A PROACTIVE APPROACH TO INCIDENT RESPONSE

4/30/2019

Brian Contos: Welcome to the Cybersecurity Effectiveness podcast, sponsored by Verodin. The Verodin Security Instrumentation Platform is the only business platform for security that helps you manage, measure, improve, and communicate security effectiveness.

Brian Contos: I'm your host, Brian Contos, and we've got a really special guest today. Joining me is MacKenzie Brown. Welcome to the podcast, MacKenzie.

MacKenzie Brown: Hi! Thanks for having me.

Brian Contos: Hey, MacKenzie, before we get going, I've got a whole list of questions I'd like to ask you, but can you give our listeners a little bit of background about you?

MacKenzie Brown: Yeah. I actually got into security by accident, if that makes sense. I was a starving college student, as most are nowadays, and trying to find a decent job, and actually ended up getting a temp job in IT support, and I worked really closely with the network team, and we didn't really have a security team at the time, but yet we had a lot of IRS audits, and security audits.

MacKenzie Brown: So, well, kind of reluctantly I ended doing one of the IRS audits for the CISO. So we didn't have a security team, but we had a CISO.

Brian Contos: Okay.

MacKenzie Brown: And did that audit, and really became familiarized NIST 800-53 R4 and Pub 1075, and all those fun information security controls. And so, I came into security through auditing, which it doesn't sounds as cool, but for me I'm, like, super OCD, and enjoy that kind of stuff. So I came in through that, and then decided that, “Hey, I would probably do this for a living.” I went to college for theater, so I'm definitely on the opposite realm of where I started up, when I was 18.

MacKenzie Brown: So, yeah, and then worked in enterprise, for a little over four years, five years. And then I got poached by my now-employer, Optiv. So I am one of those quintessential millennial babies in the industry.

Brian Contos: No, that's awesome, and I love the fact that you came from theater. I think some of the best people that we have in our field come from academic studies that are outside of computer science, or security. One of the best CISOs I know actually has a background in poetry, and--

MacKenzie Brown: No way!

Brian Contos: Yeah. So I think it's that creative element that comes to mind. And also when you mentioned NIST 800-53, I have NIST 800-53 and NIST 800-92 going around in my mind from my days on the SIEM side, and I'm like, "Oh my God, I can't believe that came up again," but...

MacKenzie Brown: Yeah. It always comes up. Yeah.

Brian Contos: So now you're at Optiv. Tell me exactly what you do there. I know you're tied to infinite response, and that's part of your focus, but what is it that you do at Optiv?

MacKenzie Brown: So, actually, when I came on, I came on to a team, a research and development team, that we had internally, and it was a really small team, and we developed program frameworks. And I actually helped write and create the enterprise incident management program framework. So I came on doing heavy technical writing, and research, and development of those sort of frameworks so that we could, essentially, create program workshops, and go in and help people develop those specific program frameworks into workshops, so that we could build out their programs internally.

MacKenzie Brown: So that's probably a really confusing way to go about it. But I started off in R&D, and then I actually, luckily, got transferred over to the incident response team, and I primarily do proactive incident response services. So we break it down in proactive and reactive, and I primarily do proactive, still waiting some fun, forensic projects to shadow. But the proactive side is really focused on the organization's level of preparedness and ability to navigate successfully through a cybersecurity incident or data breach.

Brian Contos: I see. Yeah.

MacKenzie Brown: And those services pretty much range from tabletop exercises, to playbook creation, to breach response plans and incident response plans, and even our newer purple-teaming service, which we call war-games, which is, like, straight out of a twisted TV show. It's, like, grown-up version Battleship, is the best way that we tend to describe it.

Brian Contos: That sounds awesome, actually. I remember the early days of war-gaming, people would just sit around a table with a whiteboard and try to figure out what they would do when an incident would happen. Then they'd write that information down, they'd put it in a red binder, and then it would go on top of the microwave in the break room. And there it sat and collected dust for years, without ever being looked at.

MacKenzie Brown: Aw. Right?

