Barclay Damon Live Presents *Cyber Sip*™ Episode 33: "Top 5 Security Controls You Need Now," With Dean Mechlowitz

Speakers: **Kevin Szczepanski**, Barclay Damon, and **Dean Mechlowitz**, TEKRiSQ

[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]: Welcome back, everyone. I'm really pleased to have Dean Mechlowitz of TEKRiSQ joining us on today's episode. Dean is the co-founder of TEKRiSQ. And Dean, just remind us a little bit about what TEKRiSQ does.

[Dean]: So TEKRiSQ looks at cyber wellness of small and medium sized businesses. So the issue that we see is that there's a cyber divide between the "haves" and the "have nots." Haves are those companies that have internal IT departments, perhaps they have chief information security officers, they have large budgets, they have people that understand cyber. And then you have the have nots. These are generally companies say, less than 200 employees. Oftentimes, they have no internal IT. Oftentimes, they have no chief information security officers. Oftentimes, they outsource IT as well. And they don't really have a lot of expertise. So what we do is we help diagnose what do they need to be doing in order to get them outside the crosshairs of the cyber criminals? What do they need to do to become insurable for cyber insurance? And if need be, what controls they need to put in place without breaking the budget, taking tons of time, requiring them to manage it. Because they just want this problem solved. They don't want a copy of "War and Peace." They don't want homework assignments. You know, their favorite thing to do is talk to a cyber person. Second favorite thing to do is talk to a lawyer. And third thing, everything to do is talk to a professional. Not. They want to run their business and they want to be pragmatic and get it done quickly.

[Kevin]: No, I think that's so important. I think today's cyber professionals would do well to appreciate that the number one priority of any business is getting the job done day to day. And data privacy is important, but it's not as important as providing the products and services that you're providing to make ends meet. So speaking of data privacy, we're sitting here and we're actually recording in the third week of January—this is Data Privacy Week. And I just want to pick on health care as an example, because I think we know that healthcare providers place a high priority on data privacy. Their patients demand it. The law demands it. We could talk about HIPAA in another episode, but I wanted to share with you a piece; it's actually a study that came out in late December 2022. It was the JAMA Health Forum and essentially took a look at ransomware attacks on healthcare providers over roughly a five-year period. January 2016 to December 2021. And I wanted to share some of this report with you and get your reaction. So we hear this year that in 2022, ransomware attacks were down, but—that may be partially true—but long term trend from 2016 through today is upward. So with that in mind, from 2016 to December 2021, there were 374 ransomware attacks on US healthcare delivery organizations exposing the PHI, protected health information of about 42 million Americans. Almost half of those ransomware attacks. This is where it gets interesting. Almost half of those attacks disrupted the delivery of healthcare with common disruptions, including electronic system downtime, cancellations of scheduled care, and this one, which is most alarming: ambulance diversion, downtime. So looking at these attacks, what the JAMA Health Forum reports and according to this study, is that these ransomware attacks expose the PHI of more patients. They were more likely to lead to reporting

requirements. So you suffered a ransomware attack, your data was accessed or exfiltrated. You were going to have to report that not only to patients but to federal and state authorities. And those attacks were alarmingly, I think, associated with delays or cancellation of scheduled care. Dean, I'm going to put you on the spot. What's your reaction to that?

[Dean]: Yeah, I'm not convinced they're going down when it's only growing by...I don't know the exact percentages, but it was only growing by 100% versus 150%. It's still really terrible. The average cost of a breach of $150 a record times some 44 million records. It's a massive problem still. So, though, I think those statistics can be somewhat misleading. The cybercriminals will use whatever mechanism they want, they need to make money. And whether it's ransomware, whether it's business email compromise, the compromise, how you transfer money within your organization, it's still a massive problem that needs to be addressed.

[Kevin]: Right. So and it's a massive problem in the health care industry, but in many other industries as well. All right. So what do we do about it? Are there security controls that every organization, whether you're healthcare, financial, professional services, are there, controls that excuse me, that every organization should be thinking about, regardless of what products or services you provide.

[Dean]: Absolutely. Great question, Kevin. So probably the best way to do this is just give some examples, because the challenge is a lot of employees, a lot of businesses don't understand their exact risk. So we need to understand what those risks are. Remember, these companies don't have unlimited budgets. The enemy of good is perfect. They need to put stuff in place and it has to be fit for purpose because you're not... a $1 billion hospital organization is not going to have the same controls as a 50-person local physician's office. So that's super important.

