Barclay Damon Live Presents *Cyber Sip*™ Episode 36: "You Need Exercise—Tabletop Exercise, That Is," With Kyle Cavalieri

Speakers: **Kevin Szczepanski**, Barclay Damon, and **Kyle Cavalieri**, Avalon Cyber

[Kevin Szczepanski]: Hey, everyone, this is a *Barclay Damon Live* broadcast of the *Cyber Sip*. Practical talk about cybersecurity. I'm your host, Kevin Szczepanski. Let's talk.

[Kevin]: Hey everyone, back for another episode of *Cyber Sip* with Kyle Cavalieri. Kyle has more than 15 years in the IT security industry, and since November 2020, he has been the president of Avalon Cyber. Kyle, thanks so much for joining us today.

[Kyle]: Thanks for having me, Kevin. Looking forward to the conversation.

[Kevin]: Yeah, me too. So today we're going to talk about tabletop exercises. Everyone is talking about them. A lot of organizations want to do them. And Kyle, I know you've been out there for Avalon Cyber, talking about and conducting tabletop exercises, so I thought you'd be the perfect person to tell us all about them. So let's start with the basics. What is a tabletop exercise?

[Kyle]: Yeah. So specifically, you know, it being a cybersecurity tabletop exercises, which is the area which I spend a lot of my time, you know, spending and delivering. It's a moderated exercise that really tests the organization's ability to respond to a cyberattack. If you're evaluating your incident response plans, you know, it shows how aware the organization and specifically the stakeholders are aware of their roles and responsibilities in the event that there was some type of a cyber incident.

[Kevin]: So you mentioned the stakeholders. I want to come to that in a minute. And you alluded a little bit to why it's important to do one. If I were trying to convince a client of mine to do a tabletop exercise, what do I say that really drives home the importance of doing one?

[Kyle]: Yeah. So, when I'm speaking with perspective clients, I ask, are we thinking about the right things? Right? I always start with maybe current events and evaluate kind of what's going on in the world today, what could be impacting the organization as a whole. One of the more recent conversations I had with a prospect was specifically around artificial intelligence and ChatGPT. Are we thinking about that? Do we want our team members or employees or associates, you know, leveraging artificial intelligence or ChatGPT within our organization? What sort of risks to our organization does that ultimately introduce? And if those are conversations that are worth having as a group, you know, I want to make sure that we're building some sort of a program, you know, specifically around a current event issue like that. But taking a step back and thinking more about, you know, why you should be doing a tabletop exercise. You know, do we need to evaluate our plans as a whole? Do they need improvement in some way, shape or form? Do we need any clarification in regards to the roles and responsibilities of the stakeholders? Like I discussed before. These exercises can also be used to further define budget for gaps that might exist within your response program. Maybe that's a training issue. Maybe that's a people issue. Maybe we don't have the right team members inside. Maybe we need to be considering what vendors we should be having. Maybe that's an allocation that we need to be making and communicating with our executive team to ensure that they're aware that in the event that

something happens, we need to make sure that we have budget aside to specifically deal with that. You know, the other thing too, Kevin, is that I spent a lot of time working with prospective insureds and they are specifically responding to supplemental questionnaires to their cyber insurance, you know, application that you know, where they're being specifically asked, what are you doing or when was the last time you have tested your incident response plan? These tabletop exercises are the answer to those questions, because they're exercises specifically designed as a group. How would we respond to a particular incident? And then finally—and one of the biggest "aha" moments that I see when working with organizations—is really the inter-departmental communication amongst the group. I come across organizations that are really well-oiled machines and can communicate efficiently, you know, cross-departmentally. And then there's other ones where there's definitely opportunity for organizations to improve with that communication. And it's just about knowledge of knowing, who do I need to go to when I have this type of question. And having everybody in a very comfortable environment, one that there are no dumb responses or dumb questions, "it's okay to not have the answer" type of environment. Nothing better than having those types of things flushed out there than when you're in the heat of the moment of an actual cyberattack.

[Kevin]: Right. So a lot of good reasons there. Everything from training to risk. And I think we've not done an episode on risk assessments. But for those in our audience who don't know, the requirement of an annual risk assessment is becoming increasingly important in some of the new regulations we're seeing. But overall, and very simply, you are testing your response capability. It's one thing to have it on paper. It's one thing to have policies and procedures and think you're prepared. But unless you test, you will not know for sure. It's sort of like the old adage, Kyle, "Practice makes perfect." I never hear anyone say these things anymore, but we all know it in our sports teams; if you're not practicing before a game, you're not going to do well in the game. And a tabletop exercise is really that proxy for practice in the cyber world.

