Cadence Bank Podcast: In Good Companies

Episode #4: Cyberfraud & Cybersecurity

You've probably got a security system for your building, with locks on your doors and safes for your important documents. But criminals don't just try to take what's in your cash register anymore. As the world shifts increasingly online, there are more and more opportunities for fraudsters and cybercriminals to intercept your money and data. And it takes more than anti-virus software to keep yourself safe. But your specialty isn't cloud computing, it's your business. So how do you keep up with the ever-changing world of cybersecurity?

Fortunately, there are people like Lori Johnson and Tracy Dalton, from the Treasury Management Team at Cadence Bank. They make it their business to keep up with trends in cybercrime so they can best protect their clients. Through their work with a broad range of customers, they see companies' most commonly-targeted weak points; and they're not what you'd suspect.

Cybercrime can be devastating, and nobody is completely safe. Companies of all sizes are targeted, and breaches can cause loss of consumer confidence, in addition to whatever is stolen. Lori and Tracy will escort us through the dangerous underbelly of fraud as we talk the size of the threat, cybersecurity best practices, and how to get employee buy-in. So keep your head on a swivel and listen to our cyber self-defense class!

Episode Transcript

[00:00:00] **Tracy Dalton:** It is so startling. We're all affected by it, literally, every 39 seconds, Patrick, at broad incident takes place and it's up over 39% over 2020. COVID not only created a physical virus. it gave our fraudsters a lot of opportunity to be at home and think of ways, to create opportunities for fraud.

[00:00:26] **Patrick VO:** The biggest threats to your business aren't necessarily competitors or supply chain issues. They're the threats you can't see, the ones lurking in the shadows, that can blindside you.

[00:00:38] **Tracy Dalton:** So yeah, businesses of all sizes and industries are affected - everyone from locally owned businesses, small businesses to huge enterprises and just no one is safe. So everyone has to be really diligent.

[00:00:53] **Patrick Pacheco:** I'm Patrick Pacheco and you're listening to In Good Companies from Cadence Bank, the podcast where we answer the toughest questions facing your business and guide you through the company life cycle from start to sale and success to succession.

[00:01:14] **Patrick VO:** It's an unfortunate fact of life that wherever there's money, there are people trying to steal that money. And the more digital our lives become, the more access points thieves and fraudsters have to your business. As security evolves, so do the tools and schemes they implement--so you've got to stay current to stay protected. But you're not an expert in cybersecurity, you're an expert in your business. So how can you protect yourself?

Wait a minute--what's that, up in the sky? It's a bird! It's a plane! It's Lori Johnson and Tracy Dalton! Lori and Tracy are superheroes in the fight against cybercrime--they're Cadence Bankers with a mission to protect their clients at every turn. But they can't do it alone. They need your help. So, Lori and Tracy joined us to talk about the keys to safeguarding your money and data. Together we'll cover the most common targets for fraudsters, best practices for employees, and the powerful tools your bank has on offer. Will the fraudsters weasel their way into your system? Will good triumph over evil? Will Lori and Tracy reveal their secret identities? Stay tuned to find out!

[00:02:30] **Lori Johnson:** I'm Lori Johnson and I'm a Senior Vice President—Treasury Management Sales.

[00:02:37] **Tracy Dalton:** I'm Tracy Dalton and I'm a Treasury Management Officer.

[00:02:41] **Lori Johnson:** In treasury management sales, our role is really understanding their cashflow side, the things that they have in place from a risk mitigation perspective today, um, and then helping, you know, through our trusted advisor role to layer in, you know, tools and resources that will help them mitigate their risks.

[00:03:01] **Patrick VO:** To know how to protect yourself, first you have to understand what you're up against. And let me tell you, the threat is *real.*

[00:03:11] **Patrick Pacheco:** So Lori, let's, let's take a 30,000 foot view. And how do some of these things work? And it doesn't seem like all of them are super sophisticated. What are the most common ones you see? And then how do they actually work? What are they doing?

