Season 3 | Episode 104

Cyber Security: What Small Businesses Need to Know

Gene Marks

CPA, Columnist, and Host

Kristin Harper

Manager of Operations Security, Paychex

Announcer:
Welcome to THRIVE, a Paychex Business Podcast, where you'll hear timely insights to help you navigate marketplace dynamics and propel your business forward. Here's your host, Gene Marks.

Gene Marks:
Hey everybody, and welcome back. Thanks so much for joining us. My name is Gene Marks. I am here speaking to Kristin Harper. Kristin is the Manager of Operations Security at Paychex. First of all, Kristin, thank you very much for joining me today.

Kristin Harper:
Thanks for having me on, Gene.

Gene Marks:
Yep. It's like Cybersecurity Awareness Month, right? This is it. This is like your Christmas. Does that make sense?

Kristin Harper:
Yeah, it totally does. I lead our cybersecurity team here at Paychex and part of the responsibility for my team is education, user education, both internally and externally to Paychex. So it's sort of like our Super Bowl this month.

Gene Marks:
Yeah, I believe it. It is a big month for people in the cybersecurity world. So Kristin, so just a little bit about your job so our audience can understand why I'm talking to you today. I mean, are you more concerned with cybersecurity issues protecting Paychex's data or do you work directly with clients as well to give them sort of cyber advice or cyber consulting?

Kristin Harper:
So, internally here at Paychex is where my team is focused.

Gene Marks:
Right.

Kristin Harper:
So, aside from user education, which is a huge part of protecting both our clients and our clients protecting their businesses as well as us protecting Paychex. So the education piece is probably where that crosses.

Gene Marks:
Got it. Got it. And how long have you been doing this?

Kristin Harper:
So I've been with Paychex for 24 years and the last four and a half in cybersecurity.

Gene Marks:
That is crazy. So before you got into the whole cybersecurity area, did you have any knowledge of cybersecurity or is this self-taught?

Kristin Harper:
Oh, not self-taught.

Gene Marks:
Good.

Kristin Harper:
So, I had responsibility in our incident response, so for Paychex and actually background in the business. So I learned about data protection and the importance of security hands on from the ground up, right? From as we started to see cyber really evolve.

Gene Marks:
Got it. Got it. So, okay. So guys, if you're watching this or you're listening to this, obviously cybersecurity is a big, big issue. This is a person...and Kristin who, this is her life, this is her job. It is bad situation if a company like Paychex gets hacked or if there's cyber flaws. So it is your job and your team Kristin, to make sure that you can reduce the risk of that happening.

Gene Marks:
Although you can't completely eliminate the risk of happening, but your job is to reduce it. And I think that's really important for our audience to know. So Kristin, let's jump into it a little bit. I talk a little bit about why this is important. We talk about that it's Cybersecurity Awareness Month or whatever. Tell me about cybersecurity in small businesses?

Kristin Harper:
So cybersecurity is equally important to small businesses as it is to a large one. So more and more we're seeing small businesses be attacked by cyber criminals. And that can be something small or something big like ransomware. So, in fact, more than half of the attacks are focused on small businesses. And one of the things that we see with small businesses is they're a more attractive target.

Gene Marks:
Yeah.

Kristin Harper:
For probably a couple of reasons. The first being that they have less protections, less digital infrastructure and defenses so makes them an easier target. They also have the data and the financial information that cyber criminals want. And they're oftentimes less prepared. So that can be anything from their end user education or just planning for the worst to happen to their business. For a lot of them, it's not on the radar as the threat that it is.

Gene Marks:
Yeah. The media likes to cover the big hacks and data breaches that are out there. And the amount of small businesses that have this issue is just, it's not reported. It's very tough frankly if somebody's in the media to actually interview a small business that's been hacked because those guys don't really want to share that information at all.

Gene Marks:
But it's really out there. And like you said, there's a huge amount of small businesses that are impacted by breaches themselves. So you had mentioned as well about sort of user education, and let's start with that. My understanding is in the studies that I read, Kristin, is that the number one reason why people get hacked is because of users, lack of user training. Can you talk a little bit about that?

Kristin Harper:
Yes. So with any crime, you're going after the area that has the most potential for that crime.

Gene Marks:
Right.

Kristin Harper:
Right? So social engineering, phishing, all of those techniques that are used by attackers focus on the end user. And that really makes user education important to stopping and defending against cyber crime. So half of attacks start with a phishing or user credential compromise.

Gene Marks:
Right.

