CADENCE Bank

Cadence Bank Podcast: In Good Companies

Season 2 Episode 4: Gone Phishing: Approaches to Cyberthreats

Are you doing enough to protect your business from cyberthreat? With cyberattacks at an all-time high, you may not be as prepared as you need to be. You might even think your business is too small to be targeted, but think again: the Verizon Data Breach Investigation Report states that 43% of online attacks are now aimed at small businesses. Cyberattacks are also expensive – according to the FBI's Internet Crime Report, the cost of cybercrime against small businesses totalled $2.4 billion in 2021 alone. So when you're surrounded by bad actors, what can you do to protect yourself?

Fortunately for all of us, there are people out there like Cadence Bank's Chief Information Officer Kevin McMahon and Brendan Monaghan, Senior Producer with Cadence Insurance. Brendan and Kevin both keep up to date with the latest cyberthreats and have some simple approaches they recommend for protecting your business. On this episode you'll learn what common cyberattacks might look like, their most frequent targets and what to do if you have an incident. Plus, we'll cover how to transfer your risk with the fast-evolving segment of cyber insurance.

So join the cyberthreat triple threat – Kevin, Brendan and Patrick – and together we'll brave the phishy waters of cybercrime.

Episode Transcript:

[00:00:00] **Patrick Pacheco:** Do you know how many producers it takes to change a light bulb, Brendan?

[00:00:02] **Brendan Monaghan:** Less than the number of lawyers.

[00:00:04] **Patrick Pacheco:** Zero. They tell the CSRs to do it. Client service reps.

[00:00:11] **Kevin McMahon:** The FBI put a bulletin out recently. They cited $43 billion lost in a little over five years in business email compromise. That should be an eye-popping number that that kind of an industry can pop up around just stealing email addresses.

[00:00:30] **Patrick Pacheco:** I'm Patrick Pacheco, and you're listening to Season Two of *In Good Companies* from Cadence Bank, the podcast we guide you through the forces shaping your business—inside and out.

[00:00:40] **Patrick VO:** Sound the alarms! Defcon 1! Intruder alert! Threat level red! With cyberthreats at an all time high, this is probably how businesses should be acting. But many just aren't fully aware of the danger. However, ignorance won't protect you. In fact, just the opposite. And the results for your business and reputation could be catastrophic. So, on this episode, we're giving you the guidance you need. Together, we'll cover what cyberattacks look like, how to safeguard your employees and what to do if the worst happens. Because bad actors aren't just in your kid's middle school play. They're all around us.

Thankfully, there are also people out there equally dedicated to protecting businesses.

[00:01:31] **Kevin McMahon:** I'm Kevin McMahon. I'm the Chief Information Officer for Cadence Bank.

[00:01:36] **Brendan Monaghan:** Hi, I'm Brendan Monaghan. I'm a senior producer with Cadence Insurance.

[00:01:42] **Patrick VO:** Kevin and Brendan both work with cyberthreats on a daily basis, but they come at it from different angles.

[00:01:50] **Brendan Monaghan:** In my role, the first thing that I do is engage with clients and on their cyber risk from their perspective and the perspective of their business. And after understanding that risk work in partnership with them on developing a risk management program and transferring that risk of cyber to the insurance marketplace. And once we have that risk transferred, then if—and more often now than it used to be, *when*—they had that cyber incident, working in partnership with them and the insurance company and those third parties that facilitate the incident response process to make sure that we mitigate the ultimate impact of that cyber incident.

[00:02:27] Kevin McMahon: It’s interesting, Brendan used the term risk. I actually approach it with the same terminology for every area that I work in; it's about mitigating the risk of security issues, incidents, vulnerabilities, whatever our exposures are. For me, I'm doing that from a technology point of view. How do I implement the pieces that reduce that risk or keep us safer?

[00:02:53] Patrick Pacheco: So that our listeners can level-set this. When we talk about cyber threat, what are we talking about?

