Season 2 | Episode 63

With Cyber Attacks on the Rise, What Can You Do to Protect Your Business?

PAYCHEX
Business Series
Coronavirus

Gene Marks

CPA, Columnist, and Host

Rick McElroy

Principal Cybersecurity Strategist at VMware

Full transcript

Gene Marks:
Hey everybody and welcome back to the Paychex Business Series podcast. I'm your host Gene Marks. Thank you so much for joining me. As you're aware, I write in a lot of different places, anywhere from the Hill to the Guardian, to the Washington Times, Philadelphia Inquirer every week. I also write in Forbes every week as well, actually six times a month. And I cover technology for small business for Forbes. This week's episode is something near and dear to my heart. It has to do with security.

Gene Marks:
It also has to do specifically with the security issues that we all should be aware of when working from home as business owners and things we want to do to protect ourselves. So, I've got a lot of questions for our guests. Our guest is Rick McElroy. Rick is going to be talking to us about all of the different things that we need to be aware of. And Rick let me pull you on right now and introduce you. Say hello to the fans.

Rick McElroy:
Hey everyone. Gene, thanks for having me. I'm super happy to be here to talk to small business owners. It's a passion of mine. And so I'm glad that your focus is for that group of business owners.

Gene Marks:
Good. I'm glad. Yeah. I mean, we're all burdened with a lot of different things that we know and don't know, security is one of the things that are obviously a huge issue facing small businesses around the country. Rick, you are the Principal Cyber Security Strategist at VMware. So, question number one is what exactly is VMware? And question number two is what the heck does it mean when you say you're a Principal Cybersecurity Strategist? So, go.

Rick McElroy:
Great question. Yeah. VMware, I think most famously pioneered the technology behind the Cloud. Now so the ability to take multiple servers and run those as virtualized infrastructures. So, when we looked at the explosive growth of the Cloud and all of those things, predominantly that's where VMware started. But they haven't rested on their laurels. Subsequent to that, they've added software as a service around networking. They handle thinning out the attack surface through things like workspace one, but virtual desktop offerings. And then of course, what we came on board to do, which is really, I think, provide better security outcomes for VMware's customers and more broadly, organizations.

Gene Marks:
Yeah. I remember VMware back in the day. I mean just so you know, I run like a technology consulting firm out of Philly and we do mostly like CRN applications. But I've been doing this for like 25 years and back in the days with Goldmine and Act, if I can date myself. And VMware was like a big part of it. I mean, virtualization because a lot of people were sick of synchronizing data. So, they wanted virtual access to their systems and people were, are you a VMware shop? Are you a Microsoft shop? These are all different options that people had. So, you do security. When you say Principal Cybersecurity Strategist, that's like a fairly broad title. Do you specialize in anything specific?

Rick McElroy:
I think I do. I mean, one of the big passions I have and specifically why I came over to Carbon Black is really around this idea of proactive security and threat hunting. So, when you looked at sort of where we were as an industry, this idea that you can buy a piece of technology and have an alert and that alert is meaningful and actually stops breaches, simply hasn't proven to be the case. And so we believe in the broadest coverage of visibility possible. So, when we speak about security, what we're actually talking about, is being able to turn the lights on so that when the attackers are inside of your house, they breached the perimeters of your home or your apartment building, what ever the case may be, they actually know where they are.

Rick McElroy:
And you know the appropriate responses to that. From a human perspective, if this happened in the real world. Well, we turn our lights on if it was the middle of the night, we call law enforcement and, or use some sort of weapon at our bedside to protect ourselves. But organizations aren't set up that way, right? And so I think I really came here to lead and champion the efforts around getting proactive and actually taking the infrastructure that the adversaries have breached and owned and compromised taking that back from them and giving it back to organizations. And so that's what I'm most passionate about.

