Barclay Damon Live Presents: The Cyber Sip Podcast

Episode 15: "Vetting Vendors and the Culture of Compliance, With Drew McNichol"

Speakers: Kevin Szczepanski, Barclay Damon and Drew McNichol, Director of Technology and Security Officer, HEALTHeLINK

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

[Kevin]: Hey everyone, welcome back to Cyber Sip. In this episode, we are pleased to welcome back Drew McNichol, director of technology and security officer for HEALTHeLINK, the Western New York Health Information Exchange that is part of the statewide health information network for New York. Drew, welcome back.

[Drew McNichol]: Hey, thanks for having me back, Kevin. Glad to be here.

[Kevin]: Oh, we're glad to have you back. And Drew, I want to start with your titles and talk about those because you are both the director of technology, which strikes me as an IT function, and the security officer for HEALTHeLINK. Talk to me about the difference between IT and information security. I think a lot of people think it's the same thing, but really they are overlapping perhaps, but two very different disciplines.

[Drew]: Yeah, you make a good point, as far as the overlapping, they are technically different. I wear both hats for HEALTHeLINK. We're a smaller organization, but as you mentioned, director of technology, that's more on the IT side. So it's your traditional, you know, making sure that the technology is in line with the business objectives. You're running the day-to-day operations of the systems, making sure you have what you need to be operational. But when you look at the cyber side of things, many of us think and many folks think that it's really just an extension of IT. So if you're a technology geek, you must be good at security as well, and why don't you just go solve that for everybody? And what we're finding is that you need to broaden you know, you really need to broaden the exposure. It's not just the technology folks. You do need to have an underpinning of the technology, but you really have to go beyond that. And you have to look at, you know, all elements, the behavioral side, you have a workforce that's out there working and using these tools. And then there's also the side of risk management. And so the cybersecurity professional these days has to have an underpinning of technology, but be able to really talk about cybersecurity in the business language and being able to do a risk assessment and identify what risks are we facing. And this really presents itself when you need to report this out to executive leadership or to boards, that type of stuff, you have to really be able to translate the technical jargon into business terms that can then be used to help manage the risk. So that's two different hats that you wear. And then we have resources within HEALTHeLINK that focus primarily on security and resources that focus primarily on IT. So we do segregate it by resource as well.

[Kevin]: Right, now that's so critically important. And we're going to talk more about that a little bit later when we talk about creating a culture of security. But I want to ask you something about what you mentioned to me off air before we got on. And maybe someday we'll have you come back and talk about a day in the life, because I think a lot of our listeners would find it interesting to know what director of technology and security officer does from dawn to dusk, and of course, probably goes beyond dusk depending on the issue. But you mentioned that you have a security dashboard. And I found that very interesting because we talk about monitoring and logs to sort of figure out... I always analogize it to a house: figure out who's getting in, where are they going when they get in, what are they trying to access and what, if anything, are they trying to take? So can you talk to us about that security dashboard and what it enables you to do as a security officer?

[Drew]: Sure. Yeah. So, you know, essentially one of the challenges around cybersecurity is how do you measure effectiveness? You know, what are you looking at? How do you... what sort of metrics do you put in place to know what your baseline is? Are you getting better? You know, where do the threats come from, that sort of thing. And so one of the ideas in this stems back to one of the board meetings where I was giving an update. One of our stakeholders leaned over and said, you got to jazz up your slides a little bit because it was sort of this dry security line-by-line type thing. So I took that to heart and we developed a dashboard it displays on a large screen in our office, and it's also available on a website. So if you're remote or you want to check in, you're able to do that. And it really shows a world map. It shows who's trying to get at us. Where do our users come from, what things are being blocked? What is the performance of our system? It's a whole set of metrics that allow us at a glance to see that there's this whole world of cyber out there and it brings it to light. And the idea in the office is to have folks the workforce go by and see we're getting pinged from other countries trying to get in. They don't know us specifically, but they're just looking out there, trolling, to see if there's any vulnerabilities they can exploit. So part of the security program is an awareness in fostering that awareness in our employees. So one of the ways to do it is to have a dashboard that's visible that brings it to light. So that's essentially what we're trying to do. It's some of the metrics that we track, being able to be displayed in a visual, appealing manner.

[Kevin]: So you can tell to some degree from that dashboard where the bad guys are and know that they're trying to get in every day.

