Barclay Damon Live Presents *Cyber Sip™*
Season 4, Episode 7: “Insider Threats, Training, and CISOs at Risk,” With Gregg Davis

Host: **Kevin Szczepanski**, Barclay Damon and
Gregg Davis, EPIC Insurance Brokers & Consultants

[Kevin Szczepanski]: Gregg Davis is managing principal and TAS leader—“TAS” is technical advisory solutions—in the Professional, Executive, and Cyber Solutions Unit at EPIC Brokers & Consultants. So happy to finally have you on. We’ve talked together on panels, and it’s great to have you on Cyber Sip, Gregg. Welcome.

[Gregg Davis]: Thank you very much. Great to be here as well.

[Kevin]: We’re going to… and congratulations on your recent promotion. You had a slightly less lengthy title until a few months ago, right?

[Gregg]: I did. I believe I’ve exceeded the word count on the auto response. [Both laugh.]

[Kevin]: Ha ha. Well, we’re happy to have you here. Thank you very much. And we’re going to have a wide-ranging discussion. We’re going to talk about social media training. We’re going to talk about insider threats. And we may have some other interesting discussions about the latest risk. if we have time left, I may ask you some questions about AI. Some of us just came up in a recent setting here at our firm, Barclay Damon. But let’s start, Gregg, with the subject that we talked about a few weeks ago when we were designing, or as the young people say, curating this episode. And that is about training, and I know we’re going to talk about the strengths and weaknesses of online training why I think you have rightly concluded that online training ain’t all it’s necessarily cracked up to be… but before we do that, we’ve got business email compromise. We have electronic transfer fraud, but what are some of the latest social media or cyber threats that you are seeing at EPIC? I think one of them we just touched on before we came on and that pertains to insider threats. Do you want to talk a little bit about that?

[Gregg]: Sure. So we’ve been seeing a pretty large increase in the frequency of cyber incidents among our clients. Luckily, at least in the last six to eight months, the severity has been reduced as organizations are having better response tools, are able to do better segmentation, are better able to respond to the incidents. But every so often, unfortunately, we are getting some pretty large losses. And we see a continual increase in your standardized stuff, I’ll call it the “phishing” of the world and other things and the social engineering pieces of it. The complexity of the attacks has gotten exponentially more difficult. So part of it is the use of AI, just in… able to craft better emails and better phishing things. We’re also seeing them use a lot more intelligence. So we’re seeing them do a lot more reconnaissance. People are very open nowadays. And it doesn’t take them very long to go onto Instagram and to LinkedIn and to other areas to really hone in on creating a personal experience for the person they’re trying to have…make the click or make the phone call. So, you know, we’re seeing a lot of better sophistication, a lot more time and research being spent on their targets rather than this wide blast with misspellings that we were used to from the past. So that level of sophistication is really exponentially growing. And one of the areas that my background really is as a CISO for a large multinational international organization is that, you know, we’re very, very focused a lot of times in cyber on what’s happening from the outside. We’re going to put firewalls and we’re going to block, and we’re going to tackle, and do all these things. But really the insider threat has grown tremendously. And whether that is from some of the recent media articles about North Korea getting people hired. One of our large companies that engages in phishing training actually accidentally hired a few people. So really the drive to remote work has made it a little more difficult to interview and capture some of these people that are complete fraud. They are using AI to fake people, create people that fit perfectly into the profile that will surface to the top of your HR system using AI, right? So they end up getting hired and picked and they're actually threat actors from a foreign government or foreign entity. And the other thing really is around corporate espionage still continues to grow and get extremely more sophisticated, and we can delve into that a little bit more. The recent announcement from Kroll was that almost 21% of their incidents were some type of insider threat, insider training, or insider attack and a threat. And really it's a multi-leveled situation, so it's very difficult. But if I'm making, you know, $70,000, $80,000 a year as an assistant and I get approached, somebody offers me $100,000 just to click on one thing, it's a very compelling situation. Now, the rest of the attack will be happening from them, but this type of situation is happening more and more where if it's not somebody that's being put in place from the outside companies, they are recruiting somebody inside to just... leave your computer on. You know, something very simple sometimes is that... just click on this little link and then just walk away, right? So I'm not going to do anything to hurt my company. You don't have to, just leave your computer on, right? So there's things like this that are happening that they're inside people are helping facilitate. And it is creating a really difficult scenario for CISOs and security experts and, you know, for the cyber insurance world as well.