Gene Marks:
Yeah, you're talking about infrastructure and the definition of that has been evolving particularly because of COVID, a lot of people sent home to work. So suddenly our infrastructure, which might've used to have included people just coming into the office and working off their desktops. Now it's working off of a Windows 95 machine that they're sharing with their 14 year old daughter. And that has a big impact on overall infrastructure. So Rick, I want to focus on remote working right now. And I want you to talk to me, I want you to scare me about all of the security threats, what we need to be aware of as our employees are not only working from home, but as clearly working from home and working from anywhere is going to be a critical part of our benefits plans going forward. This is going to be long-term lasting from COVID. Tell me about what we should be scared about from a security perspective?

Rick McElroy:
Yeah. Look, I think one of the things is when you look at home network technologies and the back commercial space, so your typical home Wi-Fi that we put in, the internet of thing devices, whether it's a toothbrush, whether it's a TV, whether it's an Alexa Home, whatever those cases may be, have Massively expanded what we refer to as the threat surface. And so that threat surface is really the areas that the attackers use to actually get to the things that they want to. And so in most cases, look, they want an ROI. They want to ransom, corporate systems, or a home system that you need to access corporate devices. Or they're going to do it for intelligence gathering purposes since some other, more nefarious thing. But by and far, I think SMB is really feeling the pain of ransomware.

Rick McElroy:
And that's the primary way that these threats are manifesting themselves. And so things we didn't think of prior to the pandemic that occurred, some people couldn't come back to the office. And so IT teams across the globe had to buy new equipment. They had to allow some of their employees to go to BestBuy or Fry's or wherever the case may be to procure a brand new equipment. That equipment did not have corporate security devices and pools that were put on it, simply put we're relying on the same old network infrastructure for the purposes of sharing our content and, or doing video streaming with our family that we do for businesses. So, even the idea that we're not digitally distancing our networks, meaning I don't have two networks to do work from. And then to do all of the things that might be a little riskier from a human perspective.

Rick McElroy:
And of course I want to use social media. Of course, I want to use apps, all of these things. And so I think what it's really done is given the attackers, just this huge area to come after organizations. And secondarily, I would say the other thing that happened is a lot of times whether we were using Cloud services or had a security team, or IT team, a lot of the tooling was built around protecting the offices, protecting the physical data centers. But not necessarily at the point of interaction with data, which is what we need to rethink from a security perspective. So, it's really about having great security and there's solutions out there to do that. But it has to be present at where your users are interacting with that data. And so you got to have some strong end point security out there to help alleviate some of these risks.

Gene Marks:
Yeah. You mentioned some of the ways that people can get access to our networks and you briefly mentioned IoT, which means Internet of Things. I recently wrote in Entrepreneur magazine about a casino that got hacked there and data stolen. The hackers found their way into their database through a thermometer on a fish tank on the casino floor, because all of these … And I just want to kind of reemphasize that, we've got Alexa devices and voice devices in the home. We've got refrigerators that are smart appliances, we've got the Roombas that are connecting to the internet. I mean, I'm assuming that once these devices, all these devices of the nest security things. If a hacker gets access to one of these devices, then they get access to our network and therefore they can get access to our data. Is that fair?

Rick McElroy:
Yeah, absolutely. So, what we refer to that as in the industry is lateral movement. But I know that's probably a technical term for some of the audience. What do I really mean by that? So look, my background, I actually started off on the offensive side of that [inaudible 00:09:04], breaking into e-commerce companies. Subsequent to that, did that for the Department of Defense, Department of Navy, and the Marine Corps, also. But what do we really care about? I have a, what I refer to as a foothold on a network and maybe that foothold, that initial point of presence is an IoT device that simply put the developers didn't build good enough security into it. Now I'm on a network. Now I want to see what else is on that network or what else can I get to? What are the other things?

Rick McElroy:
And so I'm going to perform an enormous amount of what I call reconnaissance once I'm actually inside of an environment to figure out how to move around, to get to the target that's going to give them the greatest sense of urgency from a ransom perspective. Or that data that has a high resale value on the dark web. And that's what I care about. And so there's a lot of times where attackers aren't actually launching a piece of ransomware or a nefarious piece of malware. What they're actually doing is learning about how you interact with your computing systems and these accounts that are associated with the identities. And so what they truly care about are getting a hold of the identities and misusing those and then moving around to as many things as possible. And so you have highlighted, I think a key risk there.

