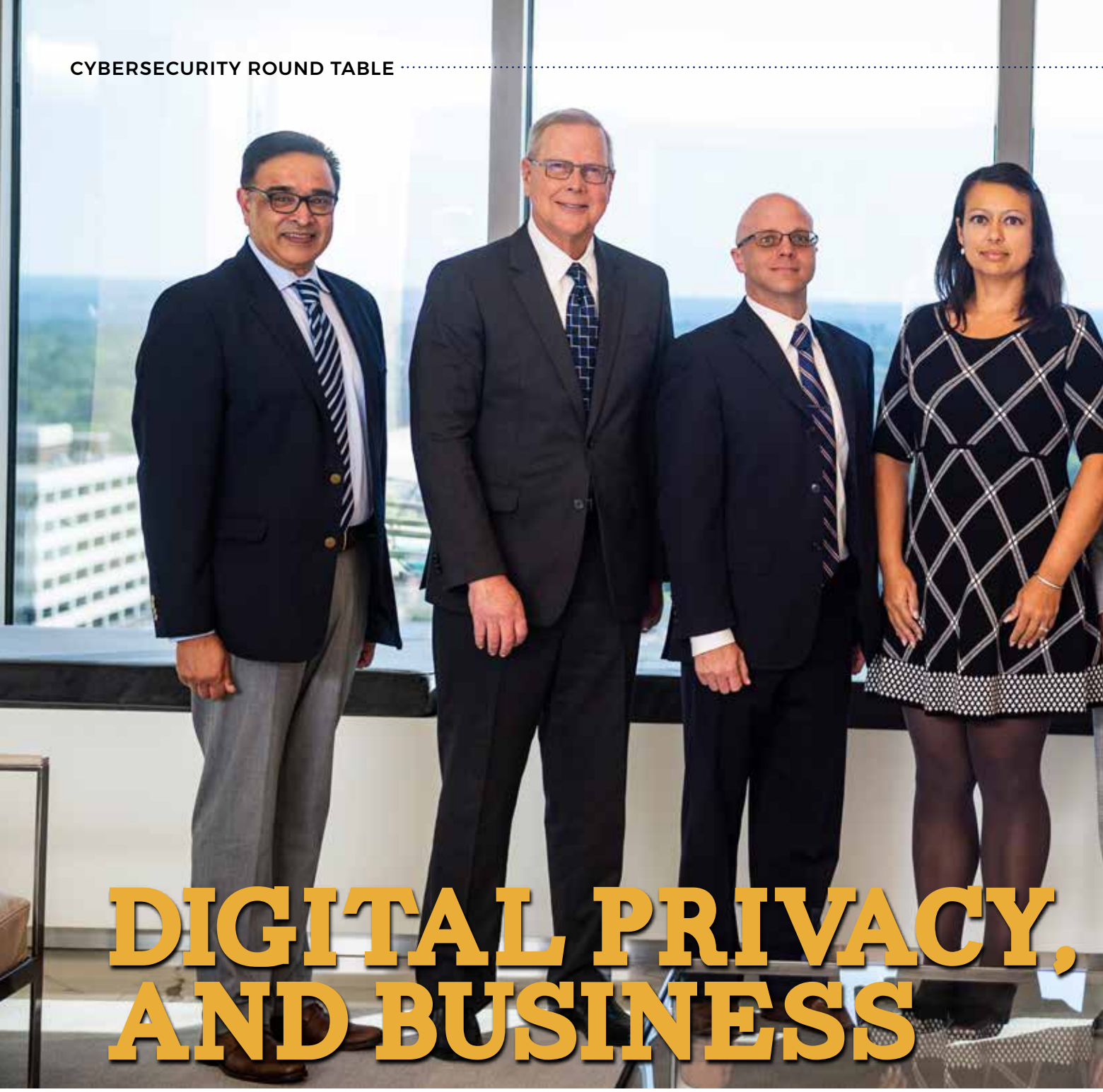


DIGITAL PRIVACY, AND BUSINESS

Standing from left:

