BUSINESS AND GOVERNMENT BATTLE CYBERTHREATS

From left: Moderator Brooks Raiford, president and CEO, Raleigh-based NC Tech Association
Angelic Gibson, senior vice president, information technology, Charlotte office of TKXS
Sen. Jeff Tarte, N.C. Senate District 41, Mecklenburg County
Charles Marshall, attorney, Raleigh office of Brooks, Pierce, McLendon, Humphrey & Leonard LLP
Clay Harris, president and chief operating officer, Durham-based WorkSmart

Cybersecurity has emerged as a dominant issue in the business world. In this month's round table, our experts talked about the technology and training necessary to cope with today's threats.

The round table was moderated by Brooks Raiford, president and CEO, NC Tech Association. Support was provided by Brooks, Pierce, McLendon, Humphrey & Leonard LLP, Dixon Hughes Goodman LLP and WorkSmart. Brooks Pierce hosted the event at its Raleigh office. The transcript was edited for brevity and clarity.

PHOTOGRAPHY BY BRYAN REGAN

Jillian Munro, senior vice president, enterprise security, Raleigh-Durham offices of Fidelity Investments Inc.
Emily Larkin, chief information security officer, Raleigh-based Sageworks
Tasha Swann Holsey, cybersecurity and compliance officer, IT department/IT security division, city of Greensboro
Tom Tollerton, senior manager, IT advisory, Charlotte office of Dixon Hughes Goodman LLP

ARE THERE PARTICULAR INDUSTRIES OR SECTORS THAT ARE MORE HIGHLY TARGETED FOR CYBERSECURITY ISSUES?

MARSHALL It's across the board. But I do think it's worth noting that we see a good amount of breaches in the retail space, both malicious and human error. I think when you're looking at industries like health care, you're seeing a good number of breaches. Given the sensitive data and potential for exposure, that's an industry where you're always hearing about a lot about breaches.

MUNRO We're seeing adversaries going after higher value targets as opposed to focusing on a particular industry. They're going after infrastructure targets or high net worth individuals so that their take-down is much larger than it had been in the past.

HARRIS The biggest change over the last two years is the effectiveness of the spearphishing that happens to our clients. Bad actors have gotten much smarter about who to target and how to infiltrate the conversations of those people. It's across all industries.

WHAT ARE THE VULNERABILITIES FOR THE PUBLIC SECTOR?

HOLSEY It's the spearphishing. It's the targeted phishing attacks.

TARTE We see it both at the county and state level. We saw Mecklenburg County deal with ransomware not too long ago. The state is getting hacked multiple times a day across different departments. They're going in through NCDOT and getting that kind of background information. At the Department of Revenue, people are trying to jump in front and determine whether you have a tax refund coming and have it sent to them before it's sent to you. We've got sensitive data in two major data warehouses. We're trying to do population health management and other things. We've got massive responsibility.

> I think when you're looking at industries like health care, you're seeing a good number of breaches. Given the sensitive data and potential for exposure, that's an industry where you're always hearing about a lot about breaches.
>
> **CHARLES MARSHALL**
> Brooks Pierce

HOW CAN ORGANIZATIONS HELP EMPLOYEES COPE WITH CYBERTHREATS?

LARKIN Employees are our weakest link in an organization. We're really big on awareness training. The day the employee comes on board, they spend an hour with my team to go through all of the expectations. Then we stick ourselves out in every staff meeting. You've got 400 people there, and that's a captive audience.

MUNRO Ninety-one percent of cyberattacks start with a phishing email. Having a good blocking attack at the perimeter is extremely important. Couple that with education. We phish every single person in the firm

over and over and over again, all the way up to our president and CEO. It's really important to do that. It's not just one thing. You've got to check the perimeter. You've got to check the interior, and you've got to check the humans.

HARRIS There's good news, at least in the small-business world. Security awareness training has taken off. Nearly a third of our clients now do security awareness training. Our partners have seen 25% to 30% of employees are susceptible to phishing at first. After three months, you can cut that in half. After a year, that goes down to 10%.

HOW DO YOU GO ABOUT TESTING EMPLOYEES? WHEN YOU HAVE IDENTIFIED THAT SMALL SUBSET THAT ARE CONTINUALLY A PROBLEM, WHAT DO YOU DO ABOUT IT?