[00:02:59] Kevin McMahon: I think when the phrase first got coined, the idea of cyber threat was either a virus or some weird image of a hacker trying to do something on a computer. Nowadays it's a lot more complicated than that. It's going to be any electronic or digital interaction that you have to do business. And to some extent even personal activity, whether that's financial or emails or wherever you have stuff that's in an electronic form, is open to being attacked. And all of that has now fallen into the category of a cyber attack. I'd say it even has blurred a little bit beyond that where there's this concept of social engineering to make cyber attack more effective. So let's talk somebody into giving me a piece of information that I can use to exploit something online that's not always electronic, it usually is, but it's a lot more sophisticated and it's come a lot further than those early definitions of a couple of different computer views of it.

> [00:04:08] Patrick VO: The threats haven't just grown in complexity--they've also grown in number.

[00:04:12] Brendan Monaghan: When it comes to statistics on the specific numbers, that's very difficult to pin down because many businesses haven't reported these incidences because of that reputational risk concern. So one sort of good gauge that you can use is how often are these events appearing in the media? And I think from that perspective, we're seeing the numbers increase dramatically in how often we are hearing of these events. The frequency is definitely increasing substantially. The number of incidents, the forms that these incidents are taking, the ingenuity and entrepreneurial approaches that some of these threat actors are coming at this from is always keeping us on our toes. But yes, the frequency is definitely more present today than it ever has been in the past.

[00:05:00] **Patrick VO:** And the consequences of a cyberattack are costly.

[00:05:03] **Kevin McMahon:** One thing we can pull though is some government statistics. Any good search out there will give you some statistics from multiple publications or security companies, but one example, the FBI put a bulletin out recently specific to business email compromise, which maybe we'll talk about in a little bit. They cited $43 billion lost in a little over five years in business email compromise. And that should be an eye-popping number that that kind of an industry can pop up around just stealing email addresses. According to, I think it was the Verizon data breach report, the vast majority of these are coming from some form of organized crime. So I think that number was over 80%.

[00:05:39] **Patrick VO:** Bad actors aren't just going after your money. So what other threats can a cyberattack pose to your business? One way to track that is to look at the mechanisms we use to protect ourselves.

[00:05:55] **Brendan Monaghan:** When the cyber insurance policy, that risk transfer mechanism first came out, it was centered around data and the risk of a company's data being compromised. Over the years, and with time, the cyber insurance policy has grown in what it covers and it does reflect the emerging threats in this cyber arena that every business faces. So now what started with simply data has expanded to actual money. So not just the data but money. And then we also have the growth into property insurance coverages being incorporated into cyber due to the risk and threat of bricking. Now for those that may not be familiar with the term bricking, it's when a threat actor gets into a system and renders your equipment as usable as a brick, and as we look forward into the future, the increase in autonomous vehicles and the amount of automation there is in the manufacturing arena, all those are going to be presenting new cyber threats.

[00:07:03] **Patrick Pacheco:** So are smaller businesses or medium-sized businesses more at risk or less at risk with regard to cyber threats?

[00:07:27] **Brendan Monaghan:** So I think that all businesses are at risk and larger businesses have a larger target for some of these bad actors. There may be more of the challenge in trying to see what they can do associated with a larger business. But smaller and medium-sized businesses have a greater risk from the perspective of they don't have the budgets and teams that are available internally to help mitigate some of those risks and make sure that some of those safety measures are in place throughout the organization. So they both face a really elevated risk, but it may be for different reasons.

> [00:08:06] **Patrick VO:** Anybody can be the target of a cyberattack, even if they think they’re too small.

[00:08:14] **Brendan Monaghan:** If they gain access to one individual, they may then use that individual's contact list to then go and spread the message further. So you don't have to be the intended target of an attack in order to be caught up in that web. And so really all businesses have this risk, and I believe it's important that all businesses evaluate that risk and then make a business decision as to how they want to handle that risk based upon their own findings and that personal assessment.

[00:08:46] **Patrick Pacheco:** Kevin, you mentioned earlier social engineering and how this is put into play with these attacks. Can you expand on that a little bit?