[Kyle]: Yeah, you're exactly right, Kevin. And you know the other piece is and I... it's almost become cliche because I hear it so often that you know, "it's not a matter of if, it's a matter of when" something like this is going to happen.

[Kevin]: Right.

[Kyle]: So there's no reason why you shouldn't be prepared as an organization. And these exercises are really designed to make sure that you have the right people in the room, you know, who to involve. And there's a there's a consistent process to follow.

[Kevin]: So you mentioned let's go there then. You mentioned having the right people in the room. So the next question I wanted to ask you is: who should participate in a tabletop exercise? And then we'll break that off from the separate question of how do you prepare for one?

[Kyle]: Yeah, sure.

[Kevin]: So who should participate? A lot of a lot of people might say, well, it's your IT. And your information security team. Others might say, no, you should have the C-suite in the room because those are the people that are ultimately going to make the decision. How do you decide whom to recommend to your clients or customers participate in a tabletop?

[Kyle]: Yeah, I mean, I've done tabletop exercises with three different types of groups, right? I've done exercises where it's been strictly technical folks in the room. So that's your IT, your IT security folks. I've done exercises where it's been your executive leadership all the way down to IT support. And then I've also done, you know, the tabletop exercises where it's just the C-suite and the executive and senior management team. I think there's pros and cons to each of them, candidly, you know, but the ones I have found to be the most meaningful and I feel like there's the most takeaways and opportunities for improvement have been where you kind of have everybody in the room. You know, from executive leadership down to IT support and

management. You know, the pro there is, you know, you're going to have the executive leadership kind of hearing what's going on. They're going to be able to opine on things where, you know, the incident itself is evolving either through an injection point or something like that, or just simply the conversation that's being had. I was doing a tabletop exercise where, you know, an IT director was describing what they would do based upon a particular fact. And the executive leadership member was like, I candidly just don't agree with you. Like, I want to make sure that that we address this a particular way. And you know, from that, that's a "lessons learned." It's an opportunity for us to go back in to reevaluate the plan and make sure that, you know, if anything, there's additional conversation about that particular talking point. But we address the plan to make sure that it meets the expectations of senior leadership.

[Kevin]: Yeah, you probably wouldn't learn that if you didn't have a tabletop exercise and I know it's going to take time and it's going to take an investment of resources on the part of senior management, but if you don't have everyone in the room who is going to be involved in responding to whatever it is, it's a ransomware attack, business email compromise—you're really missing an opportunity and your test is incomplete. It's like only testing on half the chapter that you spent the last month learning.

[Kyle]: Yep. Yep. Exactly right. Another point that I want to bring up is I really enjoy having, you know, in-house counsel involved in these conversations. There's a tremendous amount of opportunity for them to kind of learn about, you know, what's going on and then they might be the gatekeepers as it relates to the engagement of a broker or an insurance carrier.

[Kevin]: Yes.

[Kyle]: Particularly with risk management. They might be the ones that are going to be, you know, deciding how vendors are ultimately engaged. And then there's also internal decision-making that needs to be done as well for purposes of managing internal risk and communication. And, you know, making sure that outside counsel is properly involved to protect privilege and those types of things. So I just thought I would make mention of that as well. Because having legal in that room and having them, you know, providing their opinions, I think is incredibly valuable.

[Kevin]: No, I think you're absolutely right. So let's turn to the next topic, which is preparation, and then we'll talk about an example of a tabletop exercise. I know it's hard to talk about an example without doing it, but if anybody can do that, you can. But let's talk about preparation. What are you doing with the organization in the days and weeks preceding the tabletop exercise to make sure everything is good to go?

[Kyle]: Yeah. And, you know, I think with anything, planning is maybe one of the most... it's the paramount step in the process of actually executing on a tabletop exercise. There's a ton of free resources out there that are put out by CISA and some other organizations.

[Kevin]: Those are very good. They are very good. There to the in fact, I have it right here. I have one of CISA's tabletop exercise packages, that is the Cybersecurity and Infrastructure Security Agency. And you can go on their website and they will give you...you'll have access to myriad materials, multiple pages, so that if you want to set up a PowerPoint or a Word document laying out a plan for a tabletop exercise, you can do that. But I imagine you're going to tell me that that only gets you so far.