Gurpreet Dhillon, department head and professor in the department of information systems and supply chain management, Bryan School of Business and Economics at *UNC Greensboro*

Tom MacKenzie, vice president of privacy and security compliance, *TCDI*

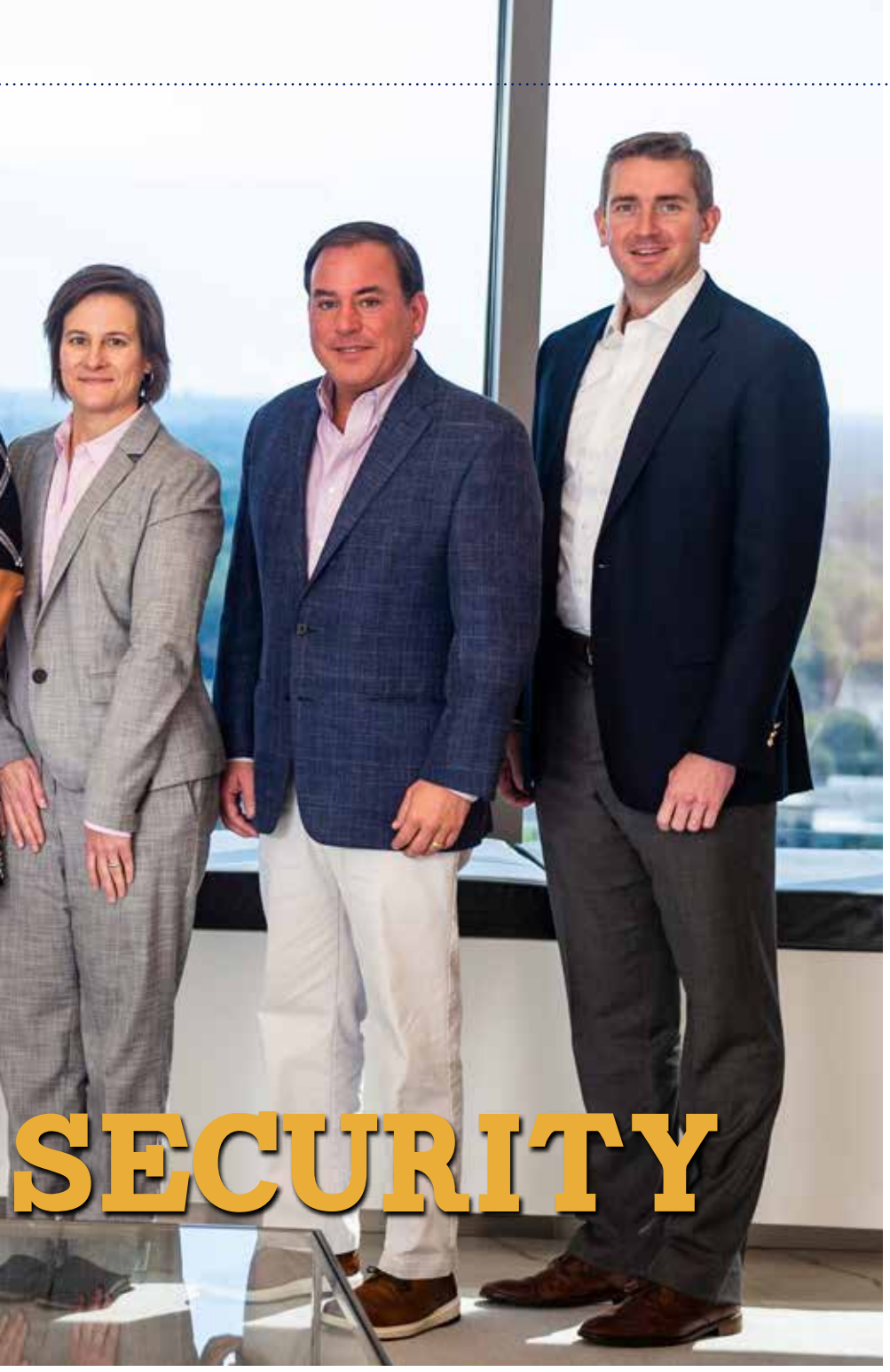
Jonathan Dallaire, senior manager and information security officer, *First Citizens Bank*