[00:08:54] **Kevin McMahon:** The bad actors are very intelligent, like we were talking about before, and what happens is they understand that people respond and react to different things based on the fact that we're all humans. And I'll give you an example of this. There was a recent breach at a public company. The mechanism that was used to get into the data was that they sent a message over and over and over again to an employee that they had their credentials, but there was a multifactor authentication in there that the employee had to click yes for. So the bad actors just continued to send a message to that employee and sent several of them saying, 'Hey, this is the help desk, don't worry. The message is exactly what it should be. Just click yes." And all of this encouraging stuff where they were trying to get the employee to go ahead and give them access, and literally the employee got sick of it and just clicked yes. And that allowed them to get in and then start compromising the data that's in there. That's social engineering, it is working on the weakness of the human. One other statistic for you, coming from that same Verizon report: 85% of data breaches require some kind of human intervention. So it is social engineering that's facilitating a lot of what's happening out there.

[00:10:26] **Patrick Pacheco:** So these attacks, they're out there, they can be expensive, they'll target any company, what could we do to protect ourselves?

[00:08:54] **Kevin McMahon:** I think the number one thing is to address that people or human component. And you get to that with training. There's enough information out there that people can make themselves individually aware, but it also helps if some of that's crafted and put into a good training program.

[00:10:48] **Patrick VO:** In the name of training and awareness, I asked Kevin and Brendan what threats employees should be on the lookout for.

[00:10:57] **Brendan Monaghan:** Backing up for a second here, a lot of these cyber threats are based around either finding a vulnerability or backdoor entry into a company system. Finding a way to convince someone, a person, to hand over credentials, so that they can then get in and then go, whether it's to cause them to send money, whether it's to get the passwords into their system so that they can then go about understanding what that internal data looks like. That's really what we're looking at from that broad perspective of either the opening, the security vulnerability, or the human element to gain entry or gain information.

[00:11:34] **Kevin McMahon:** The first one that I see as the most common threat at this point is phishing.

[00:11:40] **SFX:** Sound of someone casting a line; line being reeled in underneath next part?

[00:11:45] **Kevin McMahon:** Phishing is when an email is sent that essentially pretends to be something that it's not with the intention of capturing credentials or installing malware. So somebody may send you an email that says, "Hey, you purchased this thing on the Apple store, and here's the invoice, click it to download," and as soon as you click it, what you're really downloading is malware. Or there may be a, "Hey, click here to come collect your reward," and you have to log in and they ask you for your credentials and now they've stored those. So those kinds of things, that's phishing and they're very common. I'm sure everybody's getting phishing emails on an all but daily basis. We are starting to see them come through text messages and other ways. So any kind of communication path that can be used electronically, these bad actors will use it.

[00:12:46] **Patrick VO:** Phishing is a way of gaining access to your system. Once they're in, that's when the real trouble starts.

[00:12:54] **Kevin McMahon:** The second thing I see is something I referred to a little earlier, and that's business email compromise. The idea with business email compromise is that a bad actor gains at least some form of control over a person's email box. They tend to do that in the background so that the user of that email box doesn't know it and then they will send or receive emails as if they're that person. We take email as being the identity of the person. So when I get an email from somebody and it says it came from John Smith, and I'm pretty convinced it's John Smith, but imagine if you're giving business instructions on things to order or money to move or people activities to take or something, and it's actually being done by a bad actor in your name.

[00:13:43] **Patrick VO:** And there are other ways that a bad actor can wreak havoc if they get past your defenses.

[00:13:50] **Brendan Monaghan:** Well, so ransomware is once that threat actor has gained access into your system, how they would encrypt your files and then demand a ransom payment. With ransomware, once that information is gained and you are now in the system, this method is where the files are encrypted, typically, and then you must effectuate this ransom payment in order to receive the key to decrypt those files that they have encrypted. And then part of that process they will then post in the dark web, the cyber incident equivalent of a proof of life in a kidnapping situation where they have a proof pack which demonstrates that they were able to successfully enter your system and then exfiltrate some amount of data that they are now sharing on that dark web as proof of the success in their endeavor.

[00:14:48] **Patrick VO:** Threats like this can force you into uncomfortable decisions, and you might not even be aware of all the repercussions.

[00:14:56] **Brendan Monaghan:** What you don't want to do is make a ransom payment and then have a federal agent at your door asking why you just paid Al Qaeda or some other terrorist operation because you transferred money to a Bitcoin wallet that is a known to be associated with some terrorist organization and is on the OFAC list. So there's a whole process that you really need to be very cognizant of.

[00:15:21] **Patrick VO:** Beyond creating awareness about these threats, there are some simple, common-sense steps you can take to protect your business.

