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.

I’m your host, Brian Contos, and we’ve got a really special guest today. Joining me is Helen Patton. Welcome to the podcast, Helen. Say, Helen, before we get going, maybe you could give our listeners a little bit of background about you and the path that you took to become a CISO.

Sure. So, I moved from Australia – note the accent – about 25 years ago, and that means, when I came to the United States, we were sort of in the early ‘90s, and security was not anywhere on my radar as a potential career choice at all because I don’t think it was on very many people’s radar as a career choice. And I accidentally got involved in working with database management and Windows 311 networks and Windows 95 clients, probably because, at the time, I think I was the only person in the office under the age of 25, and they thought that would be a really good thing for me to know.

"We'll let Helen do it."

Yeah, "We'll let Helen. She must know something about this. She's a youngin'." Yeah, so I got picked up by this company to really start helping people understand what computers were and how they work in the workforce and all of those kinds of things.

And then move forward about 10 years, we were starting to deal with things like the ILOVEYOU virus and things of that nature, and it was dawning on my bosses that they needed to be thinking about business continuity, disaster recovery. And around that Y2K sort of time, I was working for a company that was really severely impacted by the Northeast power outage, which you may remember took out power from Detroit through to Boston for about two weeks.

Yeah, sure.

Yeah, so at that point, my CIO who I was reporting to at the time said, "We need someone who can do a security plan, and, Helen, you’re it." So a lot of on-the-job training in my career of learning what security was and how that worked. Somewhere along the line, I parlayed that into going to work for a Wall Street bank for about a decade, doing security and risk and those kinds of things. And
then, for the last five years, I've been here at Ohio State, being the CISO in higher education, which is a trip, and I'm really enjoying it.

Brian Contos: Yeah, it's really interesting to me, when we first started talking, and you shared some of your experiences as a CISO, and you've done the private sector and now the academic world as well. Across those boundaries, what are some of the core skills CISOs actually need in the workforce to be successful?

Helen Patton: Sure. I don't think that the industry as a whole has decided what we need. I think people will tell you what we need based on their background and their experiences, which is completely fine. But I don't think there's a common understanding of it yet, which is what's making workforce development so tremendously hard for us right now. So, for my friends who come out of a very technical background and dare I say maybe a three-letter agency or a government entity kind of background, they're definitely looking for people with skills that are grounded in technology, usually network system administration kinds of skills. There is this sort of common understanding, if you can't explain all layers of the technology stack, you have no good business being in security at all. So there's sort of that camp.

Helen Patton: There are CISOs who really want people who can communicate and are willing to hire people with limited technology skills, as long as they can really communicate very well and translate technology into business practice and so forth. So there's definitely that sort of risk management governance side of the house.

Helen Patton: I think, for CISOs themselves, we're in a little bit of a different place than we were maybe five or 10 years ago. Five or 10 years ago, when I was interviewing for security roles, people definitely saw it as a technology problem with a technology skillset requirement. I think we're getting to the point now where it's pretty obvious to everybody that, while security teams need to have technology skills, CISOs themselves need to have a background and an understanding of technology, but those are not the skills they use on a day-to-day basis.

Helen Patton: So the role itself as a CISO is morphing, and as a result, I think what we expect out of our workforces is starting to change a little bit too.

Brian Contos: Yeah, I think that's a very succinct way of saying it. Talking with CISOs all over the world and seeing how it's been evolving, really it becomes a story of business risk and mitigating business risk, and cyber's just one of those flavors that has to be addressed. So I think you're absolutely right. It's becoming more of a... in some cases, it already has. In some cases, it's maturing, but we're definitely seeing it being just like the Chief Risk Officer, the Chief Financial Officer, the Chief Revenue Officer. These are strategic executive leadership roles...
that have a say in the business mission itself, not just "I stopped WannaCry" or "I make sure we’re patched," that sort of thing.

Helen Patton: Absolutely. I think the other thing too is, especially if you're dealing in a public sector or you're a company that's owned by shareholders and a board, the people who are making decisions about risk and about funding and about risk priorities typically don't have any kind of security background, even now. Our MBA programs have for decades talked about finance and accounting and organizational structure and strategy and all of those really good MBA kinds of subjects, but they're still not talking about cyber.

Helen Patton: So, when we're trying to move a program forward, we're talking with people who, one, don't know what the underlying issues are, and then two, don't know how to put that in comparison to other business risks that they face. And so, if we can't develop skills as security professionals to be able to sit in those conversations and have meaningful conversations with those kinds of people, then our programs fail.