Brian Contos: So this is a nice evolution. In fact, it's interesting, I don't really want to talk about Verodin or our product or anything, but a lot of people actually use security instrumentation platforms for running through these war-games, and doing these assessments, all the way from when they hire individuals through practicing. And I just think it's such an important piece of the equation to have organizations doing these war-gaming exercises, and to your point, purple-teaming and bringing up the red and blue together. I think it's great.

MacKenzie Brown: Absolutely, yeah.

Brian Contos: Do you find that your audit and your R&D background have really helped you in sort of this proactive IR capability? Or are they just completely different from what you're doing, day-to-day?

MacKenzie Brown: A little bit of both. So, actually, my theater background definitely helps with the tabletop exercises.

Brian Contos: Hahaha.

MacKenzie Brown: So the theater side actually helps with that, as taking their worst nightmares, and being like, “Hey, this, throw in a couple... attribute a couple artifacts, and realistic targets in there," or, again, and just scare them, and be like, “This could happen. Now, how do you respond?” But—

Brian Contos: It's like you're playing cyber Dungeons & Dragons. Right?

MacKenzie Brown: Absolutely. Yeah, yeah.

Brian Contos: You went down this hall, and dragon did a DDoS attack.

MacKenzie Brown: Yeah. And I embarrassingly can say that we have played Dungeons & Dragons as a team building activity before at one of the SANS summits. But, anyways, so, yeah, I'd say the theater side. I'd say that auditing and coming from... So I came from enterprise on the state government level. So what I like about that, and how it helps me with the proactive services, is... and one of my colleagues called me this the other day, a “security therapist,” as I have this really soft spot to empathize with clients who have all these budgetary constraints, and internal politics, and culture, and things that really inhibit the ability to enhance, or even, like, have any sort of level of buy-in in a security program, let alone incident response capabilities.

MacKenzie Brown: So I think that coming from an area where it's hard enough to get someone... One time I had to write in a complete report, and I mean, like, a full project

request, with cost, which was zero, but a full report to our CTO to request them just putting the security banner on all of the computers. All of the endpoints.

Brian Contos: Wow, wow.

MacKenzie Brown: But I, just going through those sort of processes to get anything approved, I think I have a soft spot when I go in with clients and can understand why that not everybody can be at the most mature level, and have some sort of threat-hunting, or data analytics, or CTI program going on, that, realistically, a lot of people are at that reactionary state of maturity. I think coming from auditing helps empathize with that part.

Brian Contos: Yeah, I would definitely think so. I mean, look, you get to touch people, and process, and technology on the business side, on the technical side, so many facets. Obviously that's got to be very interesting for you. What's your favorite part of all this? What's the part that you always look forward to?

MacKenzie Brown: I think overall my favorite part is that every day is different. Seriously. Every project, every market vertical of whatever client I'm working with to even, like, maturity levels, they all differentiate between each other, which allows me to flex those creative muscles a little bit more. So I like that everyone's different, and sometimes I'm able to be more creative in my structure or strategy of doing these engagements and deliveries.

MacKenzie Brown: So among empathizing and having that sort of background in enterprise where I can understand those pains, I also hope that because I have those two things, I'm able to kind of help them navigate through those common challenges and obstacles a little bit better, a little easy.

Brian Contos: Yeah, that's got to be rewarding for you.

MacKenzie Brown: Yeah, it feels good.

Brian Contos: You know, when you're putting together a security team, where does IR fall in priorities for most organizations?

MacKenzie Brown: Number one! No. But-

Brian Contos: You wish! Yeah.

MacKenzie Brown: It's my job. It's number one. No, it's definitely my... not just like... I'm not in sales, and also it's just because it's my passion as being a part of my job. But I honestly believe it should fall as a top priority. The beauty behind it is the industry pushes this sadly-accurate statement that, “It's not if, but when you get breached,” and I think people are starting to adopt that mentality. And more

people, when they ask what I do for a living, have some sort of—it's usually wrong—but they have some sort of idea, based on the media, of what I do.

MacKenzie Brown: But businesses especially are starting to adopt that mentality, and so while navigating through an incident so that your response is trained enough to avoid, or at least ensure minimal damage is done, IR also has program activities and processes that take those lessons learned through those incidents, and through all that metrics gathering, and it really helps identify gaps that need to be addressed.