Evelyn Re, executive director and board member, *North Carolina Center for Cybersecurity*

Elizabeth Spainhour, attorney, *Brooks Pierce*

Brooks Raiford, CEO, *NC Tech Association* (moderator)

Tom Tollerton, managing director of cybersecurity and data privacy, *Dixon Hughes Goodman LLP*



SECURITY

PHOTOGRAPHY BY BRYAN REGAN

The importance of data privacy for individuals and businesses is becoming an increasingly significant factor in the new era of e-commerce, mobile marketing and the sharing of information. North Carolina experts discuss what state businesses need to have in mind as they secure their data, access personal information and protect key information.

The round table was hosted by Brooks Pierce and sponsored by Brooks Pierce, Dixon Hughes Goodman LLP, First Citizens Bank and UNC Greensboro. The transcript was edited for brevity and clarity.

RAIFORD **WHAT ARE YOUR THOUGHTS ABOUT THE DISTINCTION BETWEEN PRIVACY AND SECURITY? WHAT IS OWED TO CONSUMERS OR OTHER ORGANIZATIONS IF YOU'RE A COMPANY THAT HAS ACCESS TO THAT INFORMATION?**

TOLLERTON I think that's a good place to start, because there is a distinction. Security is how we're protecting data from unauthorized access, whereas privacy includes security, but it's also what we are doing with data that we have authorization to have. Are we transparent about how we're using it? Are we giving consumers rights around what we're doing with it?

I think that, first and foremost, is what we ought to be talking about.

MACKENZIE I often look at privacy as being the overarching umbrella associated with managing information. Security is certainly underneath that umbrella, but privacy is about the management of information through the entire information life cycle, from the point that it is collected to the point that, hopefully, it is securely deleted.

There's a lot of security along the way, but there are just processes in how you handle that data that are really more privacy-related than they may be security-related.

SPAINHOUR From a legal perspective, there's also the concept of privacy as a right. It's not a written constitutional right, but it is one that is a recognized constitutional right in certain contexts.

I certainly think of privacy as both consumer-oriented and, in certain contexts, rights-oriented. Consumers should also expect to have their data be protected.

RAIFORD **SIZE AND SOPHISTICATION OF A COMPANY HAVE A LOT TO DO WITH ITS ABILITY TO DO ALL THE THINGS WE'RE TALKING ABOUT. HOW DOES A SMALL ENTITY OR BUSINESS, WHERE THEY MAY NOT HAVE THE INTERNAL RESOURCES OF A LARGE**

COMPANY, HANDLE SECURITY OR PRIVACY? WHAT RISKS OR PROBLEMS MIGHT THEY FACE?

DALLAIRE While small companies are inherently more challenged — depending on their capacity from a resource and knowledge perspective — larger companies have the same issue, because it's equal to the volume of data and where that data resides. While a small company might outsource or insource certain aspects of core systems, larger companies, like banks and insurance, have hundreds of relationships. They've got to know where the lineage of that data sits. So that, in itself, becomes a very constraining resource requirement even for the largest companies, because it scales.

DHILLON I tend to agree with that, and what I have noticed — at least in the work that we've been doing — is there's a huge challenge with capability and competence of individuals. We're seeing a vacuum of talent. Irrespective of if you're a large company or a small company, there's a constant need for training and education, which we are not able to keep up with, and that ends up being a challenge. Education and awareness are part of it, but I think the technology is changing so quickly that we need to retrain and unlearn and relearn a lot of things, which is resource-intensive if you think about it.