[Kyle]: Yeah, exactly right. And I think one of the most important parts as part of the planning process is making sure that you're picking scenarios and that the context is relevant and culturally relevant to the organization that you're working with. There's nothing worse than sitting through a tabletop exercise for two hours and at the end of it be like, well, that was nice, but that's never going to happen here. You know, you might have those people regardless, I guess you could say. But, you know, you want to make sure that the content you're pulling together is something that is relevant, something that they can relate to, saying, oh, yeah, that's right. This team would be doing something like that. So let's talk about this further. And so making

sure that you're customizing whatever scenario we talked about ChatGPT before, if you're working with an organization, you want to make that a focal point or at least an element of your actual incident. Perfect way to figure out, okay, well, how can we use that object and inject it in some way, shape, or form so that the team as a whole needs to start making decisions? And it's totally fine, you know, when you're going through that exercise to realize, hey, we've got some work to do because this is an area that we totally were not expecting or not ready for. And so having that planning element in place is definitely a very important process.

[Kevin]: So planning... the point is you can tailor them to the particular organization, large or small, and you can tailor them to the particular industry that organization is in. Because I imagine, for example, a healthcare provider might have a very different kind of tabletop exercise than a professional services firm or manufacturer might have.

[Kyle]: Yeah, absolutely right. It needs to fit the industry that they're in, the issues that they're dealing with within that industry, etc. You know, I just wrapped up a tabletop exercise for a higher education institution. And, you know, they wanted a current event element such as ChatGPT to be an aspect of what we were going to be discussing as part of that tabletop. And it was it was fantastic because these were things that they weren't prepared for. They didn't have that information internally to properly respond, which was a huge takeaway.

[Kevin]: That's—and a quick point before we move to an example of a tabletop: If I've learned anything over the years, not only from tabletops, but in other experiences, is that folks, when you are designing a test, do not design the test to be passable or easily passable, design it to be very difficult because if it's too easy, you won't learn anything from it and it'll only be more difficult down the road. You want to design a test that frustrates you, that takes you to the failure point so that you know where you need to improve and then can identify the ways in which to improve. Am I right about that, Kyle?

[Kyle]: Yeah, I mean, not to frustrate... the, the audience by any stretch of the imagination. But I will say it is always a good idea to include novel topics, things that are unique and might press the bounds of the original plans that we might have. Because I tell you what, the conversations that come out of those novel topics are incredible because now you're really getting the creative juices going of the audience and you're getting people thinking like, oh, you know what? We might need a, you know, specifically with education, we might really need to start, you know, from an ethical perspective, how are we using artificial intelligence? What do we need to be telling our students that they can and can't do specifically relating to that, that item? So those are those are the types of things that I find really exciting because I myself learned so much from those conversations because, I mean, I'm in the trenches with them and understanding, hey, how are we going to take this topic and kind of work through it?

[Kevin]: So in a few minutes, Kyle, we talked about what a tabletop is, why you do it, and how you prepare for it. Can you give us an overview of what a tabletop exercise looks like and pick a cyber incident for us? It could be anything that you've dealt with, but you know, how long does it take and what actually happens during the exercise itself?

[Kyle]: Yeah, sure. And I'll just use ransomware as an example. It seems to be the most common one that people ask about. We do so many of these ransomware type tabletops that it's somewhat of a lighter lift for us now.

[Kevin]: Right. But it's still out there and it's...not going away.

[Kyle]: Exactly.

[Kevin]: Right.

[Kyle]: And so from an execution standpoint or the day of the event, you know, the way that we like to do it is we kind of prep the group by giving them an overview. Right? We create a scenario that makes that make sense to them. But it's an evolving... it's kind of like "learn as you go" books. I don't know if you remember those books from back in the day, you choose your own adventure type that thing where it's like we're taking a small part of the incident and we're describing it to them. It's like, This is what we know right now, what you're.

[Kevin]: Actually reading and reading it or putting it on a board...

[Kyle]: Up on a PowerPoint presentation. We're in a conference room. We're discussing this as a group, and they're taking what they know, at least at this point, is the incident. And they're having conversations specifically about that. From there, we insert what we like to call injection points. And those injection points are really the evolution of the incident itself. It could be a matter of days or weeks or months, but this is how the incident itself is ultimately rolling out. So how are the decisions that we have made previously in the previous injection points or the overall summary, you know, did we make the right call? Do we need to pivot? Do we have the right people in the room? Do we have.

[Kevin]: Yes. Can I just jump in and ask you I'm sorry to interrupt, but could you give us one example of an injection point that might happen in the hours or even the days following the initial event?