[Kevin]: You said 21% so one out of every five attacks during that period of time is an insider threat and that...

[Gregg]: ...has some form of insider. was recently from Kroll, was just released. That was their January statistics that they closed on.

[Kevin]: And that's so concerning because a lot of the safeguards that we typically talk about, like multi-factor authentication, that's not going to answer an insider threat because that person's already inside. So I know we're going to talk about training, but let's stay on inside threats because I don't think those of us out there that have been dealing with the external threats are as knowledgeable about the prevention techniques for threats on the inside. What are you seeing? What can you tell us about the strategies that good businesses are using to tamp down on those insider threats?

[Gregg]: Well, there's several of them, but we've really put a lot of time and investment into blocking the external piece and we have to get our focus back on the internal. It's just as important, if not more so these days. So we need to make sure we're doing proper data segmentation. We really should be moving zero trust ahead much faster than we are. We also have to really enforce the "least access, least privilege" situation. And, you know, no offense to law firms, they... law firms, professional firms in general tend to be some of the worst. I'm so-and-so, I need access to this, just open the floodgates, right? And then what happens is they forget to close them, or they never close them. So certain people get much broader access than they need, or they're frustrated because they can't find what they're looking for. So, the IT teams tend to open the floodgates and then that... and then on top of it, what we really have slowed down investment in because insurance companies haven't emphasized it from a cyber standpoint is people have really dropped investments in DLP or data loss prevention products. Now some of your XDRs and EDRs and some of those tools will help monitor patterns. But if I'm an engineer and I'm used to downloading large drawings, it's not going to pick up when a threat actor also starts downloading those drawings, right? So, it depends. Now the true data loss prevention products—or the DLP products—are specifically made for to watch that inside situation, also to look for data patterns, right? So security numbers, phone numbers, certain PII... and to catch them before they leave within documents and things. And just like an EDR solution, they are a challenge. They're a challenge to tune. They're a challenge to get right. They're a challenge to implement because when somebody stops... their work is stopped, they get very frustrated. But on the other hand, if we stop your data from leaving, it can be very beneficial. But it's always a fine line between the security departments and making sure the organization is productive and producing the widgets or the output or their professional services they're supposed to be doing.

[Kevin]: No, it absolutely is. And what we're seeing, I'm seeing recently in some claims is that not all EDR, not all threats, I should say, look alike. And there are instances where you think it's just set it and forget it. You've got an EDR tool, you've got Sentinel-1, or you have a third-party service provider that's monitoring. Well, you need to have a dialogue and communication with that third-party provider to know what sorts of threats you're looking for because if you don't have clear communication, that third-party service provider may let through communications or actors that seem low risk but turn out in the end to have been very high risk. We're seeing that more and more. And I guess the takeaway for me is that the threat actors are getting more and more sophisticated. What you thought was protecting you 18 months ago is not enough today.

[Gregg]: Yeah, and we see this quite often where they buy an XDR and EDR tool, they have an MSP, but then they really don't turn on the R—they don't turn on the response. Because again, it takes time, it takes months sometimes to really fine tune how to R, I'll say, or how to respond, right? And when you're working on a Sunday and you're trying to get something out and the system lops you off because it doesn't like what you're doing that time and date, and then you got to call IT, right? This level of productivity and frustration kicks in. And of course, they got to make sure that it's you calling and not a threat actor calling, right, faking that it's you. Because it only takes 30 seconds of your voice from this podcast right now. They can create a deep fake in seconds and it could be "Kevin" calling and saying, I need access to this data, right? They know where you work, right? They know everything about it, right? So...

[Kevin]: Mm-hmm. Mm-hmm.