[00:15:29] **Brendan Monaghan:** Training and that awareness are key and critical, and then making sure that you have a strong password policy in place with updating of those passwords with regularity. And then also the backups are so important because that backup is where if that threat actor is able to get into your system and do whatever they are looking to do, with a good backup protocol and policies in place, that really does help change the analysis when it comes to at least the continuity of operations for the business as well as just what that response is going to look like and how that business may choose to respond or be able to respond. Without a good backups in place, both local as well as cloud or offsite backups is really a key point in making sure that we mitigate the risk.

[00:16:22] **Patrick Pacheco:** And Kevin, you talked about multifactor authentication. They had all that information, but they still needed that one piece. So it sounds like that's a pretty strong deterrent right there.

[00:16:33] **Kevin McMahon:** Yeah, I couldn't emphasize that enough. Multifactor authentication really goes a long way towards protecting access to systems and to data. That was the last step in that example that I gave that had to be worked out. But it's the case for both our personal and our professional information, if you implement and use multifactor authentication, it is going to be much safer.

[00:16:56] **Patrick VO:** The good news? You don't have to do this on your own.

[00:17:00] **Patrick Pacheco:** How would you recommend a small business that doesn't... you know they don't have the huge budget—what do they do to protect themselves? Where do they start?

[00:17:08] **Kevin McMahon:** I think most companies should use some form of guidance, whether it's guidance from a partner or from a government agency or best practices. There's plenty of those kinds of things out there. Don't create the wheel yourself. I think that it can be difficult to find knowledgeable security people to build a program and it's often better to partner with a company that you trust.

[00:17:40] **Brendan Monaghan:** Completely agree. And it really comes down to awareness and being aware yourself as an owner of that business and then bringing that awareness to your team and a willingness to understand what this risk really is. And then with that partner, as Kevin mentioned, finding those right tools within the budgetary constraints that exist to best move the needle.

> [00:18:03] **Patrick VO:** As you've heard, an ounce of prevention is worth a pound of cure. But if your approach is *all* prevention and *no* cure then you're not fully prepared. You've got to mitigate your risk in the event that something does happen. One way to do that is with cyber insurance. But finding the right policy can present its own challenge.

[00:18:27] **Brendan Monaghan:** As we continue to see cyber expand into new areas, that's where we're seeing the coverage grow as well. So whether it's bricking coverage, which is more of a property insurance claim, now that's being built into cyber insurance as well. So it continues to evolve as the threat and the risk of cyber evolves. So the cyber policy, there is no uniformity and standard as there is in many other lines of insurance coverage where there may be a base policy that many insurance companies have all adopted and then they put their bells and whistles onto it. In the cyber insurance arena today, we still have insurance companies that are developing from scratch their own policy forms and series of coverages. From that perspective, it can be a bit more difficult to analyze and compare two different offerings and understand what coverages are being provided, what are not being provided, how does the language work. It is still a bit of the wild west out there in that regard that we don't have that standardization in place yet.

> [00:19:37] **Patrick VO:** But amidst those bells and whistles, there are some foundational components you should look for in a policy.

[00:19:44] **Brendan Monaghan:** Many cyber insurance policies include both an element of liability, but then also the first party coverages. So the cyber insurance policy, there's a cyber liability component and it's generally referred to as cyber liability insurance. But the liability is that liability to others. And yet, when you look at where a lot of the expense is being incurred in a cyber incident, a lot of it isn’t in that liability to others. It’s in your own costs. The other parts of it are going to cover that first-party risk and exposure. So that's where you have legal, that's where you have forensics, that's where you have public relations, that's where you have the lost business income related to that downtime. That's not liable to others. That is your own business loss and downtime and expense.

[00:20:30] **Patrick Pacheco:** So we've done everything: we've educated our employees, we've told them what the different risks are out there, we keep it top of mind, we have multifactor authentication, we have our clients utilizing this and something still happens. What do you do? I mean, how do you approach that?

[00:20:45] **Brendan Monaghan:** So really starting there with that incident response plan is key. So now that it's happened, you know what to do. So you're not flipping through the yellow pages or getting onto Google in that moment to now figure out what to do. But you have that roadmap and a game plan in place when that incident has now occurred.