Kristin Harper:
So our attackers are focused kind of on that weakest link and those folks that know the least about cybersecurity. So when we talk about education, and some of the best ways a business can defend themselves really starts with educating that user on how to identify the hallmarks of phishing or smishing, which is a new attack factor that we're seeing and really go after that and really educate themselves on how to stop it.

Gene Marks:
Yep. What is phishing Kristin and what is smishing and what is social engineering?

Kristin Harper:
Yeah. So phishing has been around for a while. It's phishing with a P-H.

Gene Marks:
Yeah.

Kristin Harper:
And phishing is sending a user some sort of lure.

Gene Marks:
Yeah.

Kristin Harper:
Pardon the pun, via an email. And that lure could be a link that looks just like you're tracking your UPS package that you're waiting for or something that's attractive for the end user.

Kristin Harper:
They click, it downloads malware or spyware onto their system. So something that is a key stroke logger or watching for what the user is doing or gets them to compromise their username and password. And from there, allows the attacker access to their device or their network.

Gene Marks:
You've explained what phishing is, let's move on to smishing.

Kristin Harper:
So smishing is something brand new that we're starting to see really get feet. So, smishing stands for SMS phishing or text message-based phishing.

Gene Marks:
Right.

Kristin Harper:
And what it is it has all the same hallmarks as you see with a phishing email except it comes to the user's personal cell phone or device via a text message. So phishing has been around a while, smishing's a little bit newer. And what we're seeing with smishing is there are less protections. So email gateways, even your Gmail, your Yahoo mail have protections to identify spam and phishing emails and they block a certain percentage of that.

Kristin Harper:
But when you get into a cell phone, there's less of that. The other thing that we see as a hallmark with smishing is that it's a lot more realistic and targeted. So all that information that is out about you online is used and targeted by attackers to send you a text that you're likely to click on.

Kristin Harper:
So they may have gathered your LinkedIn profile and know where you work or information about your business and they may direct an attack that seems very realistic. This could be something the IRS has brought forward, a smishing attack recently that they're seeing targeting their users, seeking to get financial information out of them.

Kristin Harper:
Because it looks real, because it's coming from a known trusted source or what you think is a known trusted source, user clicks on that and the same result happens as what happens with phishing, right? Download of malware, they can get at your credentials or they're associating that with other vulnerabilities like a vulnerability in your device that allows them to take over that device and take over your account.

Gene Marks:
And it's not just downloading malware either, although that's the predominant way that these malware gets in. It can also be redirecting you to a malicious website as well. Correct?

Kristin Harper:
Correct. And a lot of times thereafter, your username and credentials.

Gene Marks:
Right.

Kristin Harper:
So your usernames, your passwords, it's things like identifying that, not giving up your username and password to an email or to a text message, validating your source of that information and then using the extra protections like multifactor authentication, which is that second factor in addition to your username and password.

Kristin Harper:
So if they get your password through a technique or something fails that way, there's an extra fail-safe in place with multifactor authentication. So that's one of the ways that users can really protect themselves.

Gene Marks:
Yeah. We're going to get into that because that's really, it is a powerful way. One other thing you mentioned was social engineering. What exactly is that?

Kristin Harper:
So social engineering really has come about in response to the information age. Right? I have a LinkedIn profile, I have a Facebook profile, all those things have information about me.

Gene Marks:
Right.

Kristin Harper:
And social engineering is a conversation like you and I are having and I may call into a call center or your place of business and misrepresent myself. So it is that hands on trying to get information in a different way. So using what I know about the individual, the business to work my way into the organization, same way garner the information I need to start an attack or perpetuate fraud.

Gene Marks:
Got it. So, okay. So let's say I screw up and I've clicked on one of these links, whether it's on my phone or it's an email that I got or whatever and some malware does get downloaded to my device. Right? Either I got directed to a site that had that malicious malware but or it just, it came downloading. What's the impact to that, Kristin? Why should I care?

Kristin Harper:
So absolutely. So as I mentioned, I think over half of the attacks start that way.

Gene Marks:
Yeah.

Kristin Harper:
So it seems innocent, right? And the very first thing you do when you click a link and you sort of realize, "Hey, something doesn't feel right," it's embarrassing. So it's that moment of recognizing that and sort of falling on the sword.

Gene Marks:
Yeah.

Kristin Harper:
And realize, "Okay, this could be the start of something bigger." So the first thing I would suggest doing is reaching out to an IT professional for consultation, for help on that impact, doing some things like changing your passwords. Those type of things, always helpful. But start with that IT consultation and do it quickly. The quicker you say something, the easier it is to stop an attack before it starts.

