Digital Planning Podcast (Season 5, Episode 5): When Cyber Attacks Hit Home

Speakers: Justin Brown, Jen Zegel, Ross Bruch, and Kris Coleman

Justin Brown:

Welcome to the Digital Planning Podcast. I'm Justin, and I'm here with my co-hosts, Ross and Jen. And today we have a great episode for you on cybersecurity. As a warning, today is going to be one of those keep you up at night episodes, so you may not want to listen right before going to bed. We are honored today to be joined by Kris Coleman of Red Five Security. I heard Kris speak earlier this summer at a Trust and Estates Conference, and let me tell you, he scared an entire room of trust and estates attorneys into complete and utter silence. After hearing Kris speak, we wanted Kris on the podcast so that we could share with our listeners what we've learned from Kris in the area of cybersecurity. Kris, welcome to the Digital Planning Podcast.

Kris Coleman:

Thank you very much for having me. I appreciate it.

Justin Brown:

So before we get started, Kris, you have a very unique background for one of our guests on the podcast. Can you tell us a little bit about yourself and your early career before you founded Red Five Security?

Kris Coleman:

Sure. Back in the exciting days, if you will, I started my career at the CIA. I was working security issues, intelligence operations, counter-terrorism, and this goes back to the '90s, if you will, and pre-cyber, just to put that in context. And I worked all of those issues with the agency, traveled around the world, a variety of different countries, and obviously using those skills for good, if you will, a particular set of skills. But then moved over to the bureau, the FBI after that, after about eight years, and became a special agent with the FBI, where I worked out of San Francisco. There, I used the investigative authorities that were given to me as a special agent, and I worked international organized crime, working specifically large illegal gambling cases, and then I jumped into international terrorism, which was really more my forte.

And I was there during 9/11, and became the case agent there, supporting the FBI out of San Francisco Field Office. Shortly after that, four years in the bureau, went back to the agency. My skills were needed back there to work counterproliferation, and my wife was at the agency at the time, so it was good for us to get back in the same city. But working counter-terrorism, counterproliferation, which kind of goes hand-in-hand, found myself in about 70 different countries, and working with a variety of different cultures, tackling a variety of different adversaries, both in counterproliferation, helping execute the US' mission overseas, and trying to really make the world safer.

Started learning a little bit more about cyber at the time, it was starting to emerge in the 2000s as a thing, specifically around communications. But kicked off the last couple of years of my career training all of our liaison partners over the world, so helping them with counter-assault, counterproliferation, helping them with investigative tactics against terrorist groups. And that was just a fantastic time traveling the world and being paid to do it, but ideally furthering the interest of the US government. Great time, all the way around.

Justin Brown:

So tell us a little bit about Red Five Security. What exactly does Red Five Security do?

Kris Coleman:

Yeah, I left the government in 2004, and started Red five Security. We're starting our 20th year here shortly, which is great. We're excited to continue the work we started 20 years ago, really is focusing on our unique clients, and those unique clients are family offices, affluent families, corporations, and those particular clients have needs that my skillset at is a good fit for. So they come to us with unique challenges as they travel around the world, with specific threats that come in against them from unique threat actors. And so we provide bespoke security services, and really the full spectrum, where we've been told that, "You guys are the company that listens best. You guys listen to what the clients need, and you execute on that very specific solution set."

So we're a bespoke security shop that has a lot of great skills, and a tremendous network globally, which lends itself to really solving unique problems for these kinds of clients. Investigations, and intelligence, business intelligence, if you will, always staying above board on the professionalism and the ethical approach to those kinds of things. Security, design and engineering, we get into online threats, now we're into cyber. Executive protection was something we did for many, many years. Now we focus on partners to get that done. So think of us as a small sort of intel shop almost, intelligence and operation shop to support family offices and corporations to help them achieve their risk management needs across the enterprise that they manage on a daily basis.

Ross Bruch:

So I feel like cybersecurity is something that every person with any sort of cyber footprint needs to be aware of, but can you help us differentiate what the common or average person needs to be worried about from what you are specifically talking about, dealing with family offices, dealing with high-net-worth individuals, and what in particular that threat is, and how it differs.

Kris Coleman:

Cyber's a big word, let's start there. People think IT is cyber, people think threat hunting is cyber, people think online threats are cyber, people get into... Information security is cyber. It means a lot of different things to different people, but if you're talking about specifically threats where they're going after your personally identifiable information, they're going after your data, they're going after your intellectual property, they're going after the communications you have on a regular basis with your family, getting into your devices through technical means, I think that's maybe the more specific way talking about what cyber is.

To the lay person it's, "Someone broke into my email account. Someone broke into my device, they're able to read emails, they're able to read texts, they're able to change passwords and get access to other accounts." Whether it's banking, shopping, social media, whatever it is they may have access to. So really, what we're trying to do is make people safer, make people more private. And what we do on a regular basis, we really do live on the lines of our tagline, which is ensuring bad things don't happen to good people. A lot of people look at these devices, their laptops, their tablets, their cell phones, and everything that happens around the device is sort of voodoo, black magic, no one really knows how this stuff really works, but the bad guys know. And they're usually a step ahead because their whole point is to make money, they're usually tied to a criminal enterprise.

