stay in this world of well, we'll figure it out when we get there, or every cyber incident's different so we're going to have to approach it differently. instead of practicing the hard questions or doing a daily, monthly, quarterly, some conversation at the executive level of do you know what we would do if this hit us? This just got our competitors, what would happen in this situation? Or HHS just issued a ruling, how does that impact us, and what would we do if we got questioned about our website? I think the problems are kind of ripple effect. It starts with communication and silos and then it goes into the fact that because everything is so siloed and it's not important, there's these gaps of efficiencies and this almost frozen decision-making ability.

Kamran Salour:
I think you raised a really good point there, Violet, when you talk about the “it depends” vacuum. And it's easy as lawyers to fall back on the “it depends,” because obviously how you react, what legal implications a situation is going to create, is obviously going to depend on the situation. And same with respect to business decisions. So, I think that underscores the importance of doing real world exercises, obviously in a controlled tabletop type setting where you are actually forcing the business to make these difficult decisions in terms of, all right, here are the facts. Pretend that this is a real scenario, this is the situation. What are you going to decide? Not only does that help make the whole cybersecurity world a little bit less esoteric to the business folks, but I think it also helps the business folks realize, "Hey, to make some of these decisions, I need guidance from Legal. I need guidance from Security," and vice versa. Security and Legal will need guidance from the business.

And that's how you start to put a change in that notion of, look, cybersecurity is a one-off issue. It's not something that we need to really focus ourselves on. If something happens, our CISO is going to take care of it and they're going to just report to us. So, I think that's very important, not only because it's actually going to help the company practice making those decisions, but I think it's going to help with that buy-in for making people understand why it's a three-part

conglomeration of decision-making and it's not something that is siloed because what one arm does, impacts the other.

Violet Sullivan:
I was actually going to bring up Sadia's silo point as well and underscore, it really does come back to that because once you get, and I see this a lot, as soon as I hear those words and as soon as I hear the “it depends” or it'll be taken care of, and I pushed it further, it's without a doubt, once they make a decision that someone else that hears it, has an impact. So that ripple effect does not get tested if you're not forcing those decisions.

Kamran Salour:
The positive impact of forcing that is multi-fold because not only are you going to help get that buy-in, but you’re also going to help people really start thinking about the interplay between business, legal, and security. You're also going to help the company at least work through some of those potential issues with the plan that you were talking about. Duplication of efforts if two people are calling the same person, duplication of messaging. Just little things that are hard to really identify as potential issues unless you actually put pen to paper so to speak and go through the process. It's one of the problems I think as practitioners we often face is the IRP that we draft may make perfect sense in a vacuum, but until you actually work through the steps, there's almost always going to be something that comes up that's unanticipated or that nobody really thought about. And it could be something as simple as, oh, who's in charge of calling this person? The only way you can really find out those issues and work through them is if you actually go through the process.

Violet Sullivan:
And I think it saves time over all efficiencies, not just who's doing what, but what I also found is it's awesome to get the debate out ahead of time because then you can table it and say you two decide, you two go off and have this conversation separately, because if we were in an actual incident, you've seen it, Sadia's seen it, we've all seen that the amount of tenseness, anxiety and frustration, it escalates in an incident. And when you're all on the calls, that is the worst way to spend time. And I've been on three-hour calls that have been about something that could have been debated ahead of time.

Kamran Salour:
Yeah, how many times do we see on calls a company that their position is very staunch, we will not pay a ransom and they will stick by that decision for 48, 72 hours and then ultimately come back and say, well I'm just losing too much from a business standpoint, try to restore. I'm going to have to pay the ransom. And so, think of all the time and money that was lost because you didn't really have to force yourself to think about what you would actually do in that situation until you're actually presented with it.

We certainly see it all the time. Unfortunately, still, notwithstanding that we see it all the time, but notwithstanding all the benefits that we've talked about here, it still seems to be difficult bridging this gap. And I think it's something that we're going to struggle with going forward and hope that you can make incremental changes as you go through. But I'm not sure what's going to create a paradigm shift in the thought process where more and more companies will embrace this notion of working together and not siloing themselves and basically saying, "Well, that's a cyber problem. Let them deal with it and we'll turn a blind eye to it."

Sadia Mirza:
Kamran, to your point, I don't think organizations are going to be able to change the existing culture overnight. But Violet, what would you say, what are some of your top three, if you had to pick three strategies to start making baby steps in the right direction to make cybersecurity be something that the entire organization, including the board is thinking about, where would you suggest a company start?

Violet Sullivan:
Kamran was really getting to the solutions towards the end, forcing them out of “it depends” mode is probably the first one. And the way I would say how to do that is really customizing examples to the business or industry that you're talking with and whether you're the internal CISO or you're the outsider guiding this team to face their risk, I think my favorite example is knowing the points in incident response that are time sucks or pain points and we know them to be approval processes, the contracts, the big decisions, pay or not pay, ransomware. We don't advocate for one side or the other, but one of my favorite tricks for, and just to give an example of go seeing someone out of “it depends” is when I create a ransomware scenario, I usually create it to be such a hard decision not to pay the ransom.