[Kevin]: Good point.

[Dean]: So just by way of example, so one of the some of the challenges are that we have a workforce that's working remotely. Obviously, doctors don't want to be working remotely or maybe they are actually, there's telemedicine. So there's a lot of remote working and a lot of folks don't understand the problems of working remotely. In the past, we've been protected by, behind these large corporate firewalls that prevent that data from getting into the computers. Now, imagine, Kevin, if I ask you, how is your home network configured? You're like what?

[Kevin]: I have no idea.

[Dean]: Right. And you're working out of the local coffee shop. Is that wifi secure, or is there a cyber criminal with a row hotspot sitting this backpack next to you or you're working out of the hotel or or, you know, any place where there's wifi, how do you know it's safe? So VPNs are absolutely required to protect that data. So by way of example, this just happened a few weeks ago. A person connected via their phone to a hotspot in a hotel, they access their Coinbase account, they enter their password. The MFA, the multifactor authentication challenge came back, so they entered the six numbers that get texted back to you. Now the criminal has the password and the MFA code. So now they have the access token. They're in that system in 30 seconds, and they transfer $400,000 out of that in 10 to 30 minutes, 10 to 20 minutes. So folks don't understand that even when you're working anywhere, you need to be using a VPN. It's pretty simple. So, you know, when we talk about these controls, it's not nation state hacking that's causing these problems. Yeah, okay. That can be it. But it's the simpler. Yeah, it just be as simple as the hacker going to the local coffee shop outside of a corporate headquarters in the lobby and just waiting for people to give them the information. Yeah, that's true.

[Kevin]: All right. No, that's a great example. So you're remote working, you've got to be entering your system through a VPN portal. Otherwise you're putting yourself at risk. What other kinds of security controls should we all be thinking about today, Dean?

[Dean]: I'll try not to get too techie, but there's a lot of misconceptions.

[Kevin]: Yeah, you can get too techie, if you will.

[Dean]: So Macs, when you talk to the people who say, you know, my Mac is immune to viruses. Absolutely not.

[Kevin]: That's what they say.

[Dean]: Absolutely. We find when we look at employees in a company, if they have Macs, 90% of the employees have no antivirus protection at all. 90%. When you look at the PC users, we find that the antivirus protections they're using, they don't update them. There's like 20 to 25% that don't update them properly or they're using whatever comes free on the machine, like Windows Defender. To top it all off, they're not using any virus, to top it all off, standard antivirus, which are no longer sufficient. They rely on you to download what they call signature. So if there's a virus, what does that look like, detect it? The challenge with that, of course, if that there's a new virus that hasn't been characterized yet it will miss it. So insurance companies, now, all the cyber insurance companies as a prerequisite, are requiring what we call endpoint detection response. Think about that is antivirus on steroids doesn't require employee interaction. It's a piece of software that's malware or a Trojan or a virus is trying to access sensitive areas of the computer. He'll stop in his tracks. So EDR is an absolute requirement on your computers for running a business; not only to protect you, but it's also a prerequisite to get cyber nowadays.

[Kevin]: Can I just stop you there? I'm glad you mentioned EDR, because I wanted to ask you about that. And here's how I think of it. Tell me if I'm close. I think of it like my home and making sure that at every door, at every window, and every means of ingress, there is a guard standing there letting me know who's trying to get in and how they're trying to get in, when they're trying to get in. And then further... even inside the home. At every door, every entryway, every kitchen cabinet, every drawer, there's someone standing by letting me know whether someone's trying to get in. Who it is, how they're trying. And in every case, those threats are raised to the level of the information security team. And if possible, they're neutralized. Is that a is that a good metaphor to think about EDR?

[Dean]: It's great—as well as if that person is going into a room they're not supposed to be in. Once they're in your house, he'll say, well, wait a minute, they're in this room. They're not supposed to be even in there. So I'll stop that. So great, metaphor?

[Kevin]: So even if I'm in... and so we're mixing metaphors, but even if I'm it's my house. If there's a room I'm not supposed to go in. I'm not supposed to go in my teenage daughter's room. And even though I own the house and that's my daughter, I'm if...I get to the door and I'm ready to, you know, I try to enter, the red flag is going to go off so people know, oh, Dad's trying to get into my room. That's not supposed to happen.

