TABLE OF EXPERTS

CYBERSECURITY

The Minneapolis-St. Paul Business Journal held a panel discussion recently about cybersecurity.

Panelists included Emy Johnson, chief security officer at Allina Health; Wolf Lewis, Regional Vice President, Comcast Business Midwest Region; and Angie Propp, VP Cash Management Sales Manager, Highland Bank. John Ebert, professor and Cybersecurity Program Director, Saint Mary's University, served as moderator.

PANELISTS

JOHN EBERT / MODERATOR

Professor and Cybersecurity Program Director, Saint Mary's University of Minnesota

Dr. John Ebert is a core professor and director of the M.S. in Cybersecurity program, Cybersecurity Management and Technology Certificate programs, as well as the Data Intelligence and GeoAnalytics program at Saint Mary's University of Minnesota. He has been with Saint Mary's since 2002. In addition to directing multiple programs, Dr. Ebert maintains a full-time teaching load and serves other programs including the marketing undergraduate program and the business intelligence and data analytics graduate program where needed. Dr. Ebert is passionate about the use of technology and the related impacts of cybersecurity in various industries and enjoys working with graduate students on their research projects. He has written grants and partnered with Mayo Clinic on a number of research initiatives and has also presented research at Google headquarters, Minnesota GIS/LIS Consortium, State of Minnesota, Upper Midwest GEOCON, and the Saint Mary's University of Minnesota Business Intelligence Summit.

WOLF LEWIS

Regional Vice President, Comcast Business

Wolf Lewis is the Regional Vice President of Comcast Business in the Midwest Region. He's responsible for the sales, marketing, operations, and strategic direction of the Comcast Business team; providing connectivity, voice, managed services, and secure network solutions to SMB, Mid-Market, and Enterprise customers across seven states in the Midwest. Wolf joined Comcast in 2012 in Colorado and previously was the Senior Director of the Beltway Region, where he was responsible for 13 teams in three states and Washington D.C. Wolf is a seasoned business leader with experience leading Enterprise sales teams in different markets across the country. Prior to joining Comcast, Wolf held leadership positions at Guitar Center and owned a music production company in the Southeast, where he also performed as a touring musician.

ANGIE PROPP

AAP - Vice President, Cash Management Sales Manager, Highland Bank

As Vice President, Cash Management Sales Manager, Angie Propp serves commercial customers at Highland Bank by bringing over 20 years of banking experience in diverse roles, from lending to managing cashflow. Angie is all about people. From the early stages of her career in banking, her eagerness to meet people and surround herself with "thinkers" has built a foundation of experience that translates well to the consultative role of Cash Management. Digital banking continues to transform the industry, making Angie's expertise and tools especially crucial for commercial relationships. Angie holds a BSA in Marketing from the University of North Dakota. She also invests in her own continuing education by maintaining Accredited ACH Professional (AAP) designation, a certification awarded to individuals with a deep knowledge of ACH and payments systems.

EMY JOHNSON

Chief Security Officer, Allina Health

Emy Johnson, BS, MA, is Vice President and Chief Security Officer at Allina Health in Minneapolis, Minnesota. The scope and services of her 300+ team include investigations, threat management, operations, risk mitigation, technological integration, emergency management, crisis management and physical security. Prior to joining Allina Health in 2018, Johnson was Director of Theft & Fraud Operations Assets Protection for Target Corporation. Over the course of her 29-year career with Target, she led teams in a variety of capacities, including corporate responsibility, asset protection, health care theft & fraud, market investigation, communications and community relations. She has received numerous outstanding commendations including the Top 10 Global Women in Leadership Forum Connector Award, the Women in Business Award, the Women's Health Leadership TRUST award, and the SIA Women in Security Forum Power 100.

John Ebert: When we think of cybersecurity, or the landscape of security in general, three things come to my mind: issues, trends, and opportunities. Angie, what are some of the most common forms or types of fraud you see in the banking sector on a day-to-day basis?

Angie Propp: The most common fraud we're seeing right now involves checks being altered, whitewashed, and/or checks being fraudulently issued. Mail fraud is on the rise; entire mailboxes and mail trucks have been stolen. Another type of fraud we're seeing is email fraud. In a common scheme, an incoming email to a business requests that they change payee account numbers and routing numbers, so that clients are tricked into paying these fraudsters instead of their actual vendors. We've also seen cases where a fraudster impersonates the owner or CFO of a company and sends an email to accounts payable with an urgent message: "Hey, I forgot to pay an invoice, and it's past due. Can you get a wire out ASAP?" If your employees are not diligent, they could easily pay a fraudster instead of a legitimate vendor. Each of these tactics are being attempted in check transactions as well as ACH and Wires.