I make it low, like obscenely low, unrealistically low ransom, $20,000 ransom payment, $50,000. And I get the buy-in from the IT team to say, okay, I know this is unrealistic. We are creating a scenario that's intentionally trying to pit operations against IT. I need you to understand it's for your best interest so that you could argue about it now rather than arguing about it when it's a $3 million ransom. So, I create conflict in the practice scenarios or practice ideas. Even when I present to the board, I present it and show the pros and cons on both sides and try to simulate that feeling of the different values and issues because we all know that they're going through in a cyber incident, a split-second risk assessment. They don't get the value of doing the pin test and risk assessment at the same time over months.

They do it within days and they have to make an assessment of risk and make a difficult decision. So, when you force them through that, through creating the conflict in a customized way to make it close to home, that's one piece of it. The second piece I think is being able to translate it in a way that's not going to bore them to death. It cannot be presented in a writing. It cannot be presented in an IR plan. It needs to be a significant wake-up call to an organization that doesn't already prioritize it.

Now if you have culture going in, I think you have a better atmosphere to do things like sending out updates and emails and X, Y, Z and having a well-rounded security culture. But I think if you are wondering how in the world to get past the threshold of having your executive team or board care about cybersecurity, you have to realize that the other people that get money and buy in and budget are loud, squeaky wheels and security and privacy and risk have to figure out how to be a loud squeaky wheel rather than a boring, monotone academic nerd.

Sadia Mirza:
I'm curious, so when you present to boards, how often do you find a member of the board having a cyber background?

Violet Sullivan:
Well, I take that back. I was going to laugh and say very few, but I will say I always try to find that champion. There's at least one usually, and I'll tell you that the one that usually is, if they're not in it because of business, it's because they have had an incident that has impacted them. I have had incidents where I've worked on the same breach or past breach eight years ago that the head of marketing did. And then I always connect immediately with them and start bringing out their experience because once they validate, then I'm no longer someone on the outside. I think that validation that, hey, this really is scary. We did see this happen to our competitors or the company I was at did have this happen. I think that's really validated and I really think there has to be that validation internally in a company.

Then once it gets beyond that C level to say, okay, this is a real threat. We do care about this. So, I think it's important for anyone that does have that tie-in to cyber privacy or risk to really speak up that this is a real issue so that everyone else comes on board with that. There has to be a champion. You can't just have an outside person come in, tell you that this is a big deal and then nothing happened. There has to be someone to lead a task force or a committee or a movement because what I've seen over the last eight, nine years with cyber privacy is no one does this out of the goodness of their own heart. There has to be some incentive, empowerment, or elevation of importance to these areas in some way.

Sadia Mirza:
You're absolutely right. You need to find that champion because I think about myself, I do so much privacy like CPRA, right at the top of my mind. So, every time I'm in a discussion, somehow, I'm going to bring it back to, by the way, what's going on with CPRA? What are you guys doing? Because that's my area, that's what I focus on, especially right now. That's what I'm doing. And so, if you had someone on the board that also has that focus, maybe it starts there. Making sure that there's someone on the board that cares about this and keeps bringing the discussion back to cybersecurity. What is the organization doing? How are we preparing so that it's not so much of a forced conversation? It comes more organically and naturally within the board itself. That again, could be a big, maybe that's not a baby step, but I could see having that champion could go a very long way.

Violet Sullivan:
Yeah, it could be an open door or it could be something you find once the doors open, I think it could go both ways, but I agree. I think that's a big piece. Another piece, the translation piece is so important. I realized when you can't get through, I can always tell when I can't get through to a board, and one of the first things I'll just try to say is, well, what do you use your computers for? What do you use your technology for? And I'll just start asking questions because that will help me figure out what they value and where they have the value. And then I try to tie the money risk to it because if all else fails, if you can't find the champion, if you can't translate, try to find where they care about losing money and then it goes back to the thing Ron needs. It's somewhat a scare tactic, but if you can't get through any other way, put a monetary value to it and explain how they can have a negative impact.

Kamran Salour:
You raised an interesting point here. We talked about, we'll call it Ron's approach because I think we're all three of us here are big fans of Ron, which is the non-scared, straight approach where you don't want to come in and say you're going to be under attack. It's inevitable because

you tend to tune that out. But ironically, what we've really talked about here is a subtle way of scaring the board or the businesspeople into appreciating the severity and the potential consequences of having a cyber-attack. So, there's an undercurrent of fear, which I think is important for people to really appreciate what's going on. So, it's not so much as scaring them into shape, but really just having them realize the potential implications and the need really to have both somebody on the cyber side as well as on the legal side to help you get through that process.

So, I think that's just an interesting tidbit of what we've discussed. Unfortunately, we are out of time. I'm getting the signal from our producer here in studio. I am going to wrap this up, but I want to of course, thank you so much Violet for your time and your information and incredible insights. I'm sure we could have this discussion for many, many hours, but I know that Sadia will cut me off before I continue to go too much further. But I did want to thank you. I want to thank all of our listeners for their listenership this year. This has been the first six months or so of the *Unauthorized Podcast*, and this will be our last edition of 2022.

We hope to be back in 2023, but let's see what the higher ups here at Troutman Pepper say. So, this may be your last opportunity to get a hacker hoodie. Today's trivia question is a simple one, and that is where does Violet teach? If you know the answer to that question, you can email it to us at incident.response@troutman.com and the first person to send the correct answer will receive a hacker hoodie from Troutman Pepper, but until 2023, we will not speak again. Thank you so much, Violet. We really appreciate you and look forward to continuing this discussion at some point.