DALLAIRE You could argue that some fintech companies are very good at what they do and can compete very well in the markets they're in. Traditionally they're small, but they are designed with privacy in mind, so it's not an issue for them. Whereas you have legacy companies that have been in business for a long time, and they have to redesign with privacy in mind or security in the same vernacular, which can be very difficult to retool systems and retrain individuals to understand concepts like de-identification and enumeration. It's moving cultures, whereas other cultures are established that way.

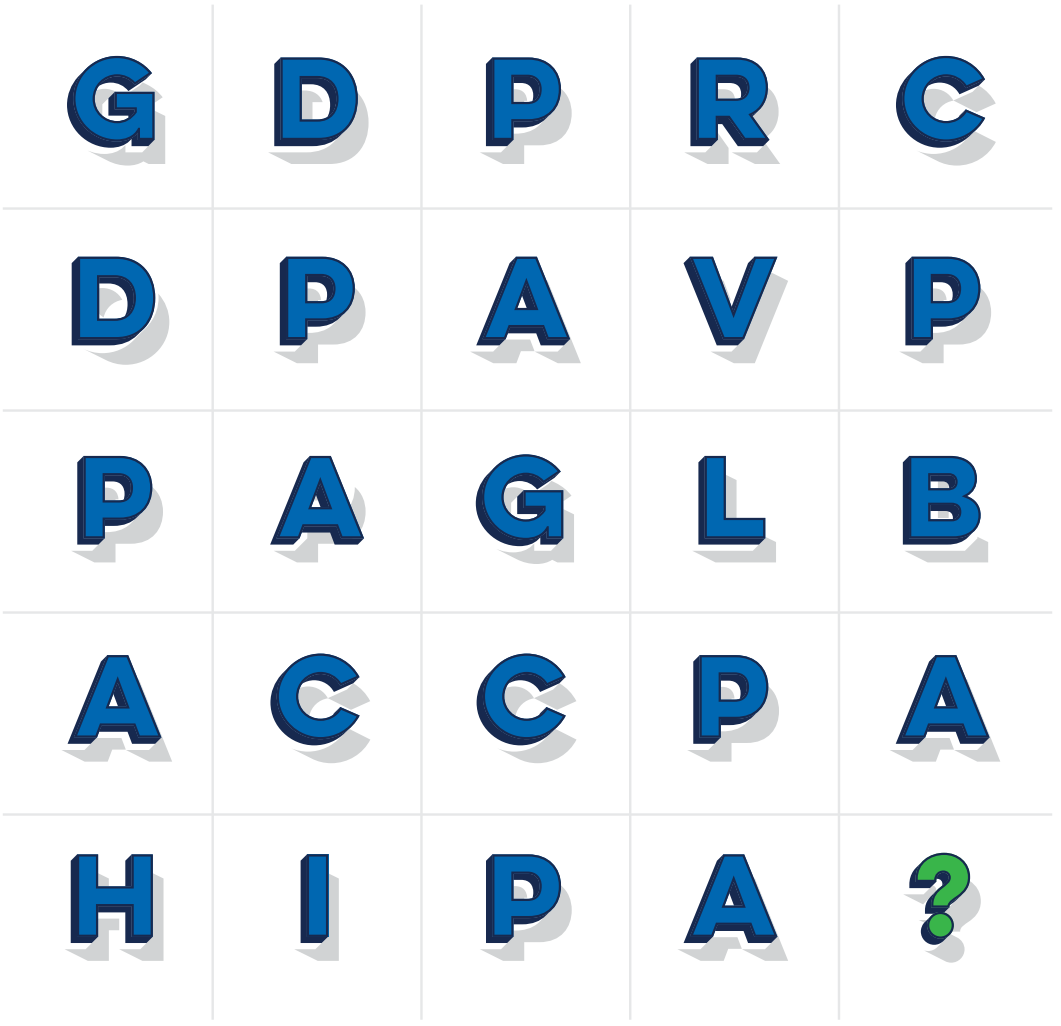
> From a legal perspective, there's also the concept of privacy as a right. It's not a written constitutional right, but it is one that is a recognized constitutional right in certain contexts.
>
> **ELIZABETH SPAINHOUR**
> Brooks Pierce

SPAINHOUR I think you've hit on an interesting thread to travel down, which is the different types of companies.