> [00:20:53] **Patrick VO:** An incident response plan is a critical part of your cyberthreat approach. When that cyberattack takes place, you'll want to know what your next steps are.

[00:21:06] **Kevin McMahon:** First and most important is to have one. You don't want to be creating an incident response plan when the incident has already happened.

[00:21:26] **Brendan Monaghan:** Two, make sure that this gets managed and handled quickly and efficiently, because time really is critical here. When a ransom event occurs, there typically is a clock that the bad actor initiates within which they are seeking to have payment made. So time is of crucial importance, and to make sure that you have that incident response plan in place that you can then turn to and begin from is going to greatly speed up how you handle the response and what you're able to effectuate and achieve.

> [00:22:09] **Patrick VO:** Another key element of an incident response plan is the team you assemble.

[00:22:16] **Brendan Monaghan:** Having those right partners, and those partners are going to include legal, they're going to include forensics for understanding how that threat actor was able to get in as well as what information has been compromised. And then public relations. Those are the three key aspects that you're going to see in many cyber responses. First and foremost, that legal team—that person really often times acts as the coach or quarterback of the entire cyber incident response. So that's going to be the first and foremost step. Now, if there's a ransom event, you may also be looking at a separate ransom negotiator or negotiation team in addition to those three other parties. And insurance companies have these panel partners that have been pre-approved, that negotiated the rates to help make sure that you've got those right partners in place. And so it's good with that cyber insurance policy to understand who is on that panel and to make sure that there's a level of comfort that you have with that panel and which direction you're going to go. Some insurance companies offer additional services in helping manage that process. Others are going to simply have the names and then you're working with those third parties. So there is a variation in the response, depending upon your insurance company partner. But really having that understanding of how you need to act, how the insurance company's going to act as a partner, the role your insurance broker plays in this equation, and then who these other third parties are is key and critical to success in the face of a cyber security incident.

> [00:23:51] **Patrick VO:** A good incident response plan can alleviate much of the harm that might have been caused by a cyberattack--particularly among the public.

[00:24:00] **Kevin McMahon:** I think what more comes into it is how the companies handle it. If you take the steps to restore the trust and confidence of the customer base, I think that you can preserve the reputation of the company.

[00:24:13] **Brendan Monaghan:** Kevin just hit on something that was really crucial and important in that, how that incident response process is handled plays so much into the reputational risk that a business faces. And that's an often overlooked element in a cyber incident is how that incident response is handled. But when handled in with engagement of those professionals that know how to walk through that process, that is where the right communications can go out, which give people an understanding of what's occurred in a way where the reputational risk is at least properly understood.

[00:24:46] **Patrick VO:** Cyber threats are out there and they can be devastating. It's becoming more and more likely that your company will be targeted, regardless of your size. What happens then depends on your actions now. Arm your employees with the knowledge they need to ward off attackers; humans are the most likely point of entry. Implement strong password and backup policies. And, most importantly, utilize multi-factor authentication!! No approach is complete without a strategy for the worst-case scenario. Cyber insurance can transfer some of that risk and help you create a sound incident response plan. Most importantly, stay vigilant--you never know where the next threat might come from.

[00:25:31] **Patrick Pacheco:** Well, Brendan and Kevin, thank you very much for being on, and as a prize for being on, I'm going to send you an email and if you want a free iPad, just click the link. Okay?

[00:25:40] **Brendan Monaghan:** I will do it right away.

[00:25:44] **Kevin McMahon:** Yeah, I don't think I'll click on that either. Thank you.

[00:25:50] **Patrick VO:** Thank you to Brendan Monaghan and Kevin McMahon for keeping us, and our clients, safe.

[00:25:56] **Patrick Pacheco:** In Good Companies is a podcast from Cadence Bank, member FDIC, equal opportunity lender. Sheena Cochran is our production coordinator. Our executive producer is Danielle Kernell, with writing and Production from Andrew Ganem and sound design and mixing by Ben Cranell at Lower Street Media. I'm your host, Patrick Pacheco. If you've made it this far, why don't you go rate and review us in your podcast app? It's the best way to grow the show so we can reach even more listeners. And while you're there, subscribe! We'd love to have you--because when you're with us, we're in good companies.

[00:26:31] **Outline:** **Disclaimer**