[Dean]: Absolutely perfect. Great analogy.

[Kevin]: And that's really...it leads me to the concept of zero trust architecture. That's really a form of zero trust, isn't it? I mean, we used to think of the perimeter of security being the wall between our own organization and the outside world. But increasingly, we are asked to think about zero trust architecture or a system of controls that does not assume that anyone, including your own employees, is trustworthy unless they demonstrate that they are. Can you walk us through that? And what do you think of "zero trust"?

[Dean]: Yeah. So absolutely right. So think of it as layers. There's layers of security we just talked about. That's one piece of it. But also think of some of the recent breaches that happened like LastPass it's a password vault. So password vaults have the keys to the kingdom. They have all the passwords. They get into your systems. But what they've done is a zero trust architecture is that nobody can get into those vaults, even if

you get into their organization. So another layer of protection is there because that first layer could break down for whatever reason. So you need another layer, and another layer, and a layer after that to fully protect yourself. And you can't trust anybody, not because they're necessarily untrustworthy people, but people click on things all the time. People do things wrong all the time. There's behaviors that aren't safe for cyber and that they're doing, and you'll never train people not to do that. It's almost impossible or it isn't possible to ensure that people aren't going to click on something accidentally and cause a problem. So you need to design your architecture, the zero trust architecture, with that in mind, that people will do things wrong all the time, either inadvertently or just out of ignorance. Every single day, time and time again.

[Kevin]: So you're protecting your organization not just from the external threat actors, but from your own employees who may make mistakes, as we all do.

[Dean]: I think when you look at cybersecurity, employee behaviors are the reason that...you look at loss ratios of the insurance companies are not really going down, even though they're putting all these things in place. They're coming up with these 20-page applications. Right. Asking more and more questions. And they're not going down. And why is that? It's because the behaviors of the people in their organization aren't matching what they're putting on the apps. Therefore, you need to have more layers of protection because things are being done incorrectly.

[Kevin]: Right. I've been thinking about that over the last couple of weeks as we've started the new year and you know that as an organization, cybersecurity, the security controls get better and better. I think the threat actors are learning from that and they're saying, well, why should I take the time and resources necessary to hack into your system when I can get you to open the door for me? And that's where the employees come in. The employees are the first line of defense, but paradoxically, the weakest link in an organization's cybersecurity these days.

[Dean]: Absolutely. So take passwords, for instance. Right. When we look at breach data, so you can look at breach data, if you have a web, if you have a dark web monitoring tool and we look at our clients and see if they're... if they've been breached, and sometimes you see their passwords in plain text, and then you see the passwords are their spouse's name.

[Kevin]: Yeah.

[Dean]: Their kid's name birthdays and they get real clever and use their pet's name with a number on the backside of it. And we see that 93% of these passwords are just terrible. So, you know, first line of defense is the password. And they're terrible in most cases. Common passwords are used, they're storing them incorrectly and files called "password dot doc" on their desktop. They're using common passwords. They're using simple ones. And they don't understand that those simple passwords with modern password cracking tools can be instantly hacked, let alone if they're using the same password that's been exposed in the dark web that people can try in other locations ...is not a credential stuffing attack. That's exactly that. Oh, look at look at Kevin's password. We're going to try that at his critical systems and variations of that. So there's huge problems and you have to protect against that. People will use lousy passwords. Yeah.

[Kevin]: And I think that's our next security control. Talking about passwords. Let's stay on this for a second. I've done some thinking about this and I think it certainly makes sense to have as long a password as possible. That's probably the most important criterion. But then you have a combination of large and small caps, letters, symbols. You can make your passwords stronger. You can anonymize your password, as I like to call it, so that you don't have proper names or names of your pets, or your children in there. But my 17-year-old son always argues with me about this point because he says, Yeah, Dad, you can have the strongest password in the world, but if somebody hacks into your system and gets access to everyone's password, then what do you have? What's your response to that? Help me respond to my son who is...who's skeptical about the use of even a super strong, smart password.

[Dean]: Yeah, great question. So in some cases, both right and wrong. So where he's right is if people store their password. Believe it or not, a 17 year old is right.