I guess that's kind of where it goes, it's, "What's their intent?" Most of the time it's monetary. They're trying to actually make money in some way, either sell your information, take assets out of your accounts. And then there's the other part of that objective of the bad guys, which is to attack your reputation, attack your profile, attack you personally in some capacity. So cyber means a lot of things, there's a lot of different attack vectors, but when talking about these families, and maybe you and me and the others on this podcast it's, everybody's got a device, everyone's got an online persona, everyone has bank accounts, everyone has these sorts of common assets, and that's the one thing that's changed in the last few years, is, some of the things that we didn't think were assets that were vulnerable to cyber, they now are vulnerable to cyber.

For instance, titles for your house, we get into titles for other assets, property records, public records now could be in theory accessed, and create a problem for you. But brand reputation, the family legacy, these are things that weren't typically attackable through a cyber mechanism. Now, they go after the family office, they go after what might be the family brand, or

the founder's brand or the original company. So it means a lot of things, there's a lot of different aspects to it, but everybody's a great target. It's just a matter of scale, complexity.

Ross Bruch:

And in instances when you're working with these individuals, are you more often called in as a preventative measure, or reactionary, something's happened?

Kris Coleman:

Yeah, great question. I'd say probably 80% of the time it's, "This happened, what do you think we should do?" Or it's a panic, it's like, "Get over here now, get started on fixing whatever the problem is." So it's reactionary, to answer the question. It becomes preventable after that, and ideally, it changes their mindset about the world, and this cyber aspect of their lives, but that takes them into a more preventive mode after that. Sometimes you'll get an advisor to the family that steps in that's been a little more, what do you call it? Cyber native, over the course of their career, and they're like, "I'm going to lead with this." With the family, or state planning council, or whomever they're talking to, and say, "We're going to get ahead of this. Let's not have the problem."

And then fascinatingly, when we talk to clients, and it's different based on, perhaps even gender, or role in the family. A lot of times it's the matriarch that says, "I never want to have a problem. So start now, be preventive." And the patriarch in some instances, and not to generalize, but the patriarch's like, "I'll call you when I need you." It's just two different interesting perspectives to the same problem. We can help in either direction. We love clients to be more proactive, and be more preventative. That's really the way to be more resilient right there.

Jen Zegel:

Well, to that end, Kris, what are some steps that people can be taking now to help prevent them from being the victim of a cyber attack?

Kris Coleman:

Yeah, so that sort of begs a different question to start, and that is, who's a good target? I mean, we get into a conversation with the family office, or we get into a room to talk out to an event, and most of the people in the room are like, "I'm not a good target. No one knows who I am, I'm not that wealthy." All these reasons, all these deflections as to why they're good. The reality is, everybody's a great target. Everybody's got a bank account, everybody's got information, social media, like we talked about, everyone's extortable. The reality is, is it $1,000, or is it $10 million that are being extorted for?

And the bad guys are looking for a volume game, they can go buy your data, and this speaks to your question, they can go buy your data online in the dark web, and go after 1,000 families with a campaign in a matter of minutes, because it's all automated. And so all they really need to do is hit a small percentage of those, and be successful to further the criminal enterprise. So back to what can you do to reduce your value as a potential target, that's reduce what information is available about you online. Because if I can't find you as a bad guy, if I can't put eyes on you digitally or physically, it's really hard to attack you. And that was something that we used at the agency all the time. You can't find the target, you really can't harm them.

And we loved that. We ran around undercover of darkness with deception, and stealth, and it made us really quite invincible to bad guys overseas, et cetera. Digitally, it's a lot harder to do that. These devices are always pinging, you're always online, there's always a presence. So I think the challenge there is, how can you be the least visible target? And that means you've got to reduce your online profile. So that's the answer to your question. Reducing the online profile, all the data about you that's out there online makes you less accessible digitally. And if I can't find where you live, I can't find where your children go to school, I can't find out where you go to work, it's a whole lot harder for me to harm you. And so that's where this attack cycle...

What I used to talk about back in the agency 30 years ago was, there was 11 steps of how bad guys figured out how to hurt you. And they would go from, "I need to pick a target. I need to go find the target's house. I need to go find the target's office. I need to go figure out where the attack site should be. What do I need to bring to the attack to be successful? Is it weapons? Is it explosives? Is it a vehicle? What is it? Is there deception needed to make the attack successful? Then I need to practice,

then I need to deploy." So think about an assassination attempt, all these things have to happen. And we learned back in the '90s that it took bad guys 21 days to carry out a successful attack, days.

So if we could interrupt that 21 days, we were doing a good job to making it harder for the bad guys to attack us. What I put forward now is that it's more like 21 minutes from a digital perspective. And so how do you disrupt that in 21 minutes? And there's no empirical data on that, but the reality is, it's gone from days to minutes, it could actually be seconds with AI, and that's going to get really ugly when that happens.

But you've got to get all that publicly available data about you reduced. And it's not a silver bullet, it's not a one-time thing to get it done, you've got to spend effort, and work with all these data aggregators that are collecting all this information on you, for marketing purposes, for banking purposes, for social media purposes. You've got to get all that information reduced. And so it's a quarterly regular process to knock all that down. Only then are you going to be seen as a less attractive target. If you're out there doing it all, anybody can go after you.

Jen Zegel:

So does Red Five Security help scrub data from the internet about people?