[Gregg]: These are the types of things that are happening. Now, in MSP, remember they're a hired outside company. If they don't want to upset Kevin, Kevin is, you know, a certain stature at this organization. And if Kevin calls, they don't want to get fired, right? They don't want to get in trouble. So, these are part of that social engineering that we're talking about that's happening, right? So, it's human nature to say, oh my God, Kevin is, you know, he's a very important person. He may decide our contract. Let him get in, right? Don't upset Kevin. So these are the social things that are happening where it's very difficult for human nature to say, I'm sorry, I need you to verify that you're really Kevin. And that takes a lot. It takes a lot of training, and it takes a lot of discussion, and it takes a lot of understanding from the organization, from the culture of the organization to say when the CEO calls, I'm not going to believe it's the CEO calling. I'm going to have a code word. I'm going to verify that funds transfer. I know he's the CEO, but we have to set a culture in this organization that says nobody will be fired for verifying the information. Nobody will be, you know, there'll be no punitive action if you verify the information. As silly as that sounds, right? How dare you question the CEO? How dare you question the senior partner, right? But unfortunately we have to today question those things when it comes to funds transfers or certain contracts or things, especially when they're top-secret projects, right? These are all the social engineering things that they're taking advantage of.

[Kevin]: You hit it... and what we're talking about in a way is the zero trust concept you alluded to earlier. We need to bring that lack of trust within the four walls of our respective organizations. It's not just the outsider threats that we view with suspicion, whether it's an insider with malevolent intent or an insider who makes a mistake, acts negligently. We have to have that level of suspicion on par with those of the external threats. We're not there yet, but hopefully by talking about it, we'll move the needle a little bit further to the right each time. All right, so I want to shift gears now and talk to you about training because one of the ways, now training may look—and feel free to address this as we go on, Gregg. Training to guard against insider threats may look a little bit different, but many of us many of our listeners out there have participated in online training with regard to social engineering broad and I have to and I don't know about you, but when I participate in those training sessions, I am not always exclusively watching the training video; I may be doing two or more other things at the time. And with that as the setup, let's talk a little bit about training when you're thinking about whether you should be training your employees. And the answer is yes. Where do you go? I don't want to pick on the third-party providers, training providers, because you know what, what they do is perfectly fine. But you and I are finding that it may not be as effective as people might have thought it was a year two ago. Let's talk about that.