Gene Marks:
And make no mistake about it. I mean, the way the hackers are doing this nowadays is quite complex. I mean, this is not some guy like Mr. Robot, just getting access, which is a great show by the way. But getting access to different, you know spending time on it. They have bots and they have Artificial Intelligence, and they have automation that's going on, I'm assuming. They can do this to hundreds or thousands of devices at any given time, following scripts and algorithms that are looking for those weaknesses. Correct?

Rick McElroy:
Yeah, absolutely. And generally speaking, what I talk about is the business behind cyber crime. I'm seeing this rise in sophistication, the rise in innovation. And so you have the dynamics of nation states competing for cyber warfare and building munition. But let's talk about what the cyber criminals have done, because I think that's a larger impact to small and medium businesses. Starting around 2016, they built massive amount of infrastructures to do what we refer to as ransomware as a service. And when you think about Cloud services from a CEO or a small business perspective, you need an email and you need some way to communicate with your customers. You need a website. You're going to go pay Microsoft, Amazon, Google, VMware, or someone to do that. Well, conversely on the bad guy side of the house, they're doing the same thing. And so it's not about actually knowing how to write malware anymore.

Rick McElroy:
It's not about knowing a specific technique, tactic and procedure or writing a Zero Day. What it's about is having some version of cryptocurrency going on to dark web forums, engaging with someone who has a Cloud service to do extortion at scale, or access mining, or credential harvesting, whatever the case may be. And then I can commit that across a broad, massive set, hundreds of thousands of devices, which is why you see some of these numbers go that big. So, I think the important thing for the audience to remember is it runs like a business, just like your business. They have quality assurance, they have metrics so that they can advertise. They have affiliate programs and partner programs. And it's gotten fairly pervasive and it's ... Oh, by the way, now a $1.5 trillion market. And it's proposed that it's looking like by 2025, it's going to be a $10 trillion cyber crime economy, which means, hey, we got to stop paying some ransoms and we've got to do better on defense to help bust that economy out.

Gene Marks:
You mentioned very briefly about crypto and I do want to get into some of your advice, how to protect ourselves. But just to also offer another warning, people like to talk about data being hacked and ransomware and all of that. But is there not a rise, a growing trend, as cryptocurrencies become that much more popular where a lot of the hackers want to kidnap a lot of computers as it is. So, to help use that computing power to mine cryptocurrency. Even though your data might not necessarily being hacked, your device is being compromised, because it's being used. Can you explain that a little bit? Do you agree? And can you explain that?

Rick McElroy:
Yes. Yeah, we absolutely agree. We refer to that phenomenon as crypto jacking. So, essentially, some malicious actor out there gets a foothold on a system. It could be a windows system, could be Mac could be Linux. It doesn't actually matter. We've seen it on mobile devices as well. So, what do they want to do? They want to mine crypto. So, they want to make it not steal it. So, you get a higher ROI, if you can make it, especially when you have these rising numbers when it's associated crypto. Largely Bitcoin I think gets the by far media market share, but there's some other currencies out there Minero specifically that's used generally when it comes to crypto mining, because you can actually do it on normal Intel processors and not some custom thing. All that being said, look, the adversary, once they have a foothold on your system, they're going to use that for a number of different things.

Rick McElroy:
They'll use it for launch attacks against your partners, against other entities. They'll use it as part of its zombie bot network to do nefarious things like distributed denial-of-service. And then of course, they're going to monetize through crypto jacking. The important thing to know with cryptocurrencies, that there are nation states active in this game today that are using this as a means to bypass sanctions that have been levied against them. And so they're actively paying for some of their more nefarious programs by doing cyber crime, which again has caused this massive increase in the amount that's occurring across the globe.