Gene Marks:
Yeah, that's great advice. Let's talk a little bit about some of the other things that we can do to prevent these things from happening. And like we said earlier, even at Paychex, I mean nothing's a hundred percent secure. Right? I mean, the Department of Defense gets hacked, so there's only so much the IT community can do.

Gene Marks:
But there is a lot of stuff we could do to minimize the risk of getting attacked. You mentioned one that if you do happen to download something, report it immediately, super important. What else can a business owner be doing in their business to lower that risk of attack amongst their employees and of course themselves?

Kristin Harper:
Yes. So I'd be remiss if I didn't start with my job, which is user education.

Gene Marks:
Yeah.

Kristin Harper:
So that can be trainings for your users on how to identify phishing, how to safely browse the web, when to validate a source. It can be something like simulation, simulated phishing emails that you send out across your company.

Kristin Harper:
It's being aware as a business owner and making sure your employees are aware as well. So that's the number one thing we can do. And the other thing is to have those defenses in place but plan for them to fail.

Gene Marks:
Yeah.

Kristin Harper:
So a lot of businesses, it's either not on the radar or there's so much to focus on as a business that you think, "It can't happen to me." And when it does happen, it's super impactful.

Kristin Harper:
So the best thing you can do is plan on what you would do if it does happen. So that can be things like cyber insurance, being there and having a partner in place to help protect your business if something gets through and impacts you. It can be understanding who your partners would be in that space.

Gene Marks:
Sure.

Kristin Harper:
Right? Putting that plan in place, who would I reach out to? Who is my IT vendor? Who would I go to if my systems or networks were failing me due to a cyber attack?

Gene Marks:
Yep, makes sense. Makes sense. I'm pretty sure you can validate, this is why I'd like to hear your thoughts, that the whole... All these employees working from home now because the pandemic and post pandemic now has not helped the situation. In fact, I think it's gotten worse. And I'm wondering if you've got any thoughts or advice for business owners that do have work from home employees, what you should be reminding them to do or doing to make sure that they are limit the risk of getting breached.

Kristin Harper:
What's really important is I would say good habits at work start at home. And so protecting your accounts at home, using strong passwords, not reusing the same password that you use at home on your business account, varying that using password managers, protecting your social media accounts.

Gene Marks:
Yeah.

Kristin Harper:
And things with MFA. All those good habits, make your home network stronger. So when I'm logging into my business from home, I'm protected, I have good hygiene, good habits. In regards to cybersecurity that are already in place, that is the biggest thing that you can do to really help that is make sure that your users are educated and they're protecting themselves everywhere, that good habits exist everywhere, not just at work because my employer says I have to.

Gene Marks:
That's good. I'm going to add something else in is our home routers as well are... Right? I mean, I can't tell you how many clients are...

Kristin Harper:
Absolutely.

Gene Marks:
They're using the same password that Linksys provided when they got their router, which you can get off of their website and anybody can hack into it, right?

Kristin Harper:
Oh my gosh, you're absolutely right. Right? So securing your home network, changing those passwords. And then the other thing that I would say that people overlook, right? Everything's working fine, you think that's great. The second way that attacks happen is through vulnerabilities. And that's because of unpatched software. So check your applications, your phones operating system, your routers firmware.

Gene Marks:
Yeah.

Kristin Harper:
And make sure you have the up to date version on that. Because what happens in those patches and those updates is they're actually fixing security flaws and vulnerabilities that let attackers in.

Kristin Harper:
So in addition, the number one thing, you're absolutely right on, change that password, don't go with the default. And the second best thing that you can do is make sure everything is updated and running the latest version of software.

Gene Marks:
Yep. So don't ignore those messages you're getting from Microsoft or Apple or Google that you need to upgrade your operating system. You should be doing it all the time. Correct? Do-.

Kristin Harper:
A hundred percent. So smart devices, I think at the very beginning...

Gene Marks:
Yeah.

Kristin Harper:
There was sort of this rule of, "I'm going to wait and see if there's a bug in this code before I update to the latest operating system." And we've really seen our smartphone providers, our Apples and Android providers get a whole lot better.

Kristin Harper:
So you're not seeing those flaws in operating systems. And a lot of times those updates are coming because there is a security vulnerability in that device that would allow an attacker, let's say, to have root access to the device.

Gene Marks:
Right.

Kristin Harper:
So without you knowing or clicking a link or doing anything, they're able to get into your device and take control of it.