[00:03:23] **Lori Johnson:** Yeah. Now, Patrick you're right there. There are a lot of different types of threads and they, they really vary in their level of sophistication. Um, and what we see from just the most common forums is that they start with social engineered. And, so hackers really use a variety of techniques, um, to, to try to trick the end-user into gaining access to their systems or information. And, so one common example, you know, that we see a lot is, is phishing. phishing attacks can come in the form of email, text, phone calls, and they really look legitimate, um, and, and are designed to persuade the end user to download an attachment click on the link.

Um, from a provide sensitive information such as passwords or account information.

[00:04:05] **Patrick Pacheco:** That sounds like a pretty, simple attack. What are some of the more sophisticated things that you see?

[00:04:13] **Lori Johnson:** Yeah, a couple of the other things that we've seen, um, that are very common is, you know, in 2021, we've seen a record high of data breaches, um, you know, which can, can really wreak havoc on a company. Um, you know, doing things such as driving down consumer confidence, these types of data breaches, um, a lot of times affect, you know, millions of in-users, you know, particularly when they are on the national and international brand level.

Um, and all over the media is an example. You know, Facebook was an example. And from, from, you know, earlier this year, um, where, you know, user's information was stolen

And another example is malware, um, which really just is malicious software and it affects the computers when users download attachments from unknown senders, um, or click on infected links.

Um, you know, there are many different types of malware that we hear about trojans, uh, viruses, spyware. Um, lots of different, lots of different types of malware, but they really all have one goal. And then it's just still information, um, you know, even damage or disrupt systems or take them over, um, such as in the form of ransomware, um, you know, re ransomware attacks have been on the rise this year, you know?

No, we heard about, you know, back in May, um, the Colonial Pipeline, ransomware attack, but what ransomware really is designed to do is there's a targeted system, um, that becomes encrypted in which the companies no longer have access to the systems or information, um, until they pay the ransom. and even then if the company chooses to pay the ransom, it's a really no guarantee that they will regain access to the system. Or information.,

[00:06:01] **Patrick Pacheco:** Tracy, so you have visibility and a big range of clients. What kind of trends are you seeing with your clients?

[00:06:08] **Tracy Dalton:** Absolutely Patrick. And there's just, so many types of fraud. Email fraud is, is obviously the most prevalent simply because we all live and die by email. But, also internet for a bank account takeover, fraud. That certainly one of my highest dealings, um, and then debit and credit fraud.

So, you know, just it's everywhere. And so many of my clients deal with this when their account information is intercepted by fraudsters. once the bank account

information is stolen, a fraudster then uses that to redirect their funds, anywhere from creating and distributing checks, um, to creating online payments with clients, banking information. I just had a client this week that, um, all of a sudden started seeing all of these credit card payments on their banking information and said, well, those aren't mine. Uh, literally fraudsters are paying off their credit cards with my client's banking information. So it's pretty darn scary.

[00:07:01] **Patrick Pacheco:** How big of a problem is this? I mean, how many businesses are affected? What kind of dollars are we talking about here? just across the business landscape in general, here in the United States.

[00:07:32] **Lori Johnson:** Yeah, it's, it's a huge issue for companies and it's reported to be, you know, really a primary threat to business growth because the losses can be so significant. And so, I would say the scale really depends on the level of sophistication. You know, if it's, if it's check fraud, the losses are typically going to be smaller. Cyber fraud, the losses will be, you know, larger, so anywhere from, you know, thousands of dollars to millions of dollars. And really what we see is it's not a matter of, if you're going to get attacked, it's a matter of when.

[00:08:05] **Tracy Dalton:** And we all take the impact from that every single one of us, and overall, our economy is affected by that right. Prices rise because companies are taking losses. Um, so, and then small businesses, it could take a small business out if they're not insured and insurance is expensive. So it's a slippery slope.

[00:08:29] **Patrick Pacheco:** Are companies taking it seriously or your company's taking it seriously? Is it at one of their top priorities? Are they, thinking if I just close my eyes, it'll go away and hope nothing happens.