[Kevin]: This is news to me.

[Dean]: Yeah. Yeah. So if they store their passwords to Google Chrome, right. And they use their personal Gmail, that's not protected with multi-factor authentication. He's right. That could be hacked. And it just happened to Cisco three or four months ago. That's the exact mechanism, the fact where the password for stored in Google Chrome, Google Chrome was logged in with somebody's personal Gmail that personal Gmail was not protected with multifactor boom. Deal. However, where he's incorrect is that there are safe ways to store passwords. So they're called password vaults for example. Mm hmm. So password vault is an encrypted area where nobody can get in beside yourself with that password. If you don't use multifactor authentication with it. He's right. But you need to use the password. You need to use multi-factor authentication. So now there's two doors to go through, right? Your password. And you've got to approve access to your phone or some other mechanism, then it's protected. All the good password vaults nowadays are encrypted with 256 bit encryption, so you can't get in unless you go through the front door. It's impossible. And nobody but yourself has access to that information. So there are safe ways to save them. The unsafe way to save them are your browsers, you know, file password file .sos on your desktop. You know, those kind of things are completely unsafe, but a proper password law with multi-factor authentication is safe.

[Kevin]: So that leads to a fifth security control that is very hotly talked about these days, and that's MFA or multi-factor authentication. I was watching a webinar a week or two ago and they invited questions and I asked a question about passwords and it was a very effective webinar, two very experienced young guys who clearly knew their stuff. But when I asked them about strong passwords, it was interesting. They said two things. They said, first, the most important criterion for a strong password is length. And the second thing they said is, you know, as important as that is, maybe the best way to guard against a weak password is to have multifactor authentication. Now, there are apples and oranges, but does that make sense to you? And how can MFA get around any possible password weaknesses that you or your employees may have?

[Dean]: Right. So they both are important because a mechanism is, first of all, like the Cisco hack they got in, they were able to get the password to the Cisco VPN and then they did what's called a MFA persistence attack. They can easily send, Hey, you need to approve this. You need to approve this access, you need to approve this access. And that employee either approved it inadvertently or actually approved it on purpose, or it was coupled with a phone call from the hackers saying, Hey, yeah, this is the IT helpdesk, please approve it. Right. So by that password being initially exposed, that led them to be exposed to an MFA persistent attack. However, MFA is the number one control you need to put in place for any important data. Otherwise you're at risk because there's only one door that needs to be gone through. And both of those together provide a very effective barrier. Now, it's not a cure-all. You still can be hacked. We started this conversation off today with how you can hacked via a man in the middle attack without using a VPN. But both of those things together are extremely important. The other thing that we see is that people will say they had MFA like when you talk to a business, they'll say, Yes, we have MFA on email. Then you ask, Was it enforced? And they're like, What do you mean? Or does everybody have to use it? Well, no, but they're using it. Then when they check, they find out that, you know. Drum roll, please: 20, 30, 40, 50% of the people aren't using it, so it needs to be enforced because it's mistakenly thought it's in place when it's not."

[Kevin]: So we've talked about five security controls. VPN, antivirus protection, endpoint detection and response, passwords, including storage of passwords, and MFA or multi-factor authentication. I want to circle back to a couple of other things, but before I do, besides those security controls, are there any other low-hanging fruit controls that everyone should be thinking about no matter what industry they are in?

[Dean]: Yes. So here's a free one. So nothing...you'll don't have to buy anything. Just encryption. So? So laptops, you know, they have a just encryption on on PC this call it Bitlocker on Macs is called Firewall. And

what it does, it's encrypted. So you can say, well, why do I need that? I have a password on my computer. Well, the reason is, is that to take a hard drive out of a computer takes four minutes. And the reason it takes four minutes because it takes you three minutes to find the small screwdriver. All the data, if it's not encrypted, can be compromised. Next thing you hear is, well, you know, we're not saving any information to our hard drives. All the employees are supposed to save it to, you know, whatever, you know, Google Drive or SharePoint or whatever. Some do, some don't. For a lot of those same folks save their passwords into their browser, which we've already talked about. The point is, if your disk isn't encrypted, all that information, including any password you stored in the browser, would be accessible by the hacker in minutes. So disk encryption, it's free Bitlocker or Firewall... just do it. And by the way, in healthcare, if your computer was stolen, your laptop, and you can't prove that that hard drive is encrypted. That's considered a breach under HIPAA.