[Gregg]: Sure. I think it's a combination. I think we need some, you know, some online things, but we really need real-world stories. We really need it to come to life. We need a presenter to come up there. We need people in a room with their cell phones in a basket focused on this situation. And it applies to outside and inside threats because unfortunately you need to keep an eye sometimes on a coworker. And I'll talk about that briefly for corporate espionage stuff because it happens on a daily basis. But we need real-life stories. I can't tell you how many claims we've dealt with or had a dealing with where that person would be like, there's no way I'm ever going to fall for this. There's no way I'm clicking on this. There is no way this would happen to me. And some of them are actually recorded during these. And then of course they end up being the one that it happens to. Again, it's not a knock on the training pieces for some of the online platforms and stuff. It is a testament to the sophistication that the threat actors are doing. They have stepped up their game far beyond watching a boring video where you can put a dental bib on because you're drooling, it's so boring. And it's on your third screen on the right and you're trying to click every so often to pay attention because they have the little quiz question, right? It's not absorbing, it's not reaching the employees the way that it should. Most of those are outdated, they're cartoony, they're not real world, and they're not really illustrating the true threat. And people are just trying to check a box, they're trying to comply with a insurance carrier requirement or an HR requirement or a legal requirement and saying, yes, we do training. And the reality is it's not hitting home, it's not absorbing. So, you know, I've embarked on several different discussions and trainings when I really focus on real-world stories and people love to hear the real-world stories because they are plentiful of examples of things that have happened and they're exciting, and they're interesting, and they bring color and life to a situation in person and when you can engage the audience and ask questions and ask people what they thought or how it would happen and play different scenarios, it's so much more absorbent and immersive and everything than sitting there through a boring lecture. And it makes a tremendous difference in the impact on the organization. And that's one of the things that we have been focused on. At the same time, it needs to raise your awareness because I'm not saying you need to be a corporate spy or anything, but you also have to just be aware of what's happening around you. There are constantly—and have been for years—there are threat actors that come from either foreign nations or from other areas that they're literally hanging out in the bars that you hang out with after work. They literally are targeting organizations and companies. They, for example, want, you know, your secret drawings. They will become friends with you at social environments. They watch your office. They see exactly where people hang out. You know, they interact with you. They become your friend. They come for lunch. They plant the bug in your desk. There's all kinds of things happening like this on a daily basis that people don't know and understand. There was a CEO in a company that said they had the most amazing security in the world and a threat actor, well, a person doing a staging to prove to them their security wasn't great, ended up being a birthday dancer to deliver a telegram, singing telegram and walked into the CEO's office because it was the CEO's birthday. So here, know, a potential… we still let our guard down. We still don't pay attention to this stuff. You know, unfortunately a large US plane manufacturer had multiple cybersecurity incidences and then a, you know, another country now is producing an aircraft that looks, you know, looks, feels, and flies almost identical to that aircraft, you know, two months after, two years later. So, there's things like this happening on a regular basis that aren't just quote cybersecurity incidents, right? But are intellectual property and other things are happening in our corporate world that we need to have awareness of these things so that we know what to look for, so that our spider senses go off and not to create a paranoia, but just awareness of what's happening. Why did I find this USB key in the parking lot, right? We all know this CIA years ago was compromised because people found USB keys laying in the parking garage, right? It's an old story. So things like that are still happening daily, not only to get your data and some of the ransomware attacks and the public things you've seen, but also just to get your intellectual property.

[Kevin]: I want to talk about some other topics, Gregg, but while we're on this one, let's talk about what employees should be doing. Dare I say the answer is still very simple, but it doesn't always work because the threat actors are getting better and better, more persuasive. What I always say is there are two things you need to be aware of. If you are on the phone with someone that is talking about an urgent matter, you must urgently take action or talking about how you must transfer money and maybe a combination of both. It's an urgent situation in which you must transfer money. You need to be…you need to stop and don't take any action and then verify that request using a trusted communication method. In other words, you think you're on the phone with the CEO, you need to say thank you very much, hang up. And then call the number of the CEO that you had yesterday before you got on the phone with the threat actor and verify that you really are supposed to transfer that $1 million because 99 times out of 100 the answer is going to be no. Why does it still happen anyway? If it's so obvious, if what I just said is true, you need to be on the lookout. Why do people still fall for these traps?

[Gregg]: Human vulnerability is all I can say. But I think there's a few quick things that can be done to not impose a difficult social situation. And I emphasize this with people's families as well, because we're now, over the weekend, the New York Times featured an article about a mother that was called, her daughter was screaming, and of course it was completely AI and she transferred money. So these are the things that are happening, even from a personal basis. But I would set up a code word that the CFO and the CEO are the only two people that know the code word. And if the CFO gets a call that says to transfer the money, he says, no problem, I'll take care of it right away, sir, what's the code word? And if that word is between the CFO and the CEO only, you can prove this. You can have this between your controller and the CFO, for example, and have a different word. So just by having a couple of code words, you can say to the threat actor, no problem, I will initiate the transfer, thank you very much. And then you can call back and ask the code word or ask them even the code word. And if they don't know it, they'll usually berate you, get defensive, have all this stuff, right? If they're just the kidnapping situation, they're going to tell you that, you know, they're not going to answer that or we're going to take it there. But it's a simple way to say, I fully agree with you. I will do everything you want. Just need the code word, right? So things like that, simple pre-discussed situations can avoid some of these things. Obviously the traditional steps of verifying account number changes and things like that. Again, I can't tell you how many times they call the phone number on the invoice or they call the phone number from the email, right? They look at the bottom of the email and they call the number that's in the signature. They'll say, didn't call from the invoice. I called it from the signature, but the signature was a fake. So they have to have—every vendor, they need a system of known numbers, known contacts, not from the email. And again, they'll do that nuance. say, well, I didn't call from the invoice. I called it from the email. Well, you know, they fell into the same trap.