Ebert: You mentioned some of the physical side, but there's also the technical or the network side. Wolf, what steps might organizations think about and/or procure to help protect some other systems?

Wolf Lewis: There are a few elements to it. First and foremost for any organization is education and awareness. You've got to invest in the awareness of your employee population, so that they are apprised of the potential threats that may be coming to them, whether it's an email or a phishing attack, or leaving a physical device unlocked while they walk away to get some water. Ensuring that employees are taking the appropriate protocols to protect passwords, and that you have the right level of sophistication in the passwords It was a lot easier to protect a company's data when everybody was in a brick-and-mortar facility, and you could have that all locked down on a server or in the cloud. It comes back to that education piece and ensuring that when folks are on their home networks, they understand that the data that they're using or engaging with still needs to be protected.

Emy Johnson: The employee population is experiencing an overload of information continuously. One of the things in the security and safety world is a continuous education in every sector. It's not just sending an email and teaching people information; it's testing their ability to retain the information over and over. When you think you've sent too much information about education and training, send more.

Lewis: You'll have your training and say look out for emails that say they're Comcast, but maybe there's a different letter in there. Then [our IT team] will start sending those emails to users to see how they're engaging with it. It's a little bit of a test. You have to have this kind of real-life testing environment on an ongoing basis to make sure you're securing your information.

Propp: One of the tips I recommend to my clients is that employees who handle financial related tasks should use a separate computer when performing other daily responsibilities, especially when visiting any social media sites, since that is where malware can come from. With the shift to a remote work environment, it's not as easy to lock that down, so ongoing training and testing is very important.

Ebert: I couldn't agree more that it's the cycle of education that never will stop. Angie, what are some tips or tools or resources that people can use?

Propp: Companies should definitely have procedures in place for any kind of transaction activity involving money movement. We always recommend dual control. If you're sending checks, have someone issue those checks and have someone else sign them. Have rules in

place when you're updating vendor information for payments. Always have something in writing, a phone number to call and a different email address, to make sure that you're actually talking to the vendor and not some fraudster. If an owner or a director or your boss asks you to pay a bill, have a procedure in place. Make sure you have a double-check system, and make sure employees are following the procedures you have in place.

Lewis: For anybody in an organization, when you have a huge list of different policies and things to follow, that becomes tricky. So it's how do you get to the one rule that helps to solve for a lot of things. An example of this would be: Don't click on links. Go to the source directly. Even if it comes from Apple, build the habit of not clicking on it, and then going straight to your own account where you authenticate it.

Ebert: Emy, how have you seen the intersection of cybersecurity and this world of physical security change over time in your role with Allina?

Johnson: The worlds are colliding more and more within. And the closer they're getting, the safer it actually is, because we take a multifaceted approach. Our teams must work together as we think about the technology. It organically is growing into a larger and stronger partnership, in the physical and the cyber spaces. It used to be that physical teams would focus on their lane and cyber would focus in their lane. But now because of the nature of the threats, we have to work together and mitigate anything that is occurring. Ten or twenty years from now, there won't even be a distinction between the two, it will just be one full security function.

Ebert: Wolf, we're looking at how businesses have adapted to these new hybrid models of working. How have your organization cybersecurity needs evolved? And then the role, at least in your organization, with the service provider? How has that changed as well from that cybersecurity landscape?

Lewis: Historically, it's been about ensuring that our network is as robust as possible so that the businesses that Comcast serves can do the things that they want to do over the network. It gets a little blurry between where does the physical network work end and where does the user experience begin, and where are the handoffs in between and who has responsibility for those? It gets even more complex when you factor in this concept of hybrid work. There are far fewer security measures on home networks, and those users are more susceptible to social engineering tactics and phishing attempts. At the same time, companies' IT staffs are faced with new pressures and challenges to manage all these devices that are connecting to a network and don't sit within a brick-and-mortar facility. If we have a solution to bring to the table, we'll try to interface with what businesses need. It could be DDoS mitigation. It could be managed security; maybe the IT team doesn't have the resources to take care of the network in the way that they need to. Endpoint detection and response is something we've really been leaning into over the last couple of years. Ultimately, I think it's all going to be based off of this concept of zero trust and ensuring that our customers are thinking of it that way, and that we are bringing forth solutions to help them solve those problems.

Ebert: With the cyber products that you're that using with your customers, what are you seeing with that today?

Lewis: Well, there's so many different ways to approach this. Some businesses want to do everything in house so they feel like they have more control, and they have more protection that way. And they want to have their own Layer 7 advanced firewalls; they feel like they have enough of a robust team that they can solve for some of these things. And maybe our job at that point is just to provide the right kind of secure network services. Or conversely, maybe we need to be the one who's bringing those solutions to the table for a business that is under-resourced. This is rudimentary, but it's like a castle and a moat. You have the road going into the castle, the moat around the castle, and then the castle itself and the people inside. As an analogy to a business, the road going in could be the Internet. And this is where a distributed denial of service attack could take out the road. Do they have a way to protect that road? What about the moat? That could be your firewall. That's the last point of resistance before getting into the castle. How are they solving for that? Lastly, what are they doing inside that castle wall, should something get through? That will be your phishing attack or your ransomware attack. You have to think about it in terms of those three things independently, to help them solve for it in the most appropriate manner.

Propp: The other perspective to consider is that many businesses are looking for efficiency and speed. So, your castle may be locked down but it still needs to be able to communicate with the bank, make remote deposits, and send out ACHs. If it's too locked down, you can't do that. If it's not locked down enough, you're opening the door to fraud. You've got to figure out some way to get it to balance.

Ebert: Emy, now that we've seen that greater interaction at the intersection of security and cybersecurity, how can those teams work together?

Johnson: I can't emphasize enough the continuous connection between not just the physical and the cyber but also with colleagues who have a vested interest in risk mitigation. I think about my partners in human resources, supply chain, around the organization that have a vested interest. A big piece of this work is having a strategic roadmap and looking at the broader strategy that we go at together. And we found that to be incredibly helpful, because while we're driving that roadmap, we're bringing those partners along with us and we're educating and teaching. And it's a fluid conversation.

Lewis: I completely agree. It is incredibly important to have an overarching strategy for how you're thinking about managing cybersecurity threats. You need to start thinking about: Who has access to what things, depending on what they need access to? And what risks does that cause for the business?

Johnson: Being nimble and being willing to adjust that plan is also important. You may have to pull out a different tool at a different time for a different reason. I think building those partnerships inside organizations helps. Because when you need to pull out a separate tool to combat something, then it's not, "Wait a minute. That's completely changing the strategy!" No, it's not changing the strategy. It's just using a new tool.

Ebert: Angie, since we're talking about opportunities, what else can the banking sector do to help protect their assets in this opportunistic environment?

Propp: I would suggest they talk to their bank; most banks offer

various products to help their clients monitor accounts for fraud. Banks have products called positive pay - one which helps monitor issued checks, while the other monitors ACH debits. For Check Positive Pay, an employee will upload your check issuance files and as the checks clear, the software matches the payee, the dollar amount, the date, and the check number. If something doesn't match, you have people within your organization that get notified and can return that item before it even hits your account. In the ACH environment, if you're a commercial account, you have 24 hours to return an unauthorized debit. ACH positive pay helps you monitor that activity. You can have people inside your organization get a notification right away, so that action is taken within that 24-hour window.

Ebert: When we look at opportunities and our connections in the security field or in the security industry, how do you form connections and relationships considering the confidential nature of processes within organizations?

Johnson: This is such an important part of being a successful leader or participant in the industry, to have a vast number of connections. Networking and engaging in dialogue were definitely more common pre-pandemic. It kind of got stagnant. We've found it imperative to ignite those relationships, and do them in person, not virtually. I feel strongly that having relationships at the local and the state and the federal level are absolutely critical. So that public-private partnership work never ends. And so, I think at the end of the day, once you get a seat at the table, hold on to the seat; once you meet someone, hang on to that partnership, because you'll use it for many, many reasons. And then, I'm always recruiting for great talent, and having a vast network helps with that as well.

Propp: Going to conferences, networking, and listening to what your peers have to say helps you protect your own company from unknown risks, potential liabilities, and possible weaknesses. You hear what's happened at other companies, and may realize, oh, wait, we might have a vulnerability there too. So, it's always good to network and have connections in your back pocket when needed.

Ebert: What advice would you recommend to someone wishing to get into the industry?

Johnson: It's one word, and that's "yes." In the world of just the word "security," people have their own perceptions of what security may or may not mean. By saying yes, you open your eyes up to opportunities and discussions that you might not normally be a part of. Just say yes.

Propp: Find a mentor or places to have informational interviews, get out there and talk to people. Look for a mentor who shares similar passions, and who always helps you move forward.

Lewis: Unfortunately, it's a growing field. So [there is] a lot of opportunity, There's a number of disciplines inside of that. So get exposure and get education about which part of the discipline you want to become an expert in.

Ebert: If you could recommend one thing to leaders in organizations that they should do to ready their organizations, for either cybersecurity or general security demands, what will that be?

Lewis: Be educated, have a plan. There you go.

Propp: Training, training, and training. Technology continually advances, so do the ways your assets can be comprised. So, continue to encourage training on ways that fraudsters are able to compromise accounts, and what you can do to recognize it and protect your assets.

Johnson: This doesn't have to be perfection. You just have to be doing something. People think of it having it be perfect, [but] there is no such thing as perfection in this work.