Kris Coleman:

Yeah, so what we do is, we work with clients, they sign up for a subscription with us called Web Scrub. And what we do is, we go in, and we find all their data that's available on data aggregators, and then through a professional legal process, we used a variety of tools, and with their approval, we go through and we take all that data down. Sometimes we have to get their signature, and sometimes we have to work through this process. But think about this, none of them really work the same way. So it's this arduous, menial task to go through hundreds of data aggregators, and take all your data down. So we have a process that does that, it's an annual subscription that renews. But every quarter, we have to go in and knock it back down, because the internet is built to be resilient.

All those DNS servers on the internet want to refresh every few months, because we never want to have downtime on the internet, we always want to be able to find every piece of data we always want. So those DNS servers are constantly recreating themselves. And so what does it become? It becomes a game of whack-a-mole, like, "How do we keep this data down?" So once you start that process of taking the data down, then you want to also change the behavior of the family, or the company, or the executive, to stop sharing. Reduce that propagation of personal data out into the internet.

And we overshare all the time, every day. People sign all kinds of agreements by the click of a box, and say yes to share my data with whomever. So can you get to the other end of the spectrum where there's nothing out there? That's really, really hard to do. But it's kind of like the old adage, do you have to outrun the bear? No, you just have to outrun your buddy who's running slower than you are. So you want to be the harder target, you don't want to be a soft target.

Justin Brown:

So when I heard you speak before, I heard what you were saying, and I made a conscious effort to reduce my digital footprint in social media, for example. So if you're traveling, don't check in from the airport to say, "Hey, I'm in Italy." So now everybody knows that you're not at home, and they can go into your house. Or not putting personal information posted, or pictures posted, or whatever. But the problem that I have, and I've run into is, my ID is on my website for my firm. My bio is on my website, or I have a LinkedIn profile, or we do this podcast, and our information is out there. So from a realistic perspective, if we want to protect our identities, how do we do that if we are professionals, and we are trying to build our networks through a social presence?

Kris Coleman:

Tough question. So we get this a lot of times from professional athletes, we get this from entertainers, that their whole goal is to go the other way, maximum exposure. So it's, where do you want to land on the spectrum? So other clients have come to us, and said, "Listen, I give up. I'm out there, I'm a known..." perhaps founding CEO that sold their company. This is a client speaking, "I am agreeing to protect the crown jewels, but I am going to sort of give up land in order to focus on protecting the

crown jewels. So I'm going to understand they're going to attack my company website, and I'm going to be available as far as a persona out there as a company on websites, and podcasts."

All that data is just going to be out there and it's part of the noise, but they're going to commit to keeping social security numbers, dates of birth, photos of the children, corporate documents. They've sort of dug this mode around what is the most protectable asset. And that's another way to look at this, it's risk management, is what we're talking about. It's, "What are we going to commit to to protecting, and what are we going to say, 'Hey, I know I'm out there.'" And I think, I'll just say this from my perspective, I wasn't out there at all on purpose for many, many years, and in some instances, I was undercover. And so I was not out there at all for many years for other professional reasons. But once I became the owner of the company, I still stayed under the radar for another 10 years, and then it was like, "It's time to be out there, I have to promote the business. I have to take some reasonable actions from a marketing perspective."

And we all still want to be social, so it's somewhere on that spectrum of being out there on social media, being connected digitally. There's some other best practices, yeah, you don't want to post that you're in Italy, but wait a week, 'cause that might be the procedure you use, as opposed to, "Don't ever post that you went out." No, wait a week before you say, "Hi, I was in Italy." Was. "It was a great time, here are my pictures. These are the people with me." Blah, blah, blah. But now you're not exposing the residents 'cause you're out of country, and everything is delayed. 'Cause it's the real-time sharing that becomes a physical vulnerability too.

We had a family come to us and say, "We can't figure out why the paparazzi always know where we are going to land." The family lands in Cabo, and there's 100 paparazzi at the airport. And the protective detail was calling me, and going, "Help us figure this out. We've locked down the boss's phone, we've locked down the website, we've locked down the tracking of the tail number, we changed tail numbers." I'm like, "Have you checked the daughter's social media?" And they were like, "Oh, no." And it was all out there, "Ready to go sport fishing, ready to go horseback riding." Whatever it is, they knew. 'Cause the paparazzi, being the bad guys, were using intelligence collection, and the attack cycle to figure out where they wanted to be to shoot the photos. And that's kind of the challenge. So you've got to find where you are comfortable on that spectrum of sharing, and make sure that it doesn't incur some kind of a risk.

And I think that leads to the question about convergence, and I think I talked a little bit about that at the event in June, which is, how does the digital matchup with the physical? So, "Oh, we're being attacked on cyber." Okay, great, but is that really a cyber vulnerability, or is it a physical vulnerability?" We've had crypto CEOs come to us, and they're like, "I had people banging on my door last night at the hotel, and I have no idea how they knew I was there." I'm like, "Did you post anything?"

"Oh yeah, I did say I'm excited to stay at this hotel again." I'm like, "Well, they're monitoring you, you gave it up, you told them in the attack cycle where you're going to be, where you're going to be predictable, and where you would be vulnerable. So it's no surprise to me they banging on your hotel door last night."

So there's this element of convergence, where the physical and the digital converge. And so we see all the time that it's not necessarily a cyber threat, "Oh, I got this thing on my phone." Okay, the thing on your phone may be to steal info, but it may be just pinging back to the bad guy, telling them where your phone is, so that they can show up, and kidnap you. Other things arise over the course of collecting data on clients.