Financial companies have been in the business of privacy for a long time with regulation, and same with health care companies. For many of the clients that I work with in marketing, communications and media, this is newer to them. They don't typically have the same type of risky data such as Social Security numbers and bank account information.

I also think the risk profile is lower for the smaller folks. They're not in the crosshairs, but there are some companies that are new to this or newer than banks and health care companies. But even though they may not have the same kind of risky data, smaller companies still need to be concerned about privacy and data security.

RAIFORD **A LOT OF THE DISCUSSION OUT THERE IS ABOUT THE THREAT FROM WITHIN. YOU CAN HAVE ALL SORTS OF PROTOCOLS IN PLACE, BUT YOUR OWN EMPLOYEES CAN**



SOLVE:

Which letter replaces the question mark?

If you know the answer, you probably know something about privacy laws. The letters represent just some of the many regulations surrounding data privacy—GDPR, COPPA, and others (including HIPAA). Compliance can be complicated, which makes legal guidance from a Board Certified Specialist in Privacy and Information Security Law* essential.

BROOKS PIERCE

*NC Board of Legal Specialization

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

BROOKSPIERCE.COM

EITHER ACT INNOCENTLY OR CREATE PROBLEMS AS BAD ACTORS.

TALK A LITTLE BIT ABOUT THE IMPORTANCE OF EMPLOYEE TRAINING. EVEN THE MOST NONTECHNICAL EMPLOYEES ARE STILL INTERACTING WITH YOUR TECHNOLOGY FROM THEIR DESKTOP, LAPTOP AND PHONE.

MACKENZIE I've read [stories] where as much as 99% of the data breaches that occur have a human component associated with it, and much of that is from a social-engineering standpoint. You used to hear all about these great technical advances that the bad guys were deploying to hack into your systems. They don't have to work that hard anymore, because they just go to the employees, and the employees give them the information that they need to do the things that they want to do.

Training is absolutely crucial, and phishing training is a great example. I heard several people say they do that within the organization, but helping employees understand the threat that really exists from a social-engineering standpoint and how to protect themselves and the company from that threat is really important.

RAIFORD LET'S LEAP TO THE GENERAL DATA PROTECTION REGULATION IN EUROPE AND THE CALIFORNIA CONSUMER PRIVACY ACT. WHAT ARE YOUR THOUGHTS ON THAT MOVING ACROSS THE COUNTRY OR BECOME STANDARDIZED?

MACKENZIE It's kind of interesting you're bringing that topic up because this last Friday was the last day that amendments were allowed to be put forward for [the California act]. It's pretty much baked at this point. The governor will very likely sign that bill, so it will go into effect at the beginning of next year. It's absolutely started things. There are, I believe, 12 other states that are in the process of similar types of laws, and you can bet they will use California as the model, as California used the GDPR as the model.