[00:08:38] **Tracy Dalton:** You know, it is so startling. We're all affected by it. Literally, every 39 seconds, Patrick, a fraud incident takes place and it's up over 39% over 2020. COVID not only created a physical virus. it gave our fraudsters a lot of opportunity, to be at home and think of ways, to create, opportunities for fraud.

So yeah, businesses of all sizes and industries are affected everyone from locally-owned businesses, small businesses to huge enterprises and just no one is safe. So everyone has to be really diligent. And people are now calling to be proactive, which warms my heart and is very exciting because, um, we can reach out. But having people reach out to us is really important as well.

[00:09:36] **Patrick VO:** The message is clear. If you're not worried about what's out there, you're not paying attention. But what can you do about it? Well, the first step is evaluating your current security setup.

[00:09:49] **Patrick Pacheco:** What are some steps that every company should be taking you know, what are some common threads, some basic things that every

company needs to think about and they haven't thought about, they need to start thinking about.

[00:09:59] **Tracy Dalton:** Every business should be asking, about their information, where is the critical data located? and what's its value. They need to identify the systems and databases where their information, it's stored. Um, whether it be out on a cloud or in their bank, they need to understand all of the different relationships that, interface with their data.

And then they need to understand how their critical data is backed up. You know, the frequency of it. Is it offsite? Is it off network? Is it encrypted? And then. You know, what are the layers of our cyber defense plan? You know, how do those layers work together and understanding which threats are mitigated by which layer. And monitoring for suspicious activity is so important. Um, are they monitoring 24 7, 365? They should be. Um, are they including vendors who connects to your, to your network and understanding those external, threats. Then, you know, what are those cyber incidents response plans include? Are they, you know, is there a business continuity plan after their attack, reputation, mitigation?

These companies need to protect their reputation. And then again, as you mentioned, with security, the liability and the limit to financial damage, and then, you know, really who's performing that information security function.

[00:11:40] **Tracy Dalton:** Um, is there accountability to business leaders and support from qualified third-party partners? When it's needed. So there's absolutely a lot of questions that every business should be asking about their security, plan.

[00:11:59] **Patrick VO:** Of course, once you've asked the questions, then you have to actually do something about it. Fortunately, you don't have to reinvent the wheel. There are plenty of companies that provide a great model with how they manage their security.

[00:12:15] **Patrick Pacheco:** I understand you have a client that's in the healthcare sector, that's doing everything right. When it comes to cyber security, it can be a really great model. Um, what is it that made this client get to that point now?

Why were they, what was their concern about cybersecurity?

[00:12:30] **Tracy Dalton:** Yeah. So my, my client is, uh, serves the healthcare industry and is a nonprofit. And so they have numerous constituents, um, throughout their footprint that they're accountable to. Uh, so they're responsible to protect each and every portion of their, that payment life cycle. So it was very important to them.

Uh it's to make an investment and a commitment to their cyber security and fraud.

[00:13:03] **Patrick Pacheco:** So when this client comes to you and says, we want to make this commitment, what did you do to help set them up for success?

[00:13:10] **Tracy Dalton:** So I spent a lot of time with my clients, um, and, uh, and they came to me and we wanted to really discuss with them what they have in place today. What are they doing? Um, What are they doing manually? What outside resources do they have? Um, and we talk about industry trends and we try to identify opportunities to increase their levels of protection. It may be as simple as adding an internal process that they may not have thought about or implementing a new service that enables them to safeguard their assets.

[00:13:51] **Patrick VO:** One of the best security investments you can make isn't fancy software--it's educating your employees. Because most fraudsters aren't trying to get in through your firewall.

[00:14:01] **Patrick Pacheco:** So you mentioned employees, it seems that as, as we've, as we've gone through the discussion, it seems like the employee is the potentially the weak link in, in these things. And, so what did they do with regard to education, both outside and, and, and, and for their, for their employees about why we do certain things.