[Kevin]: To the runner. If you can't rule it out, then you have to assume there was access and then you have to report.

[Dean]: Yeah. Have to report as a breach, right? Right. That's free. Other ones that are super important. Right. So we don't really talk about business email compromise protections, right. So business email... a lot of people are hacked this way. They click on phishing emails, which is somebody sending a fake email to you to fool you into voluntarily giving your information away. Not knowingly, but voluntarily. So having the appropriate business email protections like, you know, enterprise level email filtering. So those don't even get to the employees to click on in the first place is super important. Things that block viruses. Again, another layer of defense things that block phishing attacks, things that use a AI to uncover, you know, is that is that a fake attack or not? Right. So that's super important, business email compromise protections, if you ask me, is one of the most important because everybody's using business email and a lot of folks just don't pay attention.

[Kevin]: But no, go ahead.

[Dean]: Sorry. To give you an example, Kevin.

[Kevin]: Yeah, go ahead.

[Dean]: Phishing tests of clients. Right. We run one and nobody falls for it. And everybody's, like, clapping and high fiving. Yeah. Our employees are well trained. Then you run the I don't know, the Door Dash on a Thursday night. Guess what 15% click on it or if you're on the Amazon one right before Christmas. 15%.

[Kevin]: Yes. Yes.

[Dean]: So no matter how much training you do, we find that people will click on things, but you're not paying attention. And it's something that that's part of. It's not out of character. Like, Oh yeah, I just ordered DoorDash. I'm going to click on that. Yeah. Or my kids must have ordered it, so I'm going to click on it and oh, they just infected their computer. Boom!

[Kevin]: Let me let me ask you about one other security control that you just alluded to. And it's kind of a trick control, but it's important. I think it may be the most important control, and that is employee training. I hate saying this, but it is true. You are only as good as your weakest link and as employees, we are among the weakest links. We are the ones that the threat actors can fool with those spear phishing attacks. So, Dean, talk to us a little bit about what a good employee training program should look like.

[Dean]: Great. Great question. So I don't know if you've ever gotten a ticket, but, you know, I don't get one too often. I feel like five or six years ago I got one because I was on my phone. But I digress. And then you have to take that training course. It takes 4 hours. And it was so painful and so horrible. And all they could do is fast forward and click the button. And it actually made you start over again. It was just terrible. Yes. So first of all, I got to realize that employees don't really want to do it. So it has to be sort of effective. Five minutes, seven

minutes maybe. It can't be like watching paint dry. Should be done monthly, but some people can't really figure out how to do that. So at least quarterly is as good, monthly is better, but it has to be short effective and really the point of can't be techie. It has to be entertaining a little bit, but really has to get to the point of some of the things we've just talk about. So that's one piece of it. The second piece of it is, of course, is accountability, do people will take it or not. Because people won't take it unless they're forced to.

[Kevin]: We can't avoid that here at Barclay Damon. Because if I don't take it, I get a reminder every single day until I do. And I don't want to be the last person to go through the employee training. I have no excuse.

[Dean]: Right. Right. Like stuff that you're an expert and you know it all. But again, everybody's an expert, so we need be taking it cause there are new threats. The second part of a good training program is what they call phishing testing. So phishing testing is the business or the company that you've hired sends out fake emails trying to fool employees, into clicking on it. And when they do click on it, it's a teaching moment and some employees, it's like, Oh my gosh, I can't believe I got clicked, really opens their eyes. Some they click every week and there's no helping them, but at least you know who those are. So you can keep us closer eye on them. But those two components are super important part of a cyber awareness training program.

[Kevin]: Now you've given us a lot of great ideas and things to think about, and these are critical security controls. And I know we're running out of time, so we'll have to leave it there. But I'd love to have you back on another episode to talk more about some of these targeted attacks and how we can anticipate and make sure that we don't fall into the traps.

[Dean]: Yeah, very cool. Yeah. Love to, love to. There's a lot more you can go on all day about this and but there's a lot to it for sure.

[Kevin]: Yeah. Well, Dean Mechlowitz from TEKRiSQ, thank you so much for joining us this morning on Cyber Sip. Thank you for joining us. 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.