[Drew]: Every day, every moment of every day. We do a thing called geofencing. So we only allow access from the US and Canada. And a lot of times we need to allow Canada because that's how internet traffic routes being in Buffalo, we're so close to the Canadian border. But other countries, we will not allow traffic. So if they attempt to get us, we will block that at the firewall. But we keep statistics around that type of information. So you're right, it does at a glance show and bring to life what's happening out there.

[Kevin]: Yeah, I think we say that all the time. And I'm not sure that everyone believes us, that they are...the bad actors are trying to get into your system every few seconds of every minute, every hour, every day. And you can confirm for us that that is, in fact, the case.

[Drew]: Absolutely.

[Kevin]: So how do you then foster and let's use HEALTHeLINK as an example because you have literally millions of pieces of clinical data and you're just one of six regional HIEs in New York. There are similar set ups in other states across the country. The culture of compliance is so critically important, Drew. Talk to us about how you and HEALTHeLink go about fostering that culture of compliance across your organization.

[Drew]: Yeah, great point. In the old days, it was thought that security was one or two people's jobs. And so we continue to talk about security being everybody's job. Everybody has a role in the security. So it starts with our governance and our policies and procedures. So we have built policies and procedures that our workforce needs to follow. And that outlines very specifically what it is each of our individuals need to do.

[Kevin]: Right.

[Drew]: It even goes down to our job descriptions, governance. If you look at our job description, there are bullets in there that says these are your responsibilities around security. So although I have the title, everybody has in their job description a set of security bullets that they have to follow. We mentioned last time a lot about the certification process. I trust you to find all of that good stuff. You know, part of that, once you start putting those controls in place, everybody has a role in the controls. And so we had allocated out different procedures that people in our organization need to follow, whether that's checking the perimeter security and cameras that are in place and those types of things. So we have outlined part of people's jobs, this security mentality. When we have to implement new procedures, we have a thing called two-factor authentication. So when you log in, you also have to accept a second factor that could come on your cell phone. And it's very interesting because once you get that second factor and you accept it on your smartphone, people really got into it saying, this is my job in security. I need to press that button.

[Kevin]: Right.

[Drew]: And I know I'm helping to do security. So. So that's part of it, you know, making people part of the process. And we do a lot of awareness training. And so that's one of the things that the certifications require you to do—to bring awareness to the staff. So that could be on any variety of topics. One of the big topics in the industry these days is phishing. We've all seen it, right? We do testing around that. And so there's little competitions around. You know, we try to trick people to be really diligent about what they're reading and opening on email and they can report it and then they'll get a kudo if they reported something that was one of our phish testing. But it doesn't stop there because if you think about it now, we have something called smishing, which is SMS-phishing, right. So now they're targeting your smartphone, right, with text messaging. And so we try to, you know, keep people apprised of how the landscape is changing, what threats are out there. So we're constantly looking at that, you know, with this conflict in Russia, and there's been a lot of bulletins around cyber-attacks around what's happening. So we do education on that as well. And the other thing is we also give tips and good cyber hygiene for your home use, too, because security doesn't end when you walk out of our building now or when you're...

[Kevin]: ...working with the remote workforce.

[Drew]: Exactly.

[Kevin]: More of us are working remotely.

[Drew]: Yeah. So be careful with your home machines. Good cyber hygiene, whether it's at work or at home, really, really pays dividends. So that's how we kind of foster this culture of compliance, you know, bringing people into the fold and being able to keep them aware of the changing landscape.

[Kevin]: You know, it's interesting you mentioned the two-factor authentication. Pete Hotchkiss, who's the director of technology over here at Barclay Damon was kind enough to connect me with the FBI InfraGard presentation last week, so I did get a chance to listen. And, you know, it's amazing because you're right, smishing has become I feel like it's really heated up in the last 12 months. I'm getting texts from financial institutions I don't do business with asking me for information. That's an obvious threat actor event. But what was equally interesting to me is that you have FBI agent after agent, stakeholder after stakeholder talking about the issues. And what were they talking about? They were talking about multi-factor authentication and patch management. And I thought to myself, wow, I can't believe we're still talking about these two things in 2022. I would have thought, well, everybody knows that you have to have MFA. Everybody knows that you have to have a robust pass patch management process. But these are still significant issues out there...maybe not so much in the health care industry, but across the board it sounds like it's still a risk. So what's your take on that? Should we be farther along than we are?

[Drew]: Well, you know, one of the really interesting things is that when...we talked about the, you know, the certification around HITRUST and SOC 2s and all of these things.