Gene Marks:
Okay. So, we've established all the different types of threats that are out there. At least some of the more significant ones. We are under a threat. Our data can be compromised. Our computers, our devices can be compromised. All of this has been exacerbated because so many people are working from home. So, let's talk about what some of the stuff that we can do. I'm going to throw out some things to you, one at a time, and just get your point of view on it, okay? For starters, someone has told me, and this is right up VMware's alley. Like Gene, you should absolutely have a VPN, a Virtual Private Network. Not only on the devices in your home, but when you go traveling around, a VPN is … Well, none of these, by the way, are a silver bullet. They won't provide a hundred percent security, but what are your thoughts? First of all, do you agree? What are your thoughts on a VPN? What is a VPN?

Rick McElroy:
Yeah. So, a VPN simply put is the Virtual Private Network. Essentially, it's a technology that attempts to keep the data as it traverses various networks. In this case, let's say you're going to a website to enter a password on that website. Well, there's a whole chain and a whole bunch of infrastructure that exists between you and that server you're entering your password. The Virtual Private Network encrypts that [inaudible 00:16:25], so that attackers can't sit in the middle of that transaction and do something which we refer to as man in the middle, it was one of my specialties back in the day, and sniff those passwords and snip that [inaudible 00:16:37]. So I would say, it's good for privacy along with security. However, we've also seen to your earlier point. We've also seen VPNs get leveraged nefariously because they're inconfigured wrong, or they don't have proper monitoring overdose.

Rick McElroy:
And so what you've seen the industry do to address that is application writers are pushing that layer of security down into the applications. And so there's a number of apps today, there's a number of solutions that provide VPNs inherently to it, to protect against that. But as a general rule, if you're a small business owner, go get a VPN, make sure that you're not just attaching to public Wi-Fi. They are owned in airports. And when we refer to something as being owned, it's not the people that bought it. It's the attackers that currently have ownership of that infrastructure. And we see it all the time.

Gene Marks:
It's definitely one of my goals for this summer is we're going to equip the people in my company all with VPN. I mean, you can subscribe to services if you google VPN software, there's plenty you can subscribe to. Relatively inexpensive. And I think the other bonus is I can start watching some of my favorite shows on the BBC, if you want to know where I'm coming from. But don't tell anybody that. Okay, so that's your thoughts on VPN. Upgrades. I've had IT specialists, security people tell me, Gene, there's a lot of different things you can do. But one of the most important thing you have to be doing is upgrading your device's operating system, as annoying as it is. And that should be across the board, all of your employees, wherever they are. Give me your thoughts on upgrading operating systems.

Rick McElroy:
One of the number one ... Forget ransomware, forget phishing. We hear all this stuff. When you go all the way back to the root causes like, what happened. In most of the cases of the fundamentals of security, so patching is one of those fundamentals, system updates is missing. Now, the larger you get as an enterprise, the more scrutiny and quality assurance you're going to put over this process. With that being said, if you have a Windows box today, if you have a laptop, if you're running a surface device, if you're running an iPad. Turn on automatic updates and let them run. And here's why. As an IP security professional, as an IT professional, I would rather troubleshoot a path that I put on a system or an update that I put on a system where it breaks the system.

Rick McElroy:
Then I would having a malicious hacker take advantage of that and running around. Because the level of effort is much higher. And Microsoft has been doing a pretty wonderful job with their updates along with Apple. So, I'll leave like SQL databases and stuff out of this discussion, but strictly speaking to end points, firm them on, get them updated as fast as possible. The manufacturers are working as hard as they can when issues are identified to get them out there. And I can't actually remember the last time my Windows box broke because I did an update to it. So, just get it done.

Gene Marks:
There was a time when Microsoft updates was an enormous pain-

Rick McElroy:
A mess.

Gene Marks:
Yeah. It was a mess. And you're right, they've definitely gotten much, much at better doing it. What about if you've got employees working from home? That's what the conversation is about. Is there anything that you can recommend for me to make sure that my employees are running the most recent versions of Windows or iOS short of me knocking on their door and inspecting what they have?