Gene Marks:
Kristin, does security software still have a rolled out...as I mean, did you remember, it wasn't that long ago where you had to have Symantec or Norton AntiVirus or all those were running on your system.

Gene Marks:
I know they're still out there. But because clients ask me this question, it's the same question. They're like, "Listen, if I'm running the most recent version of Windows 11 and I've changed my passwords and all that, do I still need to have security software as well on my device?" Give me your thoughts on that as well. Do you recommend that?

Kristin Harper:
Yes, absolutely. A tiered defense is always better.

Gene Marks:
Yeah.

Kristin Harper:
So there's some inherent protections that come with your operating system, but adding to that, you're really adding to your layers of defense. So there's more that an attacker would have to go through.

Gene Marks:
Right.

Kristin Harper:
To be able to compromise your systems. So always great to consult with an IT professional on what exactly would work best for you and your business, but absolutely don't go with your standard configurations.

Gene Marks:
Great. That is great. So let's recap a little bit, okay? So we're upgrading, getting all the patches done on all of our software and operating systems. We should have security system software running. For our work at home workers, we need to make sure that their routers are secured as well, their firmware is updated, their passwords are also more complex and certainly changed.

Gene Marks:
Most importantly though, of course is training and making sure that people can, they're aware of what a potential phishing or a smishing attack is or if they're being social engineered. All of this either compromises our personal data but then also if somebody breaches one of our devices they can get access to our companies systems as well.

Gene Marks:
Some final thoughts. Oh you also mentioned about cyber insurance as well. You have a lot of great information. Cyber insurance is another really good thing to make sure that you've got. How about backups, Kristin? I mean, and some thoughts on cloud based provider?

Gene Marks:
There's a bunch of managed services providers that are available now and I have a lot of my clients going to them and saying, "We're not going to have it internally, we'll have somebody else host it for me." Some people say, "Oh I don't know. I don't want to put my stuff in the cloud because it's less secure."

Gene Marks:
And I don't know if you have thoughts. I certainly do. I'd like to hear your thoughts. Is putting stuff in the cloud with a managed service provider less secure than having it on a server in the basement of your home or wherever your small business needs to be? Kind of leading you with that answer, but what are your thoughts?

Kristin Harper:
Yeah, absolutely. So my thoughts on this are I see cyber threats changing day in and day out. So certainly if you don't want to be the one responsible for staying on top of that, always a good idea to consult with an IT professional, a security professional on what's best for your organization.

Kristin Harper:
There are pluses and minuses, right? To that server in your basement, to your point, right? It's on you. And you may not want that, but cloud configuration and cloud security is a big topic. It's expanding in the world. And making sure that that's configured in a way for you that's secure and that you're working with a reputable provider is really important.

Gene Marks:
Just sounds like this is just a cost that businesses are just have to bear, particularly if they have people working remotely and independently. There are so many chances of being breached, which can just disrupt your business like you said, to no ends.

Gene Marks:
In some cases, put you out of business. That some other recurring costs like insurance, your payroll service, your accounting firm, there are certain costs you're going to have to run your business and one of them is going to have to be IT support to make sure that your security is up to date.

Gene Marks:
Kristin, am I forgetting anything else? Do you have any other final words of advice for our audience on making sure they keep their, not only their personal devices, their employees devices, their networks secure or have we covered it all?

Kristin Harper:
I think we've got it, Gene.

Gene Marks:
I think so too. Kristin Harper is the Manager of Operations Security at Paychex. Kristin is eyeball deep at all of these security issues and that's why we wanted to have her on for Cybersecurity Awareness Month. Kristin, great information.

Gene Marks:
Thank you very much for sharing it with us. I am sure we'll have you back at some time in the future and you're going to have lots of more horror stories to tell about ways that we could be attacked and what to do to protect ourselves. But for now this is great. So thank you so much.

Kristin Harper:
Thanks for having me on and happy Cybersecurity Awareness Month.

Gene Marks:
Happy Cybersecurity Awareness Month. Everybody, you've been listening to Paychex THRIVE Podcast. My name is Gene Marks. Thanks for joining us. Do you have a topic or a guest that you would like to hear on Thrive? Please let us know. Visit payx.me/thrivetopics and send us your ideas or matters of interest.

Gene Marks:
Also, if your business is looking to simplify your HR, payroll, benefits, or insurance services, see how Paychex can help. Visit the resource hub at paychecks.com/worx. That's W-O-R-X. Paychex can help manage those complexities while you focus on all the ways you want your business to thrive. I'm your host, Gene Marks, and thanks for joining us. Till next time, take care.

Speaker 1: