BANK OF AMERICA

New perspectives on cyber awareness

Host: Jonathon Traer-Clark

Co-hosts:

- Mary Rosendahl, Managing Director, CashPro Security Product Executive
- Roland Chan, Cyber Crime Client Executive in Global Information Security

Jonathon:	00:00	You're listening to the Treasury Insights Podcast. This podcast is part of our broader objective to foster a treasury relationship that prepares you for the future, supports more strategic decision-making, creates efficiencies and helps manage risk. Put it another way we want to give you the power to see what's next. The global shift to remote working, has created further cyber security vulnerabilities, which compounded by other pandemic related factors, such as disruptions to day-to-day business processes. According to a recent survey, cybersecurity professionals have observed a 63% increase in cyber-attacks related to the pandemic. I'm Jonathon Traer-Clark, Managing Director Global Transaction Services. And with me today is Mary Rosendahl, Managing Director, CashPro Security Product Executive and Roland Chan, Cyber Crime Client Executive in Global Information Security at Bank of America. We will examine how you can create a cyber training program that aligns with your company's culture and helps to manage cyber risks and potential fraud. Mary, Roland welcome!
Roland:	01:13	Thanks Jonathan.
Mary:	01:14	Thank you.
Jonathon:	01:16	Roland, let's start with you. The global pandemic has set the stage for bad actors looking to exploit the vulnerabilities of remote access. How would you evaluate and manage cyber risks given that context within your organization?
Roland:	01:30	You're absolutely right. The pandemic has really forced every organization to reevaluate how they work every day. Now where the work from home posture for most organizations today, they've had to get really creative of how to measure and monitor risk, not just an insider or external threats, but really overall compensating controls.
Jonathon:	01:54	Can you elaborate a little bit more on that? What do you mean by compensating controls?
Roland:	01:58	If you think about, we're talking about insider threats, let's focus on that specifically. If you're looking to protect your organization, you have to have compensating controls about activity that's going on for employees. And if you think about our activity of either malicious or non-malicious activity, there just several variables that are in play today, with the current pandemic and the current environment, the current posture. If you think

about there's obviously technologies that exist that are out there today that can help implement some of these controls and detect some of this activity, but cybersecurity is not just a technology issue; it is a behavioral one.

Jonathon: 02:38 I understand. If I play back what you're saying, and I think Mary, you're going to add a bit here as well, you're essentially saying we need to consider two elements. It's not just the technological side, which I think is what people naturally gravitate towards. It's also the human side, our behaviors, the way we manage risk, the way we look at things. And perhaps even our, on the call, whether we click on things to put it more simply than that, Mary, perhaps the cut to you to get your perspective?

Mary: 03:04 I want just to piggyback a little bit on what Roland said. We had all these companies scrambling to get ready for the work from home posture, with the pandemic. Now we've got to take a look and say some of these companies are now going to stay with folks working from home. We need to take a look at that, re-look at what they set up and is the posture secure? Is it sustainable? What kind of entitlements and lease privileges have we set? That least privileged model that we always talk about and have we really looked at that now that we're operating differently with this pandemic. And I think that's one of the main things we need to look at that and then companies need to take a risk assessment and identify the company's most important assets, determine who can access those and then put the appropriate controls in place. Then we can monitor network activity, limit sensitive data, prohibit the transfer, because what makes insiders, and your people more unique, is that they right now do have legitimate, trusted access to your systems, but as an organization, then we need to look at that, and make sure that we've got the right controls around it, to make sure that that data is appropriately protected. Like Roland had said, not only do we need to look at the accesses within the company, but then how are these companies operating today to make sure that their employees are working in safe environments?

Jonathon: 04:39 Thanks, Mary, a lot of points there, but if I may paraphrase a little bit. So, essentially what we're saying is that control mechanism that we put around employees, technology for want of a better way of putting it. In other words, the walls that protect the data, integrity, the systems and the processes, I like the expression least privilege. You're entitled to do what you need to do for your job and your role and your function. We've almost had to think about how that extends out when if you like people are now accessing our systems remotely, when they're not in a workplace environment, they're now in a home environment, and therefore that presents different risks, cause we don't have control over, for example, the Internet connectivity in the home environment. Is that fair, or am I being too simplistic?

Jonathon: 08:12 David just sticking with you. That's interesting. I'm going to call it - information reporting. But it's also; you can execute instructions as well, through these channels. You're not constrained to executing an instruction with one bank. You actually execute it through any of the banks that you deal with because they all operate to common standards.

Roland: 05:22 Well, I think you should have some control of your Internet access, and the way you look at it, is it secure? Just like Mary said, we can have specific controls in place within our four walls of an organization, as a company from a technology side, but there should be the same type of controls that your employees, should take at home and some of those is connectivity. Is your wireless Internet service secure? Is it protected? Is it something that you have a robust, complicated password that can't be compromised? What is your work from home situation look like? Where are you sitting? Are you in a situation where you have other people around you, or do you have any home listening devices that are personal aides that we know most houses have today? You have to be really cognizant of a lot of the elements that you've gotten accustomed to and being around, but really heightened the awareness of, if I'm talking about specific data or information for work, then I need to make sure that I'm in an area that I can speak safely about it for my job whatever that job may be. It could be technology, it could be finances, it all depends on what your job requires.