Brian Contos: And, Helen, you're in a unique position where you have done all these different roles and currently in the academic world. How are community colleges and universities and other sort of formal education institutions, how are they aligned or perhaps even not aligned with producing the right type of cyber-skilled workers?

Helen Patton: You know, there's a lot of work happening in higher education related to cyber. There's a ton of activity, and just going out and googling cyber programs, you're going to see a lot in the United States and elsewhere that are different programs. And sometimes it can be a little confusing to try and work out which programs are the right programs and which programs make sense.

Helen Patton: So I'm going to overly generalize, and I'm going to be overly simplified here, but in general, community colleges are going to produce workers who have a two-year degree or maybe even a certificate program that really talk about currently needed skills and usually junior resource skills. So they're going to come in and talk about ... they're going to train workers to do things like be SOC analysts. They're going to train people to maybe be security engineers where they're coming in at a junior level and supporting a data-loss prevention program or a vulnerability management program or those kinds of things. And that's super important because we need lots of people in that space.

Helen Patton: What community colleges are typically not focusing on, it's not that they don't do it at all, but they're not focusing on it, is any kind of deep analytics, any kind of research-based security skills. So, for those kinds of skills, you're going to want to go to a four-year program. And in those kinds of programs, if it's a program that's based in a computer science or an engineering department,
you’re going to go very deep on the technical background related to cyber. So you’re going to get into encryption algorithms. You’re going to get into malware analysis and reverse engineering and that kind of stuff, which is awesome.

Helen Patton: So, you come out of that program with a lot of theoretical knowledge about that stuff, but probably not a lot of practical experience. So four-year colleges are starting to think about how do they partner with companies and other areas to provide on-the-ground, practical experience for their undergraduate students? But they haven't incorporated that practical experience necessarily into their curriculum yet. It's something that's done as an additional activity by the student, if the student wants to take it on.

Helen Patton: So, community colleges and four-year colleges are really performing two different services for the cyber community and for the business community in general, but they're not quite hitting the mark yet because the industry as a whole hasn't formalized yet to say what it needs. It's very easy to know how to train... here I generalize again. It's comparatively easy to train people to be accountants or lawyers or doctors because there is a professional code of practice around that work. We know what's in that discipline. It's very clear what's not in that discipline.

Helen Patton: In the security space, we haven't worked it out. We don't know if identity management is part of security or if it's part of IT or if it's part of business operations. And there isn't an understood construct of what functions really should sit in a security team and what doesn't. That makes it really hard for our academics to then define and design coursework that CISOs really resonate with.

Helen Patton: There's a lot going on. The other thing is colleges, two-year and four-year colleges can't onboard students fast enough for the industry. So there is definitely unmet demand in terms of training. The official training institutions can't address just because of capacity and scalability issues.

Brian Contos: Yeah. Yeah, you know, if there was ever an industry that needed a rich internship type program or something similar to that to get people involved. I remember when I was in college, for our database classes, we all used Cybase.

Helen Patton: Sure.

Brian Contos: And we used Cybase because it was donated to the college. They said, "Here's a bunch of free Cybase," and we ran it all on Sun Solaris systems because Sun had donated all these systems, which was fine, but it meant that you had a whole bunch of students graduating from college that really knew Sun and Solaris operating systems, and they really knew Cybase, and maybe they could
translate that to Oracle or other things later on. Who knows? But it was almost like it was vendor-driven, right, in terms of the layout.

Brian Contos: So something for us to be aware of as we go forward. We don't just need people knowing product A and product B. The theory's important, but as well as that hands-on bit.

Helen Patton: Yeah, which brings up sort of two points I'd want to make clear. One is that we've got a supply side problem in higher ed in that we don't yet have enough people who know security who are teaching. This is not a higher ed issue either, by the way. This is also a K-12 issue.

Helen Patton: So some of the mismatch in demand and supply is that we don't have enough professors and so forth who can design an entire curriculum and then deliver that curriculum. So universities and community colleges and so forth, they're really working hard to bring that up as well, but we're not there yet.

Helen Patton: I think the other thing is universities and community colleges are starting to do a better job of industry partnerships, but they also have to be very careful that they aren't, to your point, endorsing one product or another. So we're looking for people to be really creative in thinking about, okay, if there is vendor A who it would certainly make sense for vendor A to do some kind of ... maybe endow a chair, for example, in higher ed, how do they do that without locking in the curriculum to just that vendor, which we don't really have a sense of how long technologies are going to be meaningful for because the technology environment that we're in is changing so fast. So how to have a public and private partnership around education is still something that we're working out as well.