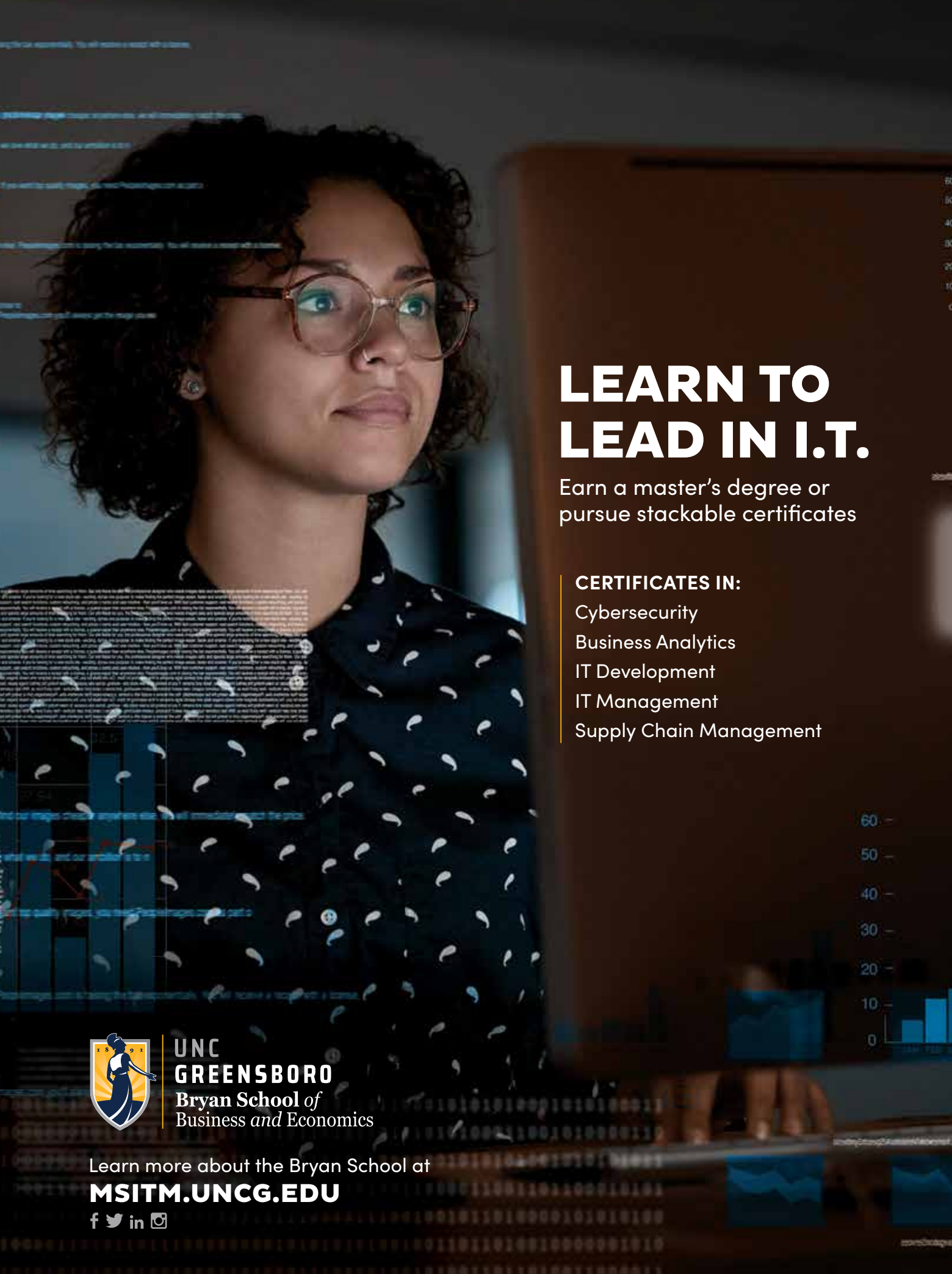
> ...Fraud risk with death is very real. It happens every day where there are actors that simply look for who is deceased and then figure out where they bank and they try to engineer their way in. And that can include family members.
>
> **JONATHAN DALLAIRE**
> First Citizens Bank

It's going to sweep across the country. I think our only hope is that there will be federal legislation that will override these things, so that we'll have one consistent regulation that we can all live with and work with instead of all of these different things, because I guarantee you, they will all be slightly different, and that will be a nightmare for business.