[Kevin]: Right, because the invoice is attached to the email. All right, before we move on to another subject that I know is near and dear to your heart right now is a CISO. I'd be remiss talking to a managing principal at EPIC Insurance Brokers and Consultants if I didn't ask about the insurance implications of all this. So whether we're talking about insider threats or what we just talked about, business email compromise or electronic transfer fraud. I'm thinking of, chiefly I'm thinking of a crime policy and a cyber policy with first-party coverage. Are these policies going to apply when we make these mistakes, or we suffer these insider threats? And here's the million-dollar question, so to speak: If they do apply, Gregg, are they going to be sub-limited so that the coverage you get is much, much less than that face amount of coverage you have on your policy?

[Gregg]: So I don't profess to be a coverage expert, because I focus really on the technical controls. But I will tell you in general, almost all of the crime, e-crime coverages that are in a cyber policy are all sub-limited. Very rarely do we ever see them at full limits. They're usually 250, 500,000, et cetera.

[Kevin]: As opposed to a million or two million...

[Gregg]: Correct. So normally you a $5 million or a $10 million on the larger organization. Almost always those are sub-limited to some level. And then of course you have your crime policy. At EPIC we do, if an organization has a separate crime policy, which we would recommend, one of the things that we do at EPIC is make sure that things like the deductibles are coordinated so that usually a crime policy has a much lower retention, not really deductible, but a retention. And that is... we try to make sure that crime policy can actually pay for the cyber retention. The circumstances matter how these things happen. The insider stuff, I can tell you, is very, very difficult to prove. It's very difficult to prosecute these things. I worked with a fellow colleague who, an employee, to make a long story short, clicked on an email, the phish came in, they lost a lot of money. And the person claimed stress and harassment because other employees were angry because they didn't get bonuses that year. And this person is now living in a $6 million beach house and didn't have that kind of income. But getting law enforcement or anybody, especially today, nobody's going to investigate this, right?

[Kevin]: It's hard to get their attention.

[Gregg]: It's hard to get their attention for stuff like this. And to connect the dots is very difficult. From an insurance standpoint, it also can be difficult. And the reason I say that it can be difficult to trigger some of these coverages depending on the circumstances. And of course, you on the coverage side, as an attorney probably see this, right? So right, there are nuances and carve-outs, especially to the crime policy about whether it truly was inside. And then you have the cyber one where it came from outside. These are hybrid attacks, so they're more complicated. So it's not black or white, but this is, these are some of the very slippery areas where, you know, legal counsels like yourselves and others need to get involved because they're not clear-cut situations. And the insurance piece of it versus the legal prosecution piece could be different bars to cross, right? Different minimal thresholds. And so it's very, very important that you have a really strong forensic firm. It's very important that you really understand what happened, keeping logs and understanding what happened, because the details of each of these attacks will matter tremendously when it comes to transferring this risk to some type of insurance product.

[Kevin]: Right, so taking this together, I think though, brilliant points, Gregg, and the takeaway is if you've got... if you've suffered, as one of our clients did a couple of years back, a $2 million loss because someone impersonating your financial institution convinced you to transfer $2 million to a threat actor's account. You probably...may or may not, and in our case you probably won't have enough insurance to cover that loss so how do you make up for that you've got to have a full court press. Yes, you want to pursue insurance. You may want to pursue the financial institution because maybe that institution shouldn't have said yes to those transfers based on certain red flags. And you want to bring law enforcement in because sometimes... for every time that they're unable to participate, many times we have found they will, and they can execute their financial fraud kill chain to bring those... claw that money back before it gets to foreign jurisdiction. All of those things very important. I agree with you completely. You've got to have a network of forensic and legal professionals and insurance professionals standing by and sometimes, Gregg, I have found we have to have some very nice as I know the folks at EPIC, do we have to have some very friendly but pointed debates sometimes with our insurance partners to say, hey we've never experienced this before. We know your claims experience is still in the grand scheme of things. These aren't auto accidents. The numbers of claims are much, much smaller. The carriers have less experience. So sometimes we need to work together to educate the carrier on why this is something that needs to get covered. So, I'm grateful for your insight in insurance. I know you're more on the technical side, but I appreciate it. But now I want to delve into something that I know you have a depth of experience in because you are a CISO. I don't even say you're a former CISO. I think once a CISO, always a CISO. Before we get to it, I don't know if I ever asked you this question. And to our audience, you'll never get this 20 seconds back. I have heard CISO say "SCISSO," C-I-S-O, and CISO. What's your preference and is one of them correct?