GIBSON We've had repeat offenders, but we continue to take them through education. We've actually created policy inside of TKXS that when an email's calling you to take action on behalf of the business and it's coming even from the president of the organization, stop, pause, ask. If that person's not available, seek out technical support to confirm. We're very active in communicating and continuing to check up as a part of our onboarding process.

TOLLERTON Security awareness goes beyond just threat awareness. It needs to speak to business process. There needs to be awareness of what the appropriate behavior is.

HOLSEY When employees fail our phishing test, we invite those users to mandatory cybersecurity awareness training. What we do is tailor that session around all the tips that you need to look for when you receive a phishing email. We've taught our employees and customers that they're our first line of defense, and we've made it a team effort. I think that's worked well, because we want to help them help the whole organization. We've made them feel like they're a part of that security team protecting the city of Greensboro.

WHAT ARE SOME TECHNOLOGIES THAT CAN BE USED TO FIGHT CYBERATTACKS?

TARTE We're primarily getting hacked from outside the U.S. every day. One of the ways to potentially control it is to leverage two technologies, identity management and blockchain, that are becoming more mainstream. The idea would be that every North Carolinian, when they hit

16, would be issued a digital certificate. We know every transaction, and it's a secure form of ID.

TOLLERTON We've actually spun up a blockchain working group in our firm, have joined the Accounting Blockchain Coalition and we're looking for use cases. I think the challenge is that the value of blockchain is having multiple parties involved before the transaction peaks. Obviously the use of a blockchain is to record a transaction to a ledger, and I think the challenge is going to be the adoption of those ledgers. I think government is going to have to probably be the leader on that, just because you have so many departments and areas that require transactions, but I think that's a great point for identity management.

IS THERE A RISK OF LACK OF STANDARDIZATION IN APPROACHES TO CYBERSECURITY?

MUNRO Technology diversity in your environment is the enemy, because you may have one small component that's weak. Then you've got a place for adversaries to infiltrate, and you've just got so much more to protect. You've got to do it in different ways. Consistency really helps you know that you've got the right protections in place.

GIBSON Every time you have a new introduction of technology, you're increasing your risk profile. Not only should you do your own internal testing to make sure that you are secure, but have a third party try to break you. We say to all of our clients we want them to do a security test against us as well. You're getting multiple viewpoints. You want a wide lens finding the break points.

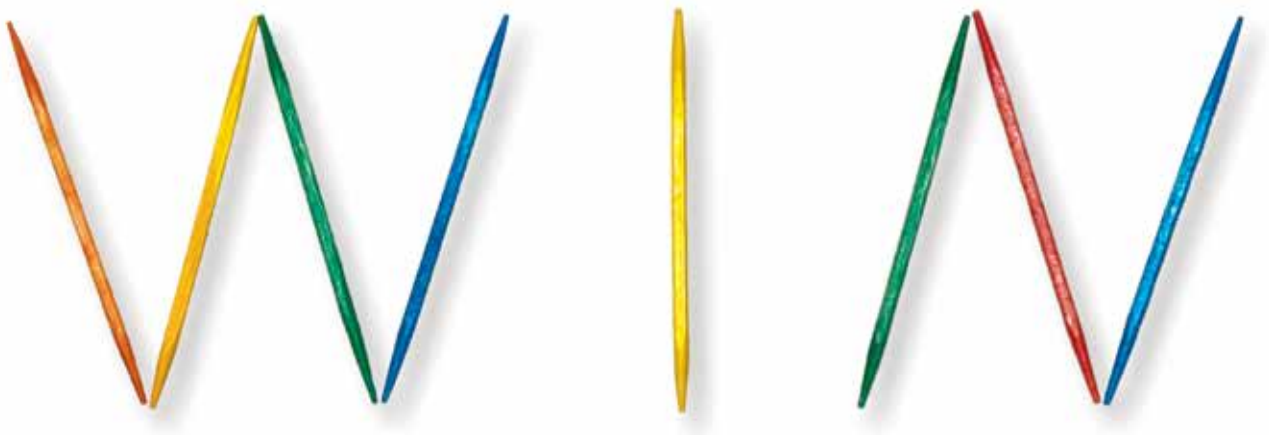
LARKIN You've got to do the foundational pieces and then layer further defenses. But if you're not getting those foundational components done — awareness, patching, things like that — you'll run into trouble.