Rick McElroy:
Sure. And look, there's a number of solutions. VMware has some. So, I'm hesitant to give you a ringing endorsement of one particular product. That being said, yes, we're here to help. The IT community and the IT security community has in fact had solutions for a number of years to help enforce things like system updates, to make sure that the security controls over that device are good. And then of course, to record activity and ensure that the cyber criminals aren't on their doing something as well. My big message, I think, for small and medium businesses is look, security is not a zero investment game. It's just not. It is going to take some investment. I think if you frame it and think about it in terms of safety, you're really providing a safe environment for your employees, for your customers, for your partners.

Rick McElroy:
You're going to build some money in to do that. And then you're going to have to be smart as a small and medium business. And one of those areas I think you can get smart on is through partnerships. Now, what's happened over the last five or six years is these high-end security providers where it used to be really costly to bring in a team, to look at your data and, or provide security services as the economy of scale has dropped on that. And so there's a number of very reasonable, very affordable partners and solutions out there that will help you with these challenges. And then of course ensure that all you need to be focused on is building your business and growing it. Let the professionals come in, let them help you, let them give you some good advice. And then I would just say, listen to your partner. So, if you're going to partner with someone, really listen to them. We're, again, here to help.

Gene Marks:
Yeah. You mentioned about the professionals and people that specialize in this stuff. And you talk about spending money. I mean, I think another big area is training for your people as well. And every study that I read about this, Rick, is, it's user error. Somebody clicked on the wrong link, because we're dopes. We don't know what we're looking at. We're going to some phishing website to respond to an email that we think it's from the CEO of the company, but it's not. Talk to me a little bit about your advice on training.

Rick McElroy:
Yeah. So, I believe in training. But I think it's got to be effective. I also operate on the premise that people are going to click. I mean, if you look at any of the apps on your phone where we train our next generation to click on things. So, I do think security and IT has a responsibility with that to meet the user at the point of interaction with the data. That being said, I think security training has changed over the pandemic. It was fairly typical and some people on the phone may have went through courses where, hey, this is a phishing link. But what's happened due to the pandemic is we've blended our home and work lives. And so even when I used to go into an office, I would know I had a badge, I had to badge in, I was aware of the policies, I was aware of there was cameras.

Rick McElroy:
So, my behavior would change as a result of that. Because I would remember that I went through training and, hey, I can't just leave social security numbers printed out on a printer, right? So, this idea that like we blended our home lives of work lives, I think does need us to revamp how we're doing education. And then secondarily, I would say, I think the idea that we can just push out like a little video training and expect user behavior to change. It's a little incorrect. And so again, what we have to be in the business of is positive behavioral changes. And then there's a number of ways to do that. But step one is you have to have security and compliance training. And then you just have to drive to make an effective. So look, if you have a learning and development department. Awesome. Work with, because they understand how people learn. So, we're not always, as security professionals, the smartest people about that. But I think if we pay attention and ask the right questions, we can get to a better spot with education and awareness.

Gene Marks:
Okay. Two more quick questions for you then I'll let you go. Number one is passwords and multifactor authentication. First of all, I just started using a password vault recently, Keeper it's called. And it's excellent. And so I'm advising everybody in my company to do the same. Multi-factor authentication, for those of you guys, most people know about it already. You log in as a password, you get a text sent back to you, usually your phone, and you respond with it with a ... Again, it was this thing to like a reply all podcast recently, an episode and they were talking about easily even multi-factor authentication can be, you can get around. Its so easy to spoof a cell phone. What are your thoughts on password security and MFA?

Rick McElroy:
They're not wrong. And I say this all the time, MFA is not a silver bullet. I think you mentioned other things that we rec--. Stem cloning is a legit risk that happens. And generally speaking that has to be a targeted attack. So, I talked about those macroeconomics earlier, this 1.5 trillion heading towards a 10 trillion dollar market. Well, why? Because the attackers get to automate all the stuff that they do. They are taking manual steps and interacting with system once they're on there. But like the defensive evasion pieces, all of the stuff that they do, that's all automated and so there's no cost to them. MFA specifically goes after one of the things they care about the most. So, I mentioned these earlier. One is I want to move around and spread as far as possible.