We had a client come to us and say, "No one knows who I am, so they're really not going to find any data on me, but I'd like you to test it, and let me know what you find." Literally within a week we came back, and it was probably sooner than that, but we took some time to aggregate it, I'm like, "I know where you live. I know where you work. I know where your kids go to school. I know where you practice your faith. I know where you go to coffee in the morning. I know whether you're a Starbucks person or a Dunkin' person. And, oh, by the way, I know where your kids stand at the bus stop." And he was like, "Whoa, that last one, now you've got my attention."

He's like, "How did you figure that out?" I said, "Well, have you looked at the PTA website for your school?" He was like, "No. Why?" He's like, "Well, there are photos."

"We know what your kids look like, 'cause there are photos of your children on the internet. We've matched it up, but what's on the PTA's website? And, oh, by the way, there's a street sign in the photograph on the PTA website, and their kids are waiting for school." And we just had somebody drive by, "Oh yeah, they're standing there." And so it's an intelligence approach to the attack cycle that people underestimate. What's in the background of photos? What are the other third-parties

sharing? The PTA groups, the faith groups, the non-profits that you're involved in, what are they sharing? What's being put out there? Because it's all aggregatable into the attack cycle, to understand where to go after you, both digitally and physically.

These devices are tracking devices. Turn on the microphone, you can turn on the tracker, you can turn on the camera remotely, it's all very doable by the bad guys. Those are tremendous vulnerabilities. And I'm not saying these are threats that the common person needs to worry about, but we don't have a good understanding as a population of how vulnerable we've made ourselves by carrying devices everywhere we go.

Justin Brown:

So let's talk a second about how we are unaware of how vulnerable we are, but probably because a lot of us feel like we're not targets. I'm not a CEO, I'm not flying around the world in my jet, so nobody's coming after me. What do you think we, as estate planners, need to be aware of with our clients who may not be these ultra-high-net-worth individuals? What should we, as estate planners, be thinking about, and telling our clients to put this on their radar?

Kris Coleman:

Yeah, and I think that's true, the intent is not to terrify everybody, it's trying to wake people up to the vulnerabilities. So there's threats, and there's vulnerabilities, and there's risk. And if you have no threat, even though you're vulnerable, you still have risk. It's just not high-risk, necessarily. Now, to your point, you're not traveling the world on a private jet, but where you're recently overseas on vacation? That's a new environment, that's a new threat environment. So while you may feel really comfortable here, like, "No one's going to threaten me here in the United States. I'm not well-known, I'm not controversial." Et cetera, et cetera, et cetera. But you, as an affluent middle class or upper class American, flying to Europe, or flying to South America on vacation, you are now in their territory. And what everybody goes back to, to your point, you don't know the threat environment in those foreign environments.

You may be a fantastic target in that foreign environment, but you have to change your mindset, like, "I'm going to that environment. It's not what I used to experience going around Northern Virginia, or California, or anywhere in The U.S." Their laws are different, their law enforcement is different, their intelligence agencies operate with pretty much free will in some of those environments. So they're going to collect. They may be into corruption, they may be into some kind of a malicious attack on an American that happens to be in their country at the time. So that's just a travel thing we have to think about. As a gatekeeper, now estate planning counsel, legal advice, wealth management, these sorts of adjacent advisors to affluent families, family offices, corporations even, and foundations, you're the gatekeeper. So if they plant something in your devices, they get involved with malicious software in your devices, whether it's your computer network, or your phone, or your device, you're unwittingly sharing information with the bad guys via your device, because you're the gatekeeper. You're the communication channel. That's what you've got to be worried about.

So your corporate network at your law firm, your corporate network at wealth management site, what's your device policy? Your mobile device management system, what's that in place? Are you bringing your own personal devices to work, or are you using a corporate device that may have a lot more protections on it? And I think that's a thing to think about as a gatekeeper. Those clients, mostly affluent clients, family office clients, they're great targets, because they are not spending what's needed commensurate to the threat. They're not investing into protections in a way that's commensurate with a threat. Threats are agile, they are forward-leaning, they're going to go after these assets, they're going to get into those computer systems, and try to get into the digital banking systems.

We get calls on a regular basis, "I just sent a million dollars to somebody, I have no idea who they are." I'm like, "How'd they do that?"

"Well, we just clicked on the email, and off it went." As a gatekeeper, you need better protections on your systems, you need access controls on your systems, you're going to need a variety of protections, and each will be different depending on the situation, and the operating system, and things like that. But you're going to need air gaps between some of these financial decisions, in these financial transactional systems. So how do you stop from accidentally sending a million dollars to a terrorist group in Africa? You need to stop what you're doing, slow down, double-check that that email is actually from a client, double-check that the amounts and the banking information are all correct. Stop what you're doing, walk down the hallway.

There are different communications medium, face-to-face would be good. "Did you actually ask me to do this? Is this approved?"

'Cause what you don't want to do is just do all this by email. There's no real way to fare it out, the spoofing, the phishing attacks, all those kinds of things, because they're getting so sophisticated. AI is now really taking off, bad guys are using it on a regular basis. The phishing emails that are coming in now look just like real emails from that vendor. The logos are right, the text is right, they're personalizing the email the way you usually speak to that person, because they've been paying attention to what's going on.