> Security awareness goes beyond just threat awareness. It needs to speak to business process. There needs to be awareness of what the appropriate behavior is.
>
> **TOM TOLLERTON**
> Dixon Hughes Goodman

HOW INVOLVED SHOULD EXECUTIVES BE IN CYBERSECURITY?

MUNRO You need your board and your senior executives to understand the threat, to be aware of it, to be monitoring it and watching it. It's got to be a board-level topic. In terms of resources, we have a threat intelligence team that works with the organizations that are monitoring the environment so that we can try and get ahead of the bad guys.

The bad guys have a process. Some of them work nine-to-five workdays. They work banker's hours. Some of them treat this as a complete job. If you have a vulnerability out there in the environment, they'll start testing against that. Then you can start to see that activity, and they'll start putting it into production just as a technologist would.



SOLVE:

Move one toothpick
in such a way that all of them
together still spell WIN

If you figured it out, congratulations. Moving the orange toothpick from first to last creates the word WIN again—if you turn the page upside down.

The puzzle demonstrates that finding solutions sometimes requires looking at a problem from an unexpected angle. That's the way Brooks Pierce lawyers approach legal issues—always questioning the conventional answers, and finding uncommon ways to solve problems.

BROOKS PIERCE
FOUNDED 1897

230 N. Elm St., Greensboro | 150 Fayetteville St., Raleigh | 115 N. 3rd St., Wilmington

BROOKSPIERCE.COM

Monitoring the environment and really understanding and appreciating what others are going through and what the government agencies are seeing is extremely important.

MARSHALL It's very easy to convince a company to invest in cyber compliance after they've finished responding to a data breach. What's been more difficult is obviously convincing them to invest on the front end, because it's often an unbudgeted expense and it seems speculative at the time. I also think that it's almost impossible to get that level of investment or buy-in without the board. It usually takes a C-suite executive or board member to raise that flag before any breach occurs and to start asking those questions in order for the company to make the investments that they need.

WHAT'S BEING DONE TO PROTECT CONSUMER DATA AND RESPOND TO PRIVACY CONCERNS?

MARSHALL We're finding that consumers are becoming more educated and better attuned about companies' privacy policies. We encourage them to be truthful, to be transparent and to be accurate when they're communicating with their consumers about their privacy policies. That means thinking about what is reasonable for the consumer to expect in terms of how their data is being handled and shared.

LARKIN With our customers, third parties are a huge piece [of what] I deal with. We try to be very transparent. Users have to sign off on every third party we do business with. Our core application does not require any third party. But if you want to do a credit report, you've got to say, "Yes, I acknowledge."

GIBSON The way people manage passwords is a problem. If somebody gets your username and password at your favorite retail location, they can start to follow you and see where else you're going on the web. Then they can just take over your entire life. At a corporate level, those passwords are coming into an organization, so now the organization's at risk. There are going to be attacks.

So how do you minimize those attacks and how do you prevent them from spreading? For an individual, it begins with password management and protecting your home PCs. It's that basic. People are not informed on protecting themselves, protecting their children. Even a child who is in elementary school is on the internet from your house opening up access. Just think of the different ways that hackers can now come in and invade a family. It's just a different game, because children are certainly not educated on how to protect themselves. We're focused on how do you protect your children from seeing particular content, but how do you actually protect your child from opening doors for identify theft for your family?

TARTE When you sign up for your operating system upgrade, you've

> "Nearly a third of our clients now do security awareness training. Our partners have seen 25 to 30% of employees are susceptible to phishing at first. After three months, you can cut that in half. After a year, that goes down to 10%."
>
> **CLAY HARRIS**
> WorkSmart

waived all your privacy rights. But there are vendors, Apple being one, that are paying real attention to the privacy aspects. But those that have a technical background realize you open up your laptop and with about three commands, you can get to your entire password history on every page that you access. The right technician can get all that. How you protect against that becomes very, very important.

We're working with an organization called TechNet, and we're the sixth state to join. California is one of the members, along with Texas and Massachusetts. We're exchanging information and looking at privacy policy, data breach policy and rules, the whole thing around privacy of information and how we're going to address that. There's probably 70 vendors that participate, from the big boys all the way down to some of the small, innovative, nimble tech companies that are sharing and exchanging ideas. ■

> "You need your board and your senior executives to understand the threat, to be aware of it, to be monitoring it and watching it. It's got to be a board-level topic.
>
> **JILLIAN MUNRO**
> Fidelity Investments