Rick McElroy:
The second one is I want your identity. I want your credentials. Well, the methods that the attackers use to pull that off, honestly, don't change very often and they're pretty rudimentary. And in my humble opinion, we should've just defeated those already. So, MFA squarely sits at this idea that an attacker is going to have to take some manual action. They're going to have to work harder to go after your credentials versus going after one of your competitors or someone else. And here's what we know about attackers. They are lazy. Like, yes, they will, especially if they're a nation state, they'll spend millions of dollars to go after you. But the most of the cyber criminals are lazy and they want an ROI, return on investment, as fast as possible on that attack. If you can stop the credential harvesting, the chances of them moving on are very high.

Rick McElroy:
So, they're going to move from you as a target to someone else. And MFA represents, I think a great way that all of us can instantly raise the bar against these attackers and really helps. It's a top recommendation for me right now. And it does, again, has to be implemented well, and it doesn't come as a silver bullet. But let's at least make them have to go swap my ... if I make them have to go do a SIM cloning on my phone, I consider that a win, because I've made them work that much harder.

Gene Marks:
Yeah. It's fair enough. I mean, they're looking for the low-hanging fruit and obviously the harder that you make it for them, it's not impossible, but they're more likely to move on. Final topic and we've had this whole conversation, Rick. We've talked about putting in a VPN, upgrading your operating system, multifactor authentication, having a password vault for your passwords with complex passwords is what I do. Getting training for your people. And I hear this from other security people, I hear less and less about security software. I mean there was the day where you would be like, you just get Norton™ or you get McAfee®. And then it runs in the background and you're secure. I mean there's still a need for that. But it just seems like it's falling down the priority list. And I don't know if that's just me or not.

Rick McElroy:
Well, that's interesting. I would make the argument security is becoming intrinsic to technology as it's delivered. And so, it's a big part of what VMware is working on. It's a big part of what Microsoft is working on. So, Microsoft has done, I think some amazing … Apple has done some amazing work when it comes to a lot of the methods that these attackers use to breach the data. They're going to continue from an operating system, thinning that out, making it much more difficult. But no, you still need to what we refer to as layered security or defense in depth. I actually think to your point about, well, I had Norton or this one piece. I think that that was miss sold to the public. Saying that I only need one security tool.

Rick McElroy:
I'm just going to tell you if anybody tells you that they're probably selling you snake oil. You will need multiple security tools in a stack, but that's not to say that you need to massively increase your complexity. Because here's what we see. Cloud vendors are starting to bake in a lot of these security technologies into the Cloud. So, if I'm an Amazon customer, an AWS customer. I get to take advantage of a bunch of the things they're already doing, which is great, which means my team doesn't necessarily have to perform those functions. But they do have to audit. They do have to provide oversight and ensure that contractually my Cloud providers are doing that. So, I think it's just another area where we're starting to consolidate security into our technology stacks. And we're ensuring that our vendors are baking that in, which is good. I think it's a good move.

Gene Marks:
It's good to know that at least the vendors … I think that's ultimately where we're going to go, particularly for small businesses. I mean, if you've got QuickBooks, you've got Dynamics, you've got Zoho. You want to rely on those vendors to be the ones that are providing [crosstalk 00:29:24].

Rick McElroy:
Yeah. And they have a number of cool controls that they're doing. It's not to say that an attacker couldn't find something tomorrow. But they've got a team. They have [crosstalk 00:29:32] programs. Yeah. Yeah.

Gene Marks:
Makes sense. Rick McElroy is the Principal Cyber Security Strategist at VMware. He can be reached at InfoSecRick, I-N-F-O-S-E-C-R-I-C-K. Rick, great conversation. Thank you so much for all this information. I'd like to have you back. I have more questions to ask you. We have a limited amount of time, but yeah. Thank you. I appreciate it. Guys, my name is Gene Marks. If you need more help, advice, tips for running a business, please visit us at paychex.com/worx, that's W-O-R-X. Thanks very much for joining us this time. We look forward to seeing you again on our next upcoming episode, take care.

Speaker 3:
This podcast is property of Paychex, Inc. 2021. All rights reserved.