So I think there's a real element here that begs for an analog air gap. Find another way to pick up the phone, not in email, not in text, not in digital. Call that client, and say, "Do you want me to do this?" Frankly, that should be a quality management piece for you to tell your clients that you do it this way. They should be asking you to do it that way in some fashion. Go analog if you have to. I know it slows things down, but I would much rather be 30 minutes slower than a million dollars out. It's a very expensive mistake.

Justin Brown:

So we had an episode on biometrics a little while back, and how our biometric information can be unknowingly given to third-parties, or it may get sold to third-parties. And I guess a question would be, as AI grows, and the ability to scrub the internet for our biometrics increases, how can we really protect ourselves from giving up, or having our biometric information stolen, so that we can do these phone calls to confirm that this is truly what the client wants? And taking that step back, and slowing down before we just automatically get the systems moving so that money transfers, and we have the security protocols in place?

Kris Coleman:

Biometrics is going to get more and more difficult, and it's probably going to be jumped right over straight to deepfakes, whether it's audio, or video, or whatever it is. It may not even be a biometric issue. This is the danger of podcasts, this is the danger of webinars. So now we've got me out there talking, we've got all of us talking, the voice patterns are out there, the visuals are out there. You've seen, I think they call it Congress to Order with a deepfake audio, this last time around this summer, and no one could tell the difference. And I think that's what's scary, is that we're going to have to find ways to detect these fakes, audio, video, whatever, and filter them out.

And I think that that's probably a big piece of the future here is... I mean, 'cause some of the devices that use biometrics, they're not actually collecting biometric data. They take a snapshot of what they see, whether it's a fingerprint or a face, and they turn it into a number string, some kind of combination of numbers, and then they use that combination of numbers to compare to what... For instance, the biometric lock, it doesn't take your fingerprint and store a fingerprint, it stores a number that's assigned to that picture of your fingerprint, and then tries to match that number to an access control list. So it depends on really what's being collected, and in what capacity. But I think when you say, "Oh, someone's collected the biometrics of my face." That may be true, but my guess is that biometric may or may not be that valuable if they're going straight to deepfake video, where it's not the biometric that's valuable, it's the ability to project your face telling someone to do something that promotes the criminal enterprise.

So those I think are maybe the challenges of biometrics going forward. It's hard to say where we're going to be in a year, or two years, or three years, but coming up in the election cycle, I think we can all stand by for a lot of chaos.

Ross Bruch:

How is Red Five staying on top of this? I assume that you still have a lot of great contacts within The U.S. government, and are learning from them, and also probably teaching them, but with criminal enterprises moving so quickly, being so advanced, what methods of education are out there for companies like yours to try to stay one step ahead?

Kris Coleman:

Well, the good news is, we've learned from the attacks that happen on others, and we are very well-networked into our industry. A security firm was just hit recently, and there was a challenge there, and we're like, "Man, we don't ever want that to happen to us, nor to happen to our clients." And if a security company can get hit, practice what you preach. So we really are trying to double down on that, and we think we've got good protection. So I think the challenge becomes trying to stay one step ahead of the bad guys. They only have to be right once, we have to be right 1,000 times an hour, or 10,000 times a day. And that's sort of the challenge with our cyber experts is, how do we non-stop fend off all these attacks?

So it's one thing if a group comes in and we attacked you 200 times today, we changed the email slightly so that you wouldn't detect it, or we used a different approach to the language, or came at you from a different ISP so that you wouldn't detect us as a bad guy. And AI can do that thousands of times a second, so how does the defense keep up with that malicious offense? And I think that's the challenge going ahead, is using those AI powers for good to stay ahead of the bad guy. It's going to get crazy. There's no doubt about it. The network we have is robust. We don't have access to government information anymore, so we're not really going down that path, but the stuff that does get published, we learn from on a regular basis.

And then we try to use all that, learn knowledge over the last period of time to assess how our clients are today, but most of our clients aren't worried about the cutting-edge top 5% of attacks, they're worried about, "We haven't updated our IT in 10 years." And you're like, "Oh my gosh, we've got to spend some effort here. We've got to get you caught up so that you, you're mostly protected." And that's a probability game. So it's risk management, how likely are they to be hit? What are the consequences going to be if they do get hit? But for family offices, it is a constant battle to get them upgraded, 'cause they don't want to spend the money, they don't see themselves as a target. They are always a great target.

Corporations, they have, in some instances, a fiscal responsibility, fiduciary responsibility. And now we're getting into the SEC saying you have to have a cyber person on your board for a publicly-traded company. Those are great steps forward. And if it's a privately held company, you don't have that kind of requirement. But private companies need to be thinking that way, "What kind of expertise am I bringing to bear to protect this enterprise?" And that's what we think about on a daily basis.

Ross Bruch:

So you mentioned practicing what you preach, if I can ask some personal questions about your methods, I'm going to guess that you routinely scrub your online profile, that you keep your online profile beyond the business to a minimum. I'm going to guess that, especially when traveling overseas, but maybe even the United States, you are not joining public wifis?

Kris Coleman:

So, yes, I try to practice exactly what we preach for aggregation of data aggregators. I really try to stay low-profile in that mix. All my social media stuff is set pretty tight. Some of it needs to be seen for business reasons. But yes, I mean, even domestically, I never connect to public wifi, ever.

Ross Bruch:

And dual-factor authentication on everything of importance?