[Gregg]: No, any of those are perfectly fine. I've been called many other things. So those are all in a good category. No, it's fine. And honestly, it's relatively new from a corporate. I mean, it used to be under the chief information officer for many, years. In fact, my title was actually CIO for many years, but I was also the CISO. So, it really has evolved over time that this role has become, you know, separate role of a security officer. But I also do want to point out while we're talking slightly about insurance is that just because you have an O in your title doesn't mean you are an O as far as directors and officers insurance goes. So the O piece being officer, if you are being hired as a CISO one of these people, or anybody that has an O in their title. There's a lot of new O titles, chief growth officers and diversity officers, there are other things that may or may not be covered under D&O policies in cyber and all these other things for stuff. Talking about for personal actions. So, they should just make sure, double check with their brokers that their O is actually covered as an O.

[Kevin]: No, that's a good point. You're right. If you're beyond CEO, CFO, COO, you're in a gray area and you want to make sure that before the policy goes into effect, you've got language there and many carriers will have it that expands that definition so that you have your CISO for one has the benefit of that protection.

[Gregg]: Right? So when you read a lot of those policies, right, it's around regulatory.

[Kevin]: Yeah, so what we're talking about just for our audience, we're talking about what and maybe Gregg, if you could, so a couple of points: first for our audience, we're talking about, okay, if you're a CISO and you're targeted like this, is this something you can turn to your insurance company and say, help me? Do I have a defense? Do I have insurance coverage? And we're going to tee that up cause you talk about whether... is this a regulatory proceeding so that it falls within one of the insuring agreements in your cyber policy. But even before that, Gregg, for those in our audience who don't know, can you tell us a little bit about Chris Krebs? This is not a fly-by-night guy that is not known to the industry, right? This is a very well known, regarded and seasoned cyber executive. Probably one of the leading executives in the country today, I would say.

[Gregg]: Yeah, apologize. I forgot people may not understand who was. Chris Krebs was the director of CISA for the federal government during the election for 2020. And he has been in cybersecurity for many years. I believe he graduated Harvard or Yale Law School, one of the top law schools. I mean, he is a well-seasoned and respected attorney and cybersecurity expert and has been doing cybersecurity for many, many, many, years. And CISA has been an amazing partner with CISOs, as we're getting too many acronyms here. So he was in charge of... not only there was a whole committee within that agency that secured the elections, but he was also the head of the whole organization of CISA.

[Kevin]: And I think that's fair. And you know, course the whole debate was the distinction—at least in certain quarters—the distinction between whether there is ever any fraud in an election? The answer which is almost always yes on some level. And whether there is any evidence of any fraud that changed the outcome of the election. For which there has never been any evidence and at which many people have looked. I don't know what does it say... how can our... you know...if you're in the audience now listening to this... what conclusion do you draw from it? Yes, I suppose if I were in the audience, one thing I might take away from this is, well, what happens if someone in my organization, publicly traded company, private business, is targeted? Do I have insurance? Do I have a defense or indemnification for any fines, penalties or other compensation I may have to pay. And you were alluding earlier, if you're Chris Krebs or someone like him down the road, there's a real question whether a cyber liability policy would apply in this situation. I don't think the underwriters of today's cyber liability policies had this sort of issue in mind when they wrote that coverage, right, Gregg?