[00:14:20] **Tracy Dalton:** My client is very diligent and keeping up with the trends and the latest scams, but they also partner with an outside IT consulting firm. And the firm provides education sessions and updates and overall support with questions and written material. How do you, how do you get employees to, to buy into, to doing this and how, how did they get their employees to buy into?

[00:14:46] **Patrick Pacheco:** Now, we're going to add a third step as it's something that the employees were ready to do. Because they communicated or is it something that took a little bit more leaning on folks to get them complying?

[00:15:00] **Tracy Dalton:** Their employees really do buy in because, you know, even though they have. You know, quarterly education trainings, they talk about cyber security and fraud every single week in their, in their meetings. And they share situations that happen or that they've heard about. and their employees are really, invested and safeguarding the company that they work for.

[00:15:28] **Patrick VO:** Once employees know what to watch for, it's about creating internal controls, so that security never relies on a single person, but rather draws strength from the collective.

[00:15:39] **Tracy Dalton:** Oh, yeah, absolutely. You know, so I can't, I can't stress enough how, you know, communication and training is so important, um, to prevent fraud. but also having this. Processes in place implementing things like dual control that run through all of the processes. Um, so my client has actually a three-step

process where someone verifies the request. A different person is entering a request and a third person. Yeah. Typically a manager is authorizing to complete that transaction. And so that's how diligent my client is, with these. And then they also leverage some of our online banking tools like alerts and notifications. That remind them or alert them when something is off and they can set those up to be, you know, specific for them.

So, but, and you look and go, you know, yeah, that's an extra step or why three step we're here. Two-step but that is how important, you know, safeguarding their money is and safeguarding, you know, their, their funds are so that extra step, it's okay. And it's okay. Because they can, for their employees, their employees don't feel that, you know, oh, I've got to do another step because they're constantly educating and constantly working together to understand, that these, these things are happening every day. And so we all have to do an extra step to, to safeguard ourselves.

[00:17:20] **Patrick Pacheco:** Cybersecurity seems to be a team effort. Um, so what seems like one of the best teammates, you know, people may not know about is their bank. How can, how can Cadence be a good teammate to the, to its customers in the cybersecurity world?

[00:17:34] **Lori Johnson:** I think there are multiple different, avenues there. Um, you know, we provide the technology tools that our clients need to protect them from various, uh, types of fraud. But also from an education perspective, um, you know, we, we see ourselves as an extension of our client's business, um, in, in part of that comes into, you know, helping them to protect their assets.

And so, you know, whether it be on the product perspective and in the tools and solutions that we provide and offer our clients, there are a ton of resources out there available in our online platform. and then through our conversations that, that we kind of talked about previously, where we're really understanding, you know, what are the tools that our clients have in place? What might be their vulnerabilities and really helping to identify those and helping them close those gaps.

[00:18:22] **Patrick Pacheco:** Let's pivot some specific offerings Cadence has and how they protect clients from fraud. So, tell me a little bit about Positive Pay.

[00:18:30] **Lori Johnson:** It's really is easy as our client, you know, uploaded. Uh, file, or, inputting the checks that they would like the bank to pay on their behalf.

And then the bank reconciles, their approved check register against the items that are clearing their account. and if anything, does it match the criteria that we're matching against the customer has, you know, an opportunity to proactively, decide to pay that item, or should they choose to return it, because it truly is a fraudulent item.

Positive Pay in a lot of cases does capture, fraudulent attempts. It's very inexpensive insurance.

[00:19:06] **Patrick Pacheco:** What about ACH Positive Pay? How's that different?

[00:19:13] **Lori Johnson:** So, just like Positive Pay works to protect against, checks, ACH Positive Pay just protects your account from unauthorized electronic transactions. So, it really allows our clients to create a database. If you will, of, companies or vendors that are offering to, to debit their account. Um, tax payments is a common example.