Kris Coleman:

Absolutely everything, yeah. And if I can go more than two, multi-factor, yes, absolutely. And then there's the availability of data. So in a corporation for example, do you really need those financial records from 10 years ago to be available digitally? Take them offline. Keep them digital, don't keep paper around, recycle that stuff, but you need to think about data in a way that's, "What needs to be readily accessible? What needs to be less available? So I can still get to it if I need it, but we're locking it down with multi-factor, just like we would do with the daily stuff." But then you get to, "What needs to be archived and offline? And then what's being transmitted on a daily basis?"

So daily communications of business, we try to do stuff on secure apps, or in our own secure environment for communications. We do very little business-wise in an open text, almost zero, and our email is encrypted. But then you get into, like you said, those archive datasets, there's no need for them to be sitting on an open drive that could be attacked and

creating that kind of exposure. So take stuff offline, put it in a hard drive, put it in a safe. You just don't need it connected anywhere. And that's sort of always been that interesting angle for clients is... They come to me, and they go, "I want to come offline. I want to completely drop off the grid." I'm like, "Okay, let's talk about what that means."

And so then stepping them through the lifestyle changes that need to happen, the legal stuff that needs to happen, the digital communication stuff that has to happen, that gets to be a very interesting conversation. But back to the proper practices when traveling, never on public wifi, period. If I have to go connect from a laptop to an internet environment, I'll go tether through a device that I trust, and not go through a public wifi, for sure. There's too many middleman attacks that can happen with wifi.

Jen Zegel:

Do you think VPNs on cell phones... What kind of extra layer of protection does that truly provide?

Kris Coleman:

This is where I would defer to a true technician that would get into your specific instance for that OS, what kind of enterprise do you have set up for your company? VPNs do provide some level of protection. So it's an encrypted tunnel through which you are connecting to devices, and I think that makes a lot of sense. We use them at the company, and some instances, companies have set up, you have to use them, and it's just that extra layer of an encrypted tunnel. So I'm a fan of them, I think it's a good idea. How they are employed in a very specific instance for a very specific company depends on their environment, and their threat level.

But we've often advised clients, "Hey, this is a good instance where you should use a VPN. It makes a lot of sense." Anything that makes it harder for them to find you, right back to that concept that we talked about earlier... VPN harder to find that data flowing around in the wifi, it's going through a specific tunnel, and ideally, it's encrypted even within the tunnel. So I think there's a lot of benefits to a VPN.

Justin Brown:

One of the things that you had mentioned before, Kris, is that we are targets, and it's a matter of what the risk is for us as targets. And we may have very high-net-worth clients, who may have security systems that are quite secure, but we may be the backdoor into our clients. And it got me thinking that not only am I a potential backdoor, but any of my employees are potential backdoors, if they're a backdoor to me. What should we be telling our employees who are potential targets indirectly to get to our high-net-worth clients?

Kris Coleman:

The human being is the weakest link. They can spoof us, they can influence us to make decisions, to click on things, to open up and share information we shouldn't. So the human being, the human engineering, the social engineering that goes after targeting people in that proper position is really... That's the weakest link. And I hate to sound like the TV show, that is truly the weakest link. And it's about training for those human beings, it's about awareness, setting them up to understand where the vulnerabilities are, what they should and shouldn't do, to identify things that are happening around them that might indicate there's some kind of an approach going on. So I think all of those are really important.

And you think, "Well, I don't understand how this works. How do you target a human being, and then end up getting access to a family office, or some other kind of wealth management system, things like that?" Well, everyone has got passwords, so let's talk about passwords. You pick your passwords, passwords could be very weak. You may use the same password across 10 different systems. Okay, they haven't figured out yours yet, but they broke into your iPhone, and they know your Apple password. And oh, by the way, you use the same thing on your office login. So they just try that. And there's dozens of instances where people are reusing passwords on sensitive systems. So once the bad guys break into one, they just go use it on your bank account, next thing you know, they're in your bank. So there's elements of passwords and humans that is fallible, weaker than it needs to be.

But then there's elements about now they've gotten into your system. So let's say they attacked your system, they're in your network, they're smart, they're going to wait, and they see that you're sending invoices to the family office for your financial

services. Well, all they do is, they embed malware in a PDF, that looks like your invoice, and then you send the invoice off to the client, and they're like, "Yeah, it goes every month. This is who they send it to." They're watching all this inside your network. And then they decide this next time around, they're going to shoot their invoice a day before you send yours. It lands, they process your invoice, and they open the PDF of the bad guy's invoice, and now that malware is implanted on the client's network. So you've been the Trojan horse, to go from the financial services, straight into the family office network, and now the family office, "Oh, this is an invoice from Acme Financial. We love them, we trust them, they're great." Open up the invoice. Now they're in.

And now, eight months later, they've been in that system, and cranking away. What they usually say is eight months is the duration of a breach until it's detected. So the thinking there is, "What's happened in the last eight months? Have you sent any sensitive emails? Has there been an investment? Have we talked about intellectual property? Is there a lawsuit going on?" All that data has probably been listened to, probably been exported out to the bad guy. Now all that dirty laundry is available to the public. So that's the challenge. So you're looking back, and going, "If it takes eight months to detect a breach..." Because your friend found out that your Facebook account was hacked, it took them eight months to figure that out, but we're talking corporate, corporate breaches, I mean, that's the average time. And so what's happened that was sensitive in that eight months? You have to think about that when you think about the risk.