I think companies can get out ahead of this. The privacy regulations, including GDPR, CCPA [and] HIPAA, have built on some fairly standard principles in privacy.

The one that I look to most is the Organization of Economic Cooperation and Development principles. Throughout the world, if you look at privacy regulations that have been put in place, they hit on most of those principles. If companies look at that and realize that whatever is coming is going to look an awful like those principles, they can prepare themselves a whole lot better.

DHILLON One of the things that the California legislation and other OECD



LEARN TO LEAD IN I.T.

Earn a master's degree or pursue stackable certificates

CERTIFICATES IN:

Cybersecurity
Business Analytics
IT Development
IT Management
Supply Chain Management

UNC GREENSBORO
Bryan School *of* Business *and* Economics

Learn more about the Bryan School at
MSITM.UNCG.EDU

directives really do is reassert the role of ownership and who owns that data, because once this data is out there in the open, that's a problem we have. You put something on Facebook, and it's out there. Who controls it? Who has access to it? Who can change it? We suddenly lose control.

These legislations harp back to that very fundamental notion of ownership, and this is a good thing. It forces companies and businesses to begin thinking about these issues.

RAIFORD **WITH MORE REGULATION AND MORE OBLIGATION COMES MORE NEED FOR COMPLIANCE, AND WITH THAT COMES THE NEED FOR MORE TECHNICAL SKILLS AS WELL AS OTHERS. WHAT DOES THIS MEAN IN TERMS OF THE SKILLS THAT ARE NEEDED WITHIN ORGANIZATIONS?**

RE The North Carolina Center for Cybersecurity has been birthed out of this need. We're taking business leaders across the state, pulling them together and asking them, "What are you missing?" We're looking to academia and asking them, "Where can you begin to fill in your research in order to answer these problems?" much like we do with medical researchers.

We're turning that over to the scholars to help figure out how we can bring up leadership that's missing a great deal — leadership that can focus on managing risk rather than the security controls, specifically.

DHILLON Security, over the decades, has been an afterthought. When something goes wrong, let's come back and plug the holes; let's do something. We have a whole generation of technologists out there who still think of it as an afterthought, and they don't put in the resources and the time necessary to build the appropriate controls.

MACKENZIE If you look a little deeper into the organization, I know what we try to develop are not just thought processes associated with privacy and security, but we're trying to develop a culture where people don't really have to think about it. It's just built into their corporate DNA.

I love it when I go into a meeting, and HR is developing a new process, and you hear privacy types of considerations being built into that process. I love it when I sit in on a meeting with our software developers, and you hear them talk about building in privacy and security components into the code that they're developing. That's a culture that is going to help keep you safe and is just as valuable as all the other safeguards you put in place.

> We're seeing a vacuum of talent. Irrespective of if you're a large company or a small company, there's a constant need for training and education, which we are not able to keep up with, and that ends up being a challenge.
>
> **GURPREET DHILLON**
> UNC Greensboro

SPAINHOUR I'm encouraged to hear all of that. I work with some smaller and medium-sized companies, and I think for a long time, privacy was how they respond to a security breach. It was very incident-based. I think it's evolving now to focus more on compliance.

I know it's hard to spend your dollars, but spending the resources on doing compliance-oriented front-end work —

Over 100 years. Forever First.®

After enough time, your name becomes more than the thing people call you. It becomes your reputation. And your promise. For more than 100 years, First Citizens Bank has helped customers make the most of the money they earn, save and invest. Learn how we can help you at firstcitizens.com. Or stop by one of our branches. Because money isn't everything. But so much depends on what you do with your money. **First Citizens Bank. Forever First.**

First Citizens Bank

Member FDIC

baking privacy and data security into your culture to prevent the need for incident response and reaching out to professionals when you need them to help you with those policies and those mechanisms and assessments — is incredibly important.