[Kyle]: Yeah. So one example that comes to mind is, you know, maybe the overall summary is, you know, the IT helpdesk receives a number of tickets specifically relating to a high volume of phishing emails that were that were reported by human resources and the finance department. You know, a lot of folks are obviously seeing these email phishings has come in. Then we're, you know, reporting back to the help desk. What do we do at this point? Right. Well, you know, the typical response to that is like, hey, well, we're going to obviously address the tickets and making sure that everyone is great and so on and so forth. The next injection point as part of that, you know, the scenario might be, you know, you might be seeing a bunch of failed login attempts to critical applications that exist within the organization, and they seem to be user accounts that were associated with HR and finance, as an example. Right. So now we're seeing that this incident is ultimately evolving and maybe, you know, the next injection point on that is that, you know, ransomware files themselves are showing up on and critical business shares, network shares, within the company. And you know, this is X, Y and Z, and this is what is ultimately then kind of held up. What where do we go now? So that's just kind of an example of maybe three different injection points that might be presented to a group.

[Kevin]: Yeah. No. So it sounds like you're running through this event in near real time and it's playing out just as it would or almost as it would in the real world. So everybody in the room from IT—assuming everybody's there—IT and general counsel and the executive team is experiencing this, and then what are they doing? Kyle, are you... do you ask questions? Do people volunteer? How does the conversation go?

[Kyle]: Yeah. So after each injection point, I usually bring up a slide and it has maybe anywhere from four to eight questions on it. And the questions are really curated based upon who's in the room, right? If I know I'm going to be doing a tabletop exercise in front of executives or IT management or, you know, business unit leaders or whoever might be there, I'm going to curate questions that is going to allow them to get their creative juices going and start thinking about what they would do based upon the information or at the very least allow them to get up and walk over to another group and say, hey, I've got questions as to what my role would be, because I know you're going to be taking point on this particular item. And so those things are really great. Those types of questions are really great because it allows everyone to kind of collaborate for like five to eight minutes. And then after that five to eight minutes, we'll get back together as a group and we'll talk about what our response is based upon the questions that were asked in the facts that were presented in the injection point.

[Kevin]: So this sounds fascinating. I'm really excited about it and I'm looking forward to doing one. But part of the problem is you get... you're so excited in the moment. But the real measure of a test is what you learn and

how you implement what you learn going forward. So let's say you've gone through and I assume this can be a multi-hour process. It can be however long you design it to be.

[Kyle]: Yeah.

[Kevin]: Yeah, but let's say that the time has expired, and if it's a good test, it's uncovered some issues with communication or issues with security controls or how an organization has designed its response to this ransomware event. What do you do to make sure that you take what you learn and implement it so that you improve going forward?

[Kyle]: Yep. Yeah. Note-taking is key here. You know, when... as we're going through the exercises, we want to make sure that we're documenting the communication that's going on amongst the group in the room because there's going to be little nuggets of information that we're going to learn so that we ultimately can take that back and put together an executive summary and then specific recommendations that are actionable that they can take to ultimately improve. Maybe they need to tweak a plan, maybe they need to design a new policy, maybe they need to, you know, identify an opportunity to educate certain stakeholders or employees based upon particular issues. So, you know, our goal is to make sure that we're capturing as much of the conversation as we can during that communication. And then from there presenting back to the appropriate stakeholders, you know, from an executive summary standpoint and recommendations perspective, these are the actionable things that I think will improve for the next time, you know, we go through this exercise. And the other piece too, is that this is not a destination type process. This is truly a lifecycle. And so it's always very, very important to consider doing these things on an annual basis. It's not something you need to do once a month, but it is something that it's important to get everybody together at least one time a year and making sure you're having these important conversations.

[Kevin]: No, I agree. And it's not generally required now, but I can guarantee in 12 to 18 months we're going to start seeing regulators and other industries asking the question. All right, you have you have done your risk assessment, you have your written policies and procedures. What are you doing to test those policies and procedures? And we're already seeing it in some of the new... I think part of the new DFS Part 500 cybersecurity rule has embedded within it an expectation that an organization will test its policies and procedures at least annually. So this is super critical. Kyle, I'm so glad that we could have you on to talk about this because I think it's a hot topic now and it's only going to heat up over the next 12 months.

[Kyle]: Yeah, awesome. Yeah, I'm happy to be here, Kevin, I appreciate the opportunity and looking forward to doing another with you sometime in the future.

[Kevin]: Thank you so much, Kyle Cavalieri. We're happy to have you on *Cyber Sip* and we will be back soon with another episode.

[Kevin]: The *Cyber Sip* podcast is available on barclaydamon.com, YouTube, LinkedIn, Apple Podcasts, Spotify, and Google Podcasts. Like, follow, share, and continue to listen.

Thanks for listening.