So you've sent the invoice, it's got the malware, it lands on the family office. Eight months later, they figure out, because they had a sweep done, or they had a vendor come in and do an IT check, and they're like, "You've got something going on in here." Now, they look back and go, "Well, who was responsible for that? Was it the person that opened the PDF, or was it the vendor that sent them the invoice that was already tainted?" So I think there's a lot of challenges here as a gatekeeper, that you really have to dial stuff in, and making sure that things that go are official, and not something going on in your own network.

And that's a real case that happened. It wasn't a financial firm, it was a vendor for a client of ours. And our client though, had a great cyber system, and they're like, "Whoa, whoa, whoa. This is a weird one. This PDF has got something in it." And they caught it, at the machine where it landed, but the reality was, that vendor did not spend the money, did not invest to protect its infrastructure the way it should have, because it had access to that kind of a really lucrative client.

Jen Zegel:

If lay individual finds that they are a victim of a cyber attack, what are best practices that we should be guiding them to take?

Kris Coleman:

Wow. Well, first thing is, you've got to lock down all the passwords, you got to change all your passwords. You need to deal with two-factor on everything. Sort of stop the bleeding, is the first thing. Look at all your passwords writ large, your bank accounts, your social media, your email accounts. Is there an email account out there you haven't looked at in 10 years? We've got clients that come in when we do these online exposure review. And we go in, and we look, and say, "You have 152 accounts out there online. We found all of them. Did your Facebook is still in use? Your MySpace account is still in use? You haven't shut down any of that stuff." So when you think about, "What do I need to lock down after an attack?" Or what you think is an attack, it's looking at all those accounts. Changing all the passwords, going to two-factor, and then you have to start figuring out how they got in.

But the first thing is to lock everything down. That's got to be step one. Some of the attacks that are happening now are... 'Cause everyone's like, "Oh, I've got two factor on my phone, so I'm good." But what's happening now in some cases is, they're coming in and they're actually going to your phone provider, and saying, "Oh, I need a new SIM card for my phone." And they're like, "Oh, well, okay, well, can you give me the cell number?" Of course they know the cell number, that's out there. And they impersonate the owner of the phone, the provider coughs up a new SIM card or SIM device, and so next thing you know, they're now owning your phone. They have a phone, an iPhone, that's got a new SIM in it that is supposed to be yours, 'cause the provider provided it, and now all your two-factor codes are coming to their cloned phone.

And so you no longer have two-factor, you no longer have actual protection on the account. Now they've jumped in and they own that account, and now they're jumping from account to account. So that concept of locking everything down as soon as you can, changing the passwords, making sure 2FA in place. The safer option is to use one of the apps on the phone that generates a digital number. It's not being transmitted through an SMS message. So one of those apps, you get into an

authenticator app, it's a digital authenticator app. Google has one, there are other ones out there for different applications. Some of the password managers have their own. But now it's happening inside software, and not coming through the SIM card, through an SMS. And so that's the next level of protection there. And even better, have it sent through your email. A trusted email receiving that code is even, in some cases, better than that authentication app.

Jen Zegel

Kris, what can people do today to better protect themselves from becoming victims of cybersecurity attacks?

Kris Coleman:

That's a great question. A lot of clients are stuck, right? They don't know where to start. They're like, "Am I a victim? Will I be a victim?" I don't know. But that's the question, where do you start today? And so how we approach this is we tell them, "Hey, start with a resilient mindset. Be ready to be attacked in cyber. Know that you're going to be hit." People get hit all the time. So just know that it's a likelihood. And so you have a resilient mindset, be ready for that kind of thing, and then know you're going to work through it. So the top three things you can do is remove your information from data aggregators on a regular basis, reduce that public profile, get your information down, don't be as available as the next person. Remove your information data aggregators on an ongoing basis.

Next thing is have a cyber privacy security assessment done. Have an assessment done of your residents, have an assessment done of your corporate network. Look at the home networks, the corporate networks. See what's in there, right? Make sure you're not vulnerable today. Just double check. And if you've got a great system, awesome, you can't worry about it anymore. But you may find old software, software that's not been patched, old devices on your network that are vulnerable. Do that cyber privacy security checkup. Know what you don't know, understand that.

And then lastly, practice good cyber hygiene, practice good practices for privacy and security, both at home and while traveling. We talked about going overseas, it's a different threat environment. Same thing at home, right? You need to be making the right choices about online sharing on your devices and your social media. If you do those three things, reduce your information on data aggregators, you do a cyber assessment, understand where you're vulnerable, and then you practice good cyber hygiene and security practices, you're going to be in a much better place, and you can start all those today.

Ross Bruch:

Well, that is absolutely terrifying. So with our last question, let's turn the subject ever so slightly. You wrote a book called Raise Your Resiliency. Can you tell us about the inspiration for that book, and what readers should get out of it?

Kris Coleman:

Yeah, absolutely. The inspiration was, I've done so much now for 30 plus years, and the first 14 of that being working with some of the world's best intelligence and law enforcement agencies, and so I was the beneficiary of a ton of great training, and then a ton of experiences around the world that said, "Learn from this, learn from that." And these are operating both in foreign environments, austere environments, non-permissive, dangerous environments. And now I've been around these colleagues for so many years, I'm like, "I want to apply these things, these tactics, if you will, to my daily life. I want to be more resilient. I want to be more prepared. I want to be self-sufficient." And so we, I mean, me and my colleagues, we talk like, "Oh yeah, I've got this. I've got this. My vehicle. I've got this. I'm always ready. I've got water. I've got food." All this kind of stuff.