MacKenzie Brown: So, as far as putting together a security team, where IR should fall, it should be one of the first things that your team structure should talk about.

Brian Contos: Yeah. Prevention arguably is extremely cheap. If you can stop it before it happens, of course. Once you start to get to detection and response, it's, humans are involved, and there's process, et cetera, et cetera, which can really become more expensive. And because it's so expensive, if you don't have it honed, right, if you don't have it practiced, if you're not ready, if you got a process, again, in a red binder sitting on top of the microwave in the break room collecting dust--

MacKenzie Brown: Yeah, yeah.

Brian Contos: —it's probably going to cost you a heck of a lot more in your response process, right?

MacKenzie Brown: Absolutely. Absolutely.

Brian Contos: So--

MacKenzie Brown: And those preparedness activities, like you said, those are sometimes the most inexpensive ways to go about IR, and people don't even go through those types of exercises, or processes, to evaluate, or baseline where they're at, make sure that they're all on the same page. So, it's surprising.

Brian Contos: Yeah. I'm sure it's two groups, those that have already done it, and those that are going to be doing soon. It just seems like such a foundational piece of your security strategy.

Brian Contos: What are some of the common pain points your clients are talking about when they're putting together their IR strategies?

MacKenzie Brown: One of the biggest things I think I see, and it sounds so simple, is critical documentation. Having things documented, having your incident response plan, and your playbooks, all of your policies, any sort of things that revolve around ...

people need that workflow, right? They need to visually see that step-by-step, and then have it documented so that it can be enforced, and you can be held accountable for specific roles. That is a big pain point.

MacKenzie Brown: And it doesn't even take necessarily a lot of money to invest into getting documentation done. But it does take people resources, and it takes time, which, of course, equates to money overall. But having people to sit down and just pick off those low-hanging fruits, it serves to be the most impactful, I think, in the overall strategy.

MacKenzie Brown: And then, I guess, another pain point would be with some level of forensics. And I'm not saying any business can employ the ability to do their own malware or log analysis, but, at minimum, should have some imaging or capturing tools available, secure location for storage, basic preservation things that support chain of custody. That's a pain point too, that we see a lot.

Brian Contos: So you mentioned something that I think is important to most of our listeners, which is budget. Most organizations have finite funds. If somebody wants to put together an IR program, but they're cash-strapped at this moment, but they want to do something, they want to get the ball rolling, what are your top three things that they should invest in?

MacKenzie Brown: Again, I'm not in sales, but I think one of the top things is definitely finding a partner. I mean, at bare minimum, you should have a Plan B. When you can't entrust that your IR processes are going to save the day, or ensure that minimal damage, you should have a retainer in place with some sort of third-party managed service provider, such as Optiv.

MacKenzie Brown: But any sort of third-party service provider that can come in and either bring the tools or expertise to help you navigate through an incident. I think that's one of the top things that people should invest in if they don't have some extravagant budget for IR.

MacKenzie Brown: And then probably people. You want to invest and hire in your workforce, that owns that program. Having a designated role is extremely important, that can facilitate all of those proactive activities, but also be in charge of the actual incident response handling, and be the commander behind it. I think that's something that everyone should invest in at minimum.

Brian Contos: I really like how the first one you brought up was partner. And I know you're not doing a sales pitch, or pitching Optiv or anything, but at the end of the day, there's many organizations that just don't have that DNA on their team. Or maybe they do, but they don't have it at a level that they need. And I always find with a trusted advisor that you're able to really get those lessons learned.

MacKenzie Brown: Yeah.

Brian Contos: And how are other companies successful, but, equally important, how have other companies failed, and what are some of the pitfalls that you can avoid, especially early on when you're building out these programs?

MacKenzie Brown: Right? Or even when everything hits the fan, right? You're in the middle of something completely unexpected, or some larger scale breach, your window, your time of window is very short, and very small, and so it's good to have that red button, that says, “Do not press,” but you can press, and call that partner.

Brian Contos: That's right.

MacKenzie Brown: I think it's vastly important.