Brian Contos: Yeah. Somebody actually mentioned to me the other day, if you're doing something in the workforce the way that you learned it in college, you're probably doing it in a very outdated way, just because everything changes so quick.

Helen Patton: Yeah.

Brian Contos: You mentioned K-12. I wonder if you could touch on that a bit more. What's happening at the K-12 level? Are you seeing cybersecurity being introduced to young people?

Helen Patton: Not as part of the curriculum very often. What's happening in K-12 is a lot of computer science kinds of constructs. We're seeing a big effort to push middle school and high schoolers to code, lots of work around robotics programs, for example, to introduce them to engineering concepts. But those things are not
necessarily focused on security, and it's very hit and miss as to whether security concepts are included in those curricula.

Helen Patton: So again we've got a little bit of a supply problem in that K-12 teachers need to be trained on how to think about security and how to incorporate that into their pedagogy. So one of the exciting things about K-12 though is I think there's a bigger understanding that, if we're going to introduce diversity into our workforce, that we have to be very targeted in middle school or earlier to diverse populations and not wait until they get into high school because, by the time they get into high school, diverse populations have already decided that they can't see themselves in the security community or the tech community because they don't.

Helen Patton: So I think the good news is we're starting earlier and earlier to introduce technology to diverse populations, and that's really exciting, but it's just tech. It's not security just yet. We're getting there, but it's pretty nascent still.

Brian Contos: Yeah, I would agree with that. I've mentioned on other podcasts I have two daughters that are in middle school, and they do after-school programs. They're learning Python and robotics and GPIO, and they do competitions like RoboRAVE. There's a good mix of kids that participate in that. I would say it's probably still, if we look at diversity, probably less than 5% female in those groups.

Helen Patton: Sure.

Brian Contos: And this is in Silicon Valley Proper, where you think you'd probably get a larger set, so it's interesting to see that that's still the case. But what I've been told is, as much as just a few years ago, it was almost zero.

Helen Patton: Right.

Brian Contos: In terms of having females, so I guess progress is being made, perhaps not at the rate we'd like to see it, but I guess change doesn't just happen overnight.

Helen Patton: Nope.

Brian Contos: I wonder if we could talk a little bit about, from a student's perspective, what are college students looking for in terms of internships and co-ops and other sort of on-the-job programs? Are you hearing students actually approaching the faculty? "Hey, we'd really like it if you could provide these types of services for us."

Helen Patton: Yeah, absolutely. Students, particularly college students, are getting the message that security is a career of the future. It has legs. It's not something
that they would study for four years, and then eight years from now it be taken over by robots. There is a career security in security, which is really great.

Helen Patton: But they also don't fully understand all the opportunities that are available in the security profession. They tend to approach people like me or other instructors with a sense of "I'd like to get a job, and it looks something like a SOC analyst or more of an engineering kind of job or maybe some level of sort of risk and auditing."

Helen Patton: When they're going for an internship or a cooperative program, they're looking for an opportunity to get exposure to the entire breadth of the security profession. So they don't want to come in and do an internship where they're doing the same thing for the entire internship. Even if it's only a summer internship, they would like the opportunity to try two or three or four different security sub-disciplines in the course of that time so that they can expand their thinking, and they can get a better understanding of really what the opportunities are.

Helen Patton: The other thing they're looking for is, even at the internship level, they want to be working on something that, at the end of the internship, they can put it on their resume as a thing that they have done that has added value. So it's not simply enough to say, "I had an internship with Company X, and I spent 12 weeks with Company X, and at the end of it, I can tell you that I spent 12 weeks with Company X." They want to say, "While I was there, I did this project, and in this project, we improved the security profile of the organization." Or "I learned a ton about ethics and how security fits into that" or "I came up with this great app that I'm going to be able to now go and market and start my own company on." They want that kind of thing to take away from the internship that they can then turn that into something that takes them on to the next thing.

Helen Patton: So, when it comes to being an employer who's thinking about taking on an intern, it's not just about exposing them to security stuff. It's about having them really get their hands wrapped around it and feeling like they're owning it. And that can be super challenging for employers to do.

Brian Contos: Yeah, I remember one of my first cybersecurity-related internships when I was in college was called UMAP: the Unauthorized Modem Abatement Project. My job was to go in and try to find all the modems that were deployed, and at that time there was a lot. This was in the mid-'90s, and there were just modems connected everywhere for vendor support and this and that.