We were trained to do that. Wherever you're going to go, you had these things. You had an ability to defend yourself, you had food, you had water, you had shelter, you had good intelligence, you had good comms, you had a plan. But people don't usually apply those in their daily lives. And as we got into the pandemic, I'm like, "It's a good time here to share some of that." And so I talked to a lot of my colleagues, former Green Beret in the Army, a former agency ground branch officer, getting into some of the other military... SEALs, and getting into Air Force Special Forces, getting into a whole variety of different groups, both law enforcement, and military, and intelligence, and saying, "What are best practices? What do you keep in your vehicle? What should be in your home in case something goes bad?"

We hear stuff from FEMA, "Oh, you need 72 hours of water, or 24 hours of food, and a bunch of batteries." What we found out during COVID, and what we found out during other major natural disasters is, 72 hours is nothing. And there is no real good way to support the population in the United States in all these different environments with multiple disasters going on simultaneously. Look at Katrina, look at Superstorm Sandy, so look at the wildfires out West, tornadoes hitting the Midwest United States, it goes on and on. And are Americans ready? Are we, as a population, resilient? And if you look at Israel, you look at Switzerland, look at some of these other environments where it's in their nature, it's in their culture to be resilient, we're that way some in the West, like the pioneering Americans that went West, some of that's still in their culture, and people living on the land, working farmers, and folks like that, they have it every day. They're carrying weapons, are dealing with austere environments out in the wilderness.

I think there's a variety of things that we need to bring back to the American family, and that's why the book was written. So it's tied to individuals, it's tied to families, and it's tied to businesses. And there are good, solid check lists from these experts I talked about, that have contributed to these checklists, like, "This is what this person keeps in their vehicle, this is what this person keeps in their home. This is how you deal with an elderly parent if you're trying to move them from point A to point B. How do you deal with pets?" I mean, it's the whole spectrum. So it's an element of understand where you're vulnerable, make sure you put the right preparations in place, practice what you've put in place, 'cause it may not work.

When I say practice, I mean test it. So people are like, "Oh, well, I've got all this stuff, and I'm good to go." Well, I understand you have this apparatus in your house, but it won't work without power. And so does your generator actually handle all those requirements you've put inside your house? Or will your generator only handle the refrigerator 'cause pulling a lot of amps? And so I think there's an element there of, understand it, get prepared, practice it, test it, and have in place what you need. But it's really five things is what I put out in the book. So it's awareness, raise your awareness to what's going on, understand where you're vulnerable, understand what's going on in your neighborhood. Mindset, so you need to have a positive growth mindset. You get a cyber attack, are you going to curl up in the corner, and say, "It's over." Are you going to bounce back, deal with it, push through the problem?

Same thing with an illness, a bankruptcy, anything else, talking about business, talking about family. Then you get into fitness. And that can be not only physical fitness, it needs to be emotional fitness. It needs to be mental fitness. Are you flexible? Do you have endurance, from a fiscal perspective, on your company? Can you work through the fiscal challenges? So there's awareness, a mindset, and a fitness element to resilience. And then there's skills. Do you have the skills? Can you start a fire without a set of matches or a lighter? Can you find and filter water? How do you build a shelter when the tornadoes hit? I mean, it's kind of dark thinking, but I would much rather be prepared than not. And will you need this on a daily basis? I can't imagine you would, but we're seeing Americans challenged every day with natural disasters.

And then you get into the last pillar, which is relationships. No one got to where we are today in any level of success without someone else helping us. It could be a mentor, family member, it could be friends, it could be a business partner, it could be anybody, spouse, partner, whatever it is. So what I put forward in the book was that there's five pillars of resilience, awareness, mindset, fitness, skills, and relationships. And if you apply those to the family, the individual, and the business, you're really going to become a success. In some capacity, you'll achieve what you want to achieve. So five pillars, three critical units, and then you can achieve the one goal, which is to be successful. And it's sort of a self-help on steroids, that's kind of the thinking, was to help everybody be a little more resilient.

Jen Zegel:

Kris, you have truly painted a very scary picture, and I'm sure a lot of our listeners are going to want to learn more about you, about your company, and your book, of course. How can they get in touch with you? Where can they find you?

Kris Coleman:

So our website is out there, and it's www.red5security.com, that's red5security.com. And that's the best way to find us. We're on LinkedIn if you also want get to us that way. I'm out there speaking on a regular basis, so hopefully I can see folks out there. That's the easiest way to get ahold of us, and we're happy to respond to inquiries or challenges. And I'm having big been a former instructor in those organizations, I'm really big on education. And so I thank you guys for having me on today, and hopefully, if someone listens to this, they can take a couple of steps to be more secure.

Jen Zegel:

Well, Kris, on behalf of Justin, Ross and myself, thank you so much for joining us today. Thank you for scaring us and sharing your knowledge and expertise to help guide us and our listeners through the realities of cybersecurity threats. I mean, in the digital age, knowledge is really our best defense. So thank you to our listeners for tuning into this episode of the Digital Planning Podcast. Until next time, stay secure.