Maybe payroll fees, merchant services, fees, um, you know, but really just setting that foundation for companies that you have provided your account number and routing number to, that can come in and draft your account and making sure that you are proactively, able to stop, any transactions that are unauthorized

[00:19:48] **Patrick Pacheco:** So I needed that for, for my account because my son had some, some money on a Venmo accounts and said “I can't get it off. Can you, can you let me link it to your, to your debit card? So you could give me my $200.” So I linked it to the debit card and I didn't think anything. And then I kept questioning my girlfriend

“Why are you spending so much money? Why are you spending so much money?” She looked at it and she goes, “I didn't spend money at Champ Sportswear.” And I thought had, “I've got fraud on my account.” And then I started looking at the other locations. It was Champ’s Sports where Dick's Sporting Goods, started looking and said, “Hey Grant,” (that's my 15 year-old son who people have heard about before.)

“Have you been using my Venmo account?” And he said, “No, I've been using my Venmo.” I said, “Is it my card on it?” He goes, “Yes.” I said, “Why did you do that? He goes, well, you didn't tell me to take it off.”

But, uh, yeah, it's, it's amazing how quickly things can spiral out of control. If you don't look at your bank statements so I, I may need to enlist your help at some point to protect myself against my son.

[00:20:50] **Lori Johnson:** Sounds like Grant had a nice shopping spree.

[00:20:53] **Patrick Pacheco:** You know, the bad part about it. He actually bought me some. Like he bought me a cap and something else.

I forgot that. I thought that was, “Yeah, that's great Grant. That was really nice.” And I'd realized he bought it with my own money, but, uh, I guess it's the thought that

counts. So that at least that's what he, that's what he told me. “It's the thought that counts, Dad.”

[00:21:10] **Patrick VO:** With the general public more aware than ever of cyber-attacks, I asked Lori if companies have improved their cybersecurity protections. The answer is yes, but that doesn't mean we can let our guard down.

[00:22:05] **Lori Johnson:** You know, I would say that it has improved. However, a lot of what we see are just the repeatable, very simple mistakes that we've talked about. Maybe it's not authenticating a wire request or doing that callback verification to the trusted number. Maybe it's, relaxing internal controls or becoming lax on software updates and things like that.

I would say regardless of the industry, we kind of talked earlier about assuming that an email is bad until it is proven good. Particularly when there are regarding requests for payment or any type of financial wires. This most common.

It only takes just a few minutes, And I think, you know, we get busy and, uh, we have, we have our jobs to do, or, maybe the, the request, you know, came from a big fish in the company, if you will.

And, so, um, you know, we don't, we don't want to question those folks. And so, it's just being hypervigilant, staying curious, second guessing everything.

[00:22:26] **Patrick Pacheco:** I'm going to use, you're assuming it's bad until proven good with my son. That's going to be my new, my new mantra I have with him.

[00:22:33] **Patrick VO:** And through her work with all her clients, Tracy's learned to keep her head on a swivel.

[00:22:40] **Tracy Dalton:** I can't say it enough. Uh, the best way to audit your set up is to be diligent. Be diligent about checking your bank account and bank transactions daily, just a quick look and find an[d?] uncover something very significant. Communicating! Communication, communication. Communicating internally, and having multiple sources to educate your staff about cybersecurity and fraud prevention, and really, you know, to have a good relationship with your trusted banking advisors.

[00:23:14] **Patrick VO:** So what have we learned? An ounce of prevention is worth a pound of cure; and a pound of prevention, well, that's even better. Educate your employees, consult outside sources, and utilize your bank! Cadence, in particular, has become an industry leader in security, so we're ready to be your partner in crime. Or partner out-of-crime. Partner in crime-prevention? We're working on it.

Above all, work together to stay vigilant. That way you won't need a superhero to save you. You'll be the superhero!

If you want to [learn/know?] more about how to protect your business, visit the Business Fraud Knowledge Center on the Cadence Bank website. We'll put a link in the show notes.

Thanks to Lori Johnson and Tracy Dalton, two real-life superheroes, always saving the day.

[credits]

[disclaimer]