[Gregg]: Yeah, I think that's true. And I think that if you take it to other policies that you have broader experience with, if that organization's share value drops tremendously because of this and the third party or investors come after the organization, how this evolved, it's not your standard situation. It's not your regulatory, it's not your criminal, it's not your cyber. So ...this is a new area that is putting a lot of people on nerve, and this is the first time where individuals have been named in situations rather than like you say, even a law firm naming a firm is, even in the case of Mr. Emhoff, the prior vice president's husband, they still named the firm. This is the first time that it's been an individual name as far as I know. And I completely understand national security and coming from my background and I would understand saying this organization, because they might have done something, you know, that's one thing.

[Kevin]: That's, I don't know, how does that make you feel as a CISO?

[Gregg]: Makes me feel that I'm glad I'm not actively a CISO right now. So my role as a technical advisory is, you know, I advise clients and work with clients on a regular basis. EPIC Brokers has their own CISO and IT team. So I have transitioned out of that role. It's worse than dog years. So one year as a CISO is way more than seven years. You know, I have this gray hair, but I'm actually only 29. No, I'm kidding.

[Kevin]: Yeah.

[Gregg]: But you age quickly and the threats and the attacks and everything are really multifaceted. And it’s very, very challenging to have state regulations, federal regulations, reporting requirements, and all the other things that are happening inside or outsider threats. So managing all of this and getting any sleep at night is becoming even more of a challenge. And it takes a really good solid security team and I hope organizations really do their best to invest in that because their entire organization could be gone in a matter of an hour with this stuff. And I just want to quickly get back to you on the team about the financial fraud stuff. The clawing back of money you mentioned, that normally has to happen no later than 72 hours, usually 48. So going through tabletop exercises and practicing these things and knowing who’s going to call and when you’re going to call them, and all these things are absolutely critical because that clock is ticking and if you want to try to get that money back, you need to do it immediately. And we hear a lot of times for these claims—we suspected, we had some anomalies for about two weeks in our system, then, right? So these threat actors are not coming in and in seconds and doing something, right? They’re in your system sometimes weeks, months in advance planning a situation. So that’s also one of the changes that have happened with this stuff. It used to be, they would log in quickly, would encrypt you, and that would be the end of it. That’s not the case anymore. It’s all about extracting as much data, as much pain, and putting as much pressure on you to pay.

[Kevin]: So we are up at the end of our time, Gregg, but before we go, we talked about two very important steps I think every organization should take, talking about in-person training, tabletop exercises, which is a subset of that in-person training. Last word, Gregg, if you had to tell an organization, this is what you should begin to do first thing tomorrow, what would you say to an organization that’s really interested in upgrading their employee training and internal security.

[Gregg]: I would really focus on the insider threat. I would focus on enhancing data loss prevention tools, DLP tools. I would focus on setting up zero trust and really making sure that that is in place. I think we’ve done a very good job in recent years of buttoning as much as in many cases from the outside. We now have to go back and re-button up the inside because we did it for a while and then we really backed off. And now we got to go back and look at the inside and really understand what our employees are doing and what new hires are doing and how they’re accessing it. An employee working 20 hours because they’re new and they’re remote looks incredible. But a lot of times that could be a team of people from a foreign country that are actually working together, trying to penetrate your system. They’re not actually working like you think they’re working. So things where you say, goodness, they were logged in for 18 hours. They’re a great employee, actually may not be that great. So you really got to look at it and take a step back and understand what’s happening with your data and your systems.

[Kevin]: We’re going to leave it there. But Gregg Davis of EPIC Insurance Brokers and Consultants, thank you so much for joining us. Really appreciate it. And I want to have you come back and talk about AI next time. That’s another episode into itself. But thank you so much for joining us today.

[Gregg]: My pleasure, Kevin. Thank you very much. Appreciate it.

[Kevin]: Thank you and thanks to all of you for joining this episode of *Cyber Sip*. We’ll be back soon with another episode.

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

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.

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. Thanks for listening.*