Brian Contos: Absolutely. How do businesses really quantify the value of IR, when they're talking to their management, and they're trying to get future buy-in, where does sort of the “rubber hit the road” in terms of quantification?

MacKenzie Brown: So people always want to know, how do I sell this to my boss? They sign the checks, but may not fully understand the purpose behind incident response, and that's completely fine. And I have my good friend, Dawn-Marie Hutchinson, coined, she's with Optiv as well, that you need to develop that server room-to-board room translation ability.

MacKenzie Brown: So the things you want to translate are those direct costs that they understand, as far as those key identifiers, type of attack and industry, total records lost, how to quantify costs to that. Notification costs, legal communications. Your technical people, all the rates behind those. Your insurance protection. Mitigation strategies once ... basically to put in those controls after an incident, so that it doesn't happen again. Usually you can tie a dollar value to all those items.

MacKenzie Brown: But it's really hard to quantify. I think the most important thing is to reiterate to your board that the thing that should scare them the most is the thing that you can't tie a dollar amount to, which is your reputation. The potential customer and regulatory impact that can be had during a live incident often supersedes that quantified value of IR. But that's how I would sell it.

Brian Contos: Yeah. Yeah, I've seen so many organizations that, when they initially start putting these numbers together, they forgot legal costs, potentially class-action lawsuits, PR firms, what they're going to have to do for brand damage.

MacKenzie Brown: Right?

Brian Contos: I mean, there's so many of these things besides, “I guess we have rebuild the service, and buy credit card monitoring service 5000 customers now.” It goes so far beyond that.

MacKenzie Brown: Yeah. And I keep seeing it's getting more expanded, too, as far as those, not just insurance, cyber insurance of course, but also people are investing in PR firms. They're having retainers with these outside firms to have them on-hand, as well. So it's very instantaneous backup plans to make sure that things go quick and effectively, and done right. So.

Brian Contos: Yeah, yeah. All the way down to having your executives, your CEOs, being coached on how to deal with the media during these crisis situations for these very high-profile organizations. So, yeah, it can be very expensive.

Brian Contos: So, MacKenzie, let's switch gears a little bit. I know you're also involved with some organizations outside of Optiv, specifically The Ms. Greyhat Organization. I was hoping you could tell our listeners a little bit about what this organization does.

MacKenzie Brown: So The Ms. Greyhat Org, I guess, it's my non-profit endeavor here in Idaho, and it's very ad-hoc. We have a three-person team. Very small. We're all in cybersecurity. But when I started it solo, I was facing a lot of challenges, and not, like, discrimination-wise, but I was just facing a lot of culture things, within transferring over from the public to private sector, that not just being a young female, but just being a female in the industry, was sort of revealing to me.

MacKenzie Brown: And we have there's a lot of really great other non-profits out there focused on women, but the thing about Ms. Greyhat that I wanted to make different was, why are we having this household name of cybersecurity not being educated to the entire society, including children, as well? And why are we facing some of the problems like 11% to 14% women in the industry? Or just 25% women in technology alone.

MacKenzie Brown: Then a shortage of those women being on the C-suite level or cybersecurity. Why are we seeing these number, not just from a diversity standpoint, but in general, struggling to build a workforce and create that talent pipeline in our industry?

MacKenzie Brown: And so, we focus on a couple things. We focus on the empowerment of women, of course. But as a whole we focus on the culture, and how cybersecurity is taught. So myself and my co-chair, Shawna, who's a cybersecurity manager here in Idaho, also. We want to focus all of our projects, and we have been focusing on education. And we're helping build out the cybersecurity curriculum, so that we can start integrating it into the public school systems, and get everywhere from third-graders, to middle-schoolers, to high-schoolers, if we start

integrating these topics, and these lessons at a younger age, not only are we hoping it's going to have that trickle-down effect, with everyday, common activities that people at home experience, whether they're being phishing, or scammed on Facebook, or there're elderly people being called and exploited for money.

MacKenzie Brown: Essentially, we're hoping that outside of that trickle-down effect we can inspire kids to have a different viewpoint of the industry, including girls, and when young girls are being educated in high school, essentially the same thing, that a security analyst making 80K a year understands. To me, I think that's the biggest impact.