[Kevin]: Yes.

[Drew]: And if you by the letter of the law, just look at the controls that outline that and you get it a SOC 2 or a HITRUST that doesn't translate necessarily to having a good information security program.

[Kevin]: Right.

[Drew]: Because you might be hard pressed to find something in a SOC 2 that says you have to have multi-factor authentication. They talked to you about what it is you need to do, not necessarily how...

[Kevin]: How.

[Drew]: So the way. So a lot of organizations might bank on the fact that they have a certification and that's their substitute for a good information security program. We, on the other hand, had built a very secure information security program, and then we had that certified. So there's things that we do, such as multi-factor authentication, such as tracking a metric. Are all your machines patched on a regular basis, and can you validate and provide evidence of that? That might not be explicitly described in one of the audits, but it's good hygiene to be able to do that and also have it part of your information security program. So I think my view on it is, you know, those organizations haven't yet matured into a robust program that is, you know, up to date on where they need to be and then looking to the future to say, what should we be entertaining going forward.

[Kevin]: Right, it sounds like what you're saying is that the certification is not the be all and the end all. The certification reflects—or should reflect—the robust cybersecurity plan that you already have in place.

[Drew]: That is correct. That is correct.

[Kevin]: So we talked a little bit about creating a culture of compliance within the organization. Let's talk about outside the organization because HEALTHeLINK, I think is a vendor, but also has vendors. So, Drew, how do you go about ensuring, I suppose, prequalifying vendors and ensuring that your vendors have appropriate safeguards in place for what you need as an organization?

[Drew]: Yeah, great point. We do, even though we're a small organization, we have many, many vendors that we do business with—larger vendors and smaller vendors. And so we'll start with putting them through their paces from a security assessment standpoint. One of the processes that we have is onboarding a vendor, Kevin, to say, okay, this is a new vendor. There's a lot of financial things that you do to onboard a vendor, but there are now cyber and technology, things that you do to onboard a vendor, right? And so we ask things like, do you have a HITRUST report? Can we review it? Do you have any corrective action plans? And we ask them a series of questions to make sure that what they're presenting to us is compliant with what we require. And that doesn't stop there. We actually put this language into an agreement, right? Well, if I'm signing an agreement with you, you're committing to doing these things, whether it's part of a BAA—a business associates agreement—and then an addendum that says, in addition, you will do these things, right? So we build it into our agreement from day one on what the vendor needs to do. And it's not just a one and done; we'll review that on a periodic basis. So you may qualify today, but as we talked about, the landscape changes. So how are you keeping pace with what's happening out there? And we'll put the vendors through another assessment on a periodic basis to make sure they're maintaining that good cyber hygiene that we would require as one of our third parties or partners.

[Kevin]: Yeah, so it really is a three-step process. First, you're doing the assessment, second, you're building the cybersecurity into your vendor contract. And third, and probably is part of the contract, but you're doing your auditing compliance, right?

[Drew]: That's right. We're monitoring it, yes.

[Kevin]: Now, I feel like time was—and I've been part of these conversations over the years; I'm sure you have as well—you might say, an organization might say, well, we'd really like to use vendor A and it's ... It's a choice between vendor A and vendor B. Vendor B hat seems to have the more robust safeguards, but vendor A is really the all-star in this space. So we're going to just...we're going to overlook some of the issues we have with Vendor A, we're going to onboard them. But if they can't give us everything we need, we're going to let them slide because we just really need to use vendor A and vendor B is not quite as good. I feel like that has changed in the marketplace today. There is a barrier to entry that will prevent the vendor As from getting work today if they do not have the basic cyber hygiene in place.

[Drew]: Well, you're exactly right. And I call it "table stakes," right. So at these days that to be at the table, you have to have a certain level of security in place. And if you're not, you're going to be overlooked and you're not going to have a seat at the table. You know, there are some things where if there's a compelling business reason and you've done a risk assessment and the vendor says it's on our horizon to do something and it's within your timeframe and you've done a risk analysis—that might be an exception that you deal with. But, you know, any more these days it's more common—and we talk to a lot of vendors now that are saying, I need to pursue some level of certification in order to stay in the game. So, yes, that has changed.