Brian Contos: So there was a tool, a piece of software called ToneLoc that ran under DOS actually. It was basically a war dialer. Well, it was a war dialer.

Helen Patton: Yeah, right on.
Brian Contos: So I just was dialed the entire phone number bank of the company, which not everybody liked for me to do that.

Helen Patton: Yep.

Brian Contos: But yeah, it's getting your hands dirty. Like you said at the very beginning of the podcast, there's so many areas, and you could be super technical and find a great job in cyber, and you could be really not super technical at all and still find a great job in cyber because of all the roles. I think that's what's important.

Brian Contos: We've talked about educational institutions. We've talked about the students. Let's talk about the companies a little bit. What are companies doing to grow their cyber workforce in the face of this supply shortage, if you will?

Helen Patton: Sure. So there's sort of two things that I'm seeing companies do. The first is to think about how to get more people in, I will say, at the bottom of the industry sort of our young people into cyber. So I'm seeing companies, and I'm sure you've seen these things online, they're doing things like sponsoring Girl Scout badges. They are sending their employees into K-12 schools to talk about cyber.

Helen Patton: They are also partnering with community colleges. One of the things I'm starting to see is, particularly at the community college level, the community colleges willing to make a cyber curriculum specifically for a company, that the company can then send their employees to get them introduced to cyber concepts and so forth.

Brian Contos: Oh, that's an awesome idea.

Helen Patton: Yeah. And it's sort of a win-win, right? And it applies largely to mid-size or larger companies, but they get to set what their skill needs are, and then the community college gets to develop that and then leverage that knowledge for what they are then teaching other students as well, which is really great.

Brian Contos: Let's say I'm a CISO.

Helen Patton: Yeah.

Brian Contos: And I wanted to start up one of these partnerships with a college, university, what have you. What's the best way to approach that? Where do I even begin for that type of thing? Because it sounds like a fantastic idea.

Helen Patton: So most institutions will have an industry outreach office included in their administration somewhere, so you can certainly start there and just go in and find some time to meet with someone, say, "This is what we're looking for, and
this is how we might want to partner with you in terms of funding or in terms of scholarships or in terms of whatever to make this happen."

Helen Patton: So industry liaison officers is definitely a place to go. You can certainly reach out ... if the college already has a cyber program, usually they’re advertising it online, and usually all the contact information for the program and the instructors and the administrators who run those programs are available online. You can cold-call people like that, and they will also help you out.

Helen Patton: And then the third option is go to people like me, who are the security people at the organization and establish a partnership with that individual, and then from there work out with some insider knowledge where it might make most sense to engage with the academic side of the school. So there’s a number of different ways that people can go in and do that.

Helen Patton: I will tell you that I think that most of the schools, to be on the receiving side of this, would want to say how do they create a long-term partnership with a company? And that can be, well, yeah, okay, there’s some kind of financial exchange for this partnership. It can be "We’re interested in making higher education affordable for our students, so let’s talk about some kind of scholarship program in exchange for this kind of partnership." There are all kinds of really... you can get as creative as you want, and I’m sure you will find people in higher institutions who are willing to discuss that option with you. Lots going on.

Brian Contos: Yeah, lots going on, a lot of opportunities and angles you can go. Thank you so much for sharing that because I truly believe that that’s going to be an important go-forward strategy as we’re trying to fill this supply gap we have.

Helen Patton: Sure.

Brian Contos: So, Helen, as we wrap up here, I have a very important question that we ask all of our guests on the show, and that’s who’s your favorite superhero or super-villain and why?

Helen Patton: I think I would tell you that Jack Nicholson's Joker in "Batman" was probably my favorite super-villain.

Brian Contos: Classic, classic choice absolutely.

Helen Patton: Only because he just ... well, one, I really like the makeup, and two, he just didn't take himself seriously at all, and I appreciate that. I think the other thing as a CISO that resonates with me is that our adversaries are definitely a pain in our anatomical region, but they are also super smart, and, in some ways, you
admire them because they are super smart, and they're super clever. I think that Joker character really embodied that for me.

Brian Contos: I love it. I love it. And we'll see how Joaquin Phoenix does it now. I know they're coming out with a new Joker-based film, so that will be interesting.

Helen Patton: Yeah. You know, I think Heath Ledger may have probably culturally sort of won the Joker wars, but we'll see.

Brian Contos: Yeah, yeah. It's hard not to think of Heath Ledger, that's for sure. Well, thank you, Helen. Again, thanks to all our listeners for joining. And be sure to check out other Cybersecurity Effectiveness Podcasts, sponsored by Verodin.