MacKenzie Brown: So The Ms. Greyhat Org is really focused on transforming the culture behind cybersecurity. We want to differentiate ourselves from other groups, because we're hoping that we can fix those fundamental issues at younger ages.

Brian Contos: Yeah, I think that's such a noble, and much needed cause. In Silicon Valley, there's so many opportunities that I see a lot of young children, both boys and girls, taking advantage of, whether it's learning Python, or Pygame, or GPIO, or—

MacKenzie Brown: Yeah!

Brian Contos: —another program in robotics. I mean, it's great, but let's be honest, it's a lot cooler if they go, "Hey, I'm going to learn about security, and how to hack, or how to defend." It just has a certain feel and flow that just piques their interest.

MacKenzie Brown: It's cool to us, Brian. It's cool to us.

Brian Contos: Yeah. Right?

MacKenzie Brown: I feel like there's... We have Code.org, and a lot of code camps going on here locally too, but and we've gotten... My boyfriend's son is in some coding classes and stuff, too, and he's ten. And so but we see Scratch, and we see these things, but all I want to do is be like, “Well, what about cybersecurity? You could learn a lot. It's a lot of fun.” But, alas.

Brian Contos: Alas, we're the people that are playing Dungeons & Dragons at SANS.

MacKenzie Brown: Yeah, no kidding. Yeah, and that is where you'll end up. Welcome.

Brian Contos: That's right.

MacKenzie Brown: No, I think it's important too, but my co-chair and I, we try to get it out there more. And I'm not saying because we're, like, normal people, because I'm very not normal. But we try to get out and speak to... We did a workshop, we did a threat-modeling workshop, at this SheTech conference here locally, and it was the most fun, because I had 15 high school girls in a room, and I'm like, “All right. How I can relate to them?” They're doing the snap of the chatting, and the tweeting, and all the stuff that, even me, as a millennial, I am not in that zone as they are now.

MacKenzie Brown: So, of course, a lot of the girls, though, where interested in the workshop are like, “We want to be hackers,” and... You know?

Brian Contos: Of course they do. Yeah.

MacKenzie Brown: I'm like, “But be the good guys. Good hackers.”

Brian Contos: Read TCP/IP Illustrated Volume 1-

MacKenzie Brown: Right.

Brian Contos: And then come back to me, and tell me if you still want to do it.

MacKenzie Brown: Yeah. No kidding, right? Yeah.

Brian Contos: So, MacKenzie, as we wrap up here, a final question I like to ask everyone that's on the show, who's your favorite superhero, or supervillain, and why?

MacKenzie Brown: Okay. So I kind of went with the super villain, but she is kind of the anti-heroine. It's Catwoman. And not just because I'm, like, a cat lady at heart. I love cats, and cats on the internet, and all that things. But the reason I chose her is, well, for a couple things.

MacKenzie Brown: She is the femme fatale of Batman, where they have this love-hate relationship, that still kind of allows him to see through her crimes, and never really lock her up, because she seems to keep getting out. And I like the fact that she's wild at heart. And but my favorite part is she does a lot of the wrong things for good reasons, so rather than most villains have this traumatic event that leads to their nefarious lifestyle, she came from the streets, and her moral code is ambiguous, and she may be stealing jewels one day, but she's also beating thieves in an alley the next.

MacKenzie Brown: So I really like Catwoman. She seems to be relatable, or realistic, where at least there's this hope that even bad guys can be good.

Brian Contos: I love it because she's... I think the modern interpretation of Catwoman, as well, is one that's kind of has that hacker mentality, right?

MacKenzie Brown: Yeah.

Brian Contos: I mean it's just something that kind of follows that, “I'm doing the wrong things, but for the right reason,” maybe? So I guess it all kind of fits into that situation. No, that's a great one. I appreciate that. Thanks for sharing.

Brian Contos: So, MacKenzie, thanks so much for joining us. And, again, thanks to all our listeners for listening to another episode of the Cybersecurity Effectiveness podcast, sponsored by Verodin.