[Kevin]: Right. So, Drew, where I see we're coming, we've almost out of time, but, I want to ask you one more question, if I may. I was looking at the HEALTHeLINK board and we were talking about this a little bit before we started. And you have a very impressive board in representing providers, payers, educators, consumer, and employer stakeholders. It is diverse and inclusive in all the right and important ways. But there are no cybersecurity experts on the board, per se. Very intelligent group of men and women, but not experts in cybersecurity. So how do you go about communicating with the board in a way that conveys the critical information, the threats, the response, the certifications, while at the same time speaking in a way that these intelligent board members can understand and digest and make the decisions that they need to make.

[Drew]: Yeah, great question. And we do have a great, diverse board. We actually have our annual board meeting tomorrow and I'll be giving an update on our information security program. So timely question. We have a set of KPIs that we provide. So, you know, business deals with KPIs. And so it's things like percentage of laptops that have been patched. What are the types of things that we're measuring? So not to spend too much time technically, but we basically show what are the KPIs that we're measuring. So it could be we talked about phishing. How many of our staff fell for a phishing test? Do we have 100% compliance or are we at 50? And then we have to take some action to raise the awareness there? Do all our machines get patched on a timely basis? That type of nuts-and-bolts type things. So we basically say, look, we have a broad set of KPIs. They should look at that and say that that feels comfortable, those are the things we measure in our industry as well, in our corporations as well. And then we talk about, you know, where are we spending the effort? How do we improve those KPIs even better? And then I'll talk about a set of tools that we've organized to say we're looking at bringing in some additional, for example, email filtering so that we can detect more phishing; so it won't come to the end user. So I talk a little bit about here's our activity for the year here. There are focus areas that we're doing and here's the areas that we want to improve. But it really goes back to explaining it in business terms and then being able to express it in terms of risk management. You know, here's the things we see. Here's where we see a risk. Here's what we're doing to prevent it.

[Kevin]: Right.

[Drew]: And the other thing I'll add. We're very, very fortunate that each of these organizations that you mentioned that are our stakeholder group, I have a security committee and we meet periodically and it's made up of their chief security officers in each of those organizations. And we come together and we work on things as a team. So when we raise the level of security for one, we raise it for all. So even though these folks are competitors in the marketplace, their security professionals work with us and we learn from them and they learn from us so that we can work together in the security area. So there's a lot of synergy there and a lot of opportunity for us to build in best practices across the health care fabric in Western New York.

[Kevin]: Right. And that's a great place to end. And I just want to ask you, before we leave one other question. So you're talking about interacting at the board level and the security committee level and having a culture of security that expands from inside the organization to outwardly to your vendors. But not every organization is as robustly focused on cybersecurity, right, there are a lot of small organizations where you may have one or two IT professionals. They may not have the same background in information security. The board may not be as engaged as the HEALTHeLINK board is. And I'm sure the boards of your many stakeholders...Drew, what advice would you give to, let's say, the IT manager of a small- or medium-size organization that is trying to develop the culture that you have and that is evolving every day. What advice would you give that person for trying to create that very same culture in an environment that may not be as open?

[Drew]: Yeah, great question. And what comes to mind immediately and I'll say this every time, conduct, you know, prepare and conduct a mini-risk assessment and this doesn't have to be multiple weeks and months, but if you work with a third-party security organization, do a broad brush and identify what do you think are the major risks? And then talk to the business in terms of "I see a risk here." This is a risk if our email were to get compromised and somebody got into our email. Here's the risk that I see, and you can do a risk assessment in two or three days at a high level. That's the kernel. That's how you get started. And that builds some interest and you talk about risk. And then that evolves over time where you say, okay, we've handled that. What's our next set of risks? So identifying the threats and the risks to the business if we don't address it, and I've seen that help get to the point where it frees up some funding for IT to start down that path. So that would be my recommendation to get started. Start with a mini-risk assessment, threat and risk assessment and go from there.

[Kevin]: With that is great advice and that is a great place to end. Drew, thank you so much for joining us once again on Cyber Sip. I hope you'll come back and talk to us again about another topic that will ...that probably doesn't exist today, but it will when we talk again.

[Drew]: No doubt. Yeah, I'd be happy to do that. And thanks for having me back.

[Kevin]: Well, thank you so much. And thanks to all of you for joining us on Cyber Sip. We're 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.

Disclaimers:

This material is for informational purposes only and does not constitute legal advice or legal opinion. No attorney-client relationship has been established or implied. Thanks for listening.

Barclay Damon Live podcast transcripts and captions are automatically generated through artificial intelligence, and the texts may not have been thoroughly reviewed. The authoritative record of Barclay Damon Live programming is the audio file.