Jonathon: 06:39 It's interesting I've seen notices on elevators, for example, that say, please, don't discuss company business outside in public spaces. That's verbal communication, but what we're essentially saying is there's electronic chatter through wireless connectivity and so on that equally can be overheard by some of the devices you mentioned, or if your home environment isn't perhaps as secure as it should be. Given all that, how do we get our employees to understand that scenario, and then how do we help them to create an environment and a culture that kind of questions that, and then helps to meet and remediate it?

Mary: 07:15 I want to say one thing that kind of where Roland was going in the beginning, when we look at the organization and what's happening today, and we look at the pandemic, typically one of the factors that we would do as managers is to visibly see the temperament of employees. Because we know now there's more people under financial pressure. Organizations just need to be more on a higher alert because we're not in the physical setting to actually evaluate the temperament of what we're seeing in the office and the people we're working with. Now, to go specifically to your question, is the training, which Roland in Global Information Security just rolled out this really great cybersecurity journal. And it's going to talk about some of these fundamentals, don't skip the onboarding and the training, it's critical. It can't just happen once and done, but what a company's doing to look at their training policies that they've had in place when everybody was working in the office and what needs to change, how

		do they need to reinvent that wheel now that they have a more employees dispersed?
Jonathon:	08:23	That's great, Mary, thank you! And it can be potentially perceived as cultural aspects can be perceived negatively, how do you go about doing it in a positive fashion? How do we make employees infused about being cyber aware and enhancing that culture while simultaneously protecting our system?
Roland:	08:41	I think messaging and support has to be a top-down approach. The support of your C-suite and senior management is critical. The more you can empower your employees to be more successful around this program of cybersecurity awareness; the better program you can have. For example, do your senior management sponsor the positive messaging? Is there positive reinforcement around it? Do your employees have the freedom to ask needed questions, to make sure that they can continue to follow established protocols that are set in place for your organization without the fear of senior management questioning or their managers really questioning what they're doing? And the ultimate goal, as Mary mentioned, is protecting your organization. The more, I think, you can establish that trust with your team is key, establish that right culture, the right behaviors.
Jonathon:	09:39	You both touch on a number of interesting points; I completely agree about. In the pandemic, they love the social interaction that can be gained through them and various different applications and platforms. How do we keep our employees broadminded enough to be able to understand that you can get instant messages, you can get telephone calls and all sorts of different things? How do we go about creating that learning culture, that it's not just the password? It could be any form of engagement?
Mary:	10:08	From my perspective, it's actually showing examples, making it real so that employees understand how easily their email can be actually hacked. The malware gets into the company system, right, and then they take over those accounts. Companies are talking about it; they're sharing about it, so that they see it's real, and how it can happen. The more examples that companies bring to their employees to show real life examples, the more it's going to resonate them, that this isn't just make believe in a fairy tale, but this is happening every day at companies.
Jonathon:	10:45	Thank you for that. Mary, obviously, CashPro is one of our core offerings. Have you seen an uptick in engagement from clients wanting to understand more about, not just CashPro security itself, but also how they can perhaps take some of those tools and techniques and impart them across their own infrastructure and systems?
Mary:	11:04	Absolutely. As Roland had talked about, training is so critical, and what

we've seen with best practices of companies is that they're actually attending these webinars because educated folks are typically the ones that aren't taken advantage of because they're learning about the scams, they're understanding what's happening. For example, we've had an uptick of hearing about vishing scams, where fraudsters are pretending to be service centers, whether at telecoms or banks or whatever, and tricking individuals to giving up credentials, actually even sometimes generating one-time passwords. Having that knowledge, paying attention to webinars, where you're getting current information on what the latest scams are, how powerful is that? To go back to your employees and say, this is happening because we know when somebody gets on a phone call and they get terrorized by one of these elaborate scams, they don't think, right? And we need to teach people to slow it down, to think about exactly what you said. Would you give this information to somebody? Why aren't you going back to your source system, you know, hang the phone? Back to the main thought here is, the fact is education, understanding scams, what's the best practices, so you can go back and talk to your employees about the latest.

Jonathon: 12:24 Very interesting. And it's that circular feedback loop, which you both referenced. The learning is ongoing; techniques evolve, cyber criminals manifest new ways to try to extract information from us. So, the process is ongoing. It's not a one-time event. The culture has to be one of continual reinforcement and learning.

Mary: 12:45 Exactly.

Roland: 12:46 Our world just does not stay static. Cyber criminals find ways to exploit and compromise. The challenge that we have as security professionals to make sure we can stay in front of that.

Jonathon: 12:58 Perfect! What a great way to conclude. Mary, Roland thank you very much! I think we'll end it there. Some extraordinary insights from both of you. I think we'll all be watching this as it evolves over time, as it has continued to evolve in the past. So, thank you very much, both of you!

Mary: 13:13 It's a pleasure to be here. Thank you.

Roland: 13:15 Thanks, Jonathon.

Jonathon: 13:17 Thank you! You've been listening to Treasury Insights. I'm Jonathon Traer-Clark, Managing Director Global Transaction Services. My co-hosts today are Mary Rosendahl, Managing Director GTS Fraud and Cybersecurity and Roland Chan, Cyber Crime Client Executive Global Information Security. As each day brings innovation and an opportunity, we are dedicated to working with you to turn technological advances into intelligent treasury.