RAIFORD **WHAT SORT OF DATA SHOULD COMPANIES AVOID COLLECTING?**

TOLLERTON Many businesses don't think about that. You talk about designing privacy upfront. Part of that is saying, "What do we need to do, or what data do we need to collect in order to operate the business?"

They think about that upfront, but so many businesses don't do that privacy by design.

MACKENZIE The [Fair Information Practice Principles] of collection limitation and purpose are really important here. You can't tell a company not to collect a specific type of data because they may very well need that, and they may have a legitimate purpose for having that data. One of the areas that I have issues with internally is our marketing people and the type of information they want to collect on people. I'll often ask them, "What are you going to use that information for?"

Oftentimes, the response I get is, "Well, we don't know yet, but we think that would be good to have down the road." That's a dangerous way to proceed. If you don't need that information, don't collect it today, especially personal information.

DHILLON The problem is, many times consumers don't know the data is being collected. I mean, we all have smartphones and your locational information. I used Waze to come here all the way from Greensboro, and it's popping up all these ads. They've collected the data that I have been driving at such-and-such speed from Greensboro to reach here on time, and they know everything about me.

> "I think that's a good place to start, because there is a distinction. Security is how we're protecting data from unauthorized access, whereas privacy includes security, but it's also what we are doing with data that we have authorization to have.
>
> **TOM TOLLERTON**
> Dixon Hughes Goodman LLP

Thinking back to the original question that was asked about security privacy versus usability and convenience: Yes, it's convenient to do that, but I think therein lies this very interesting situation where you have to balance it out.

Now, even today, if I go into my iPhone, I go through four or five steps to figure out which app I'm going to allow and which I'm not going to allow to use my location. It's a challenge, and they're all free, of course.

TOLLERTON Brooks made a comment at the start that we're willing to give up our privacy. Gurpreet, I think your comment was great — that we don't realize what's being collected.

You can make an argument one way or the other as to how well [the California act] was implemented, but I think the intention is to bring transparency and to give consumers those rights.

SPAINHOUR This is not a unique or original thought. Europeans have a particular view about their privacy — they view it as a fundamental right — and that has not necessarily been the case here.

We have viewed our privacy as something that will get us $5 off on a pizza or whatever. What we learned from the Cambridge Analytica experience is that actually made people really mad. That's what led to the CCPA, and I think there's maybe a shift in our American attitudes about our privacy.

DHILLON I grew up in India. In Europe, there's a difference between opt-in and opt-out. In North America, by default, you are in. Over there, by default, you are out, and then you opt to be in. That will require a huge cultural shift. That kind of filters your distinction.

RAIFORD **LET'S TALK ABOUT WHO OWNS DATA AFTER AN INDIVIDUAL DIES. WHAT CAN CONSUMERS DO ABOUT THIS?**

SPAINHOUR I would expect that each platform has a procedure for that. I have a small client, and that is what his company tries to do: Have a plan in place for everybody around this table. This person has access. This person knows my logins. I think people should also consider including this in your estate or end-of-life planning.

DHILLON I think Facebook allows you to nominate an individual who can take over. I put in my son's name. The question is, do we know about it? Are we aware about these mechanisms? That's number one.

Number two is the question that you addressed: How do we think digitally about our identity protection? Where are you going to leave your physical keys? It's a very important question to be addressed.

DALLAIRE From a business point of view, I can't answer the privacy question on who owns the data. But entities have to have verified challenge, because the fraud risk with death is very real. It happens every day where there are actors that simply look for who is deceased, then figure out where they bank and they try to engineer their way in. And that can include family members.

As a consumer, my LastPass [password manager] key is going to my wife. But as a practitioner in digital fraud, it is very difficult to weed out who's a verified relative versus who's not in order to do that from a data perspective, because we have to protect our assets as well.

RAIFORD **ARE THERE SOME NORTH CAROLINA ANGLES ON ANYTHING WE'VE TALKED ABOUT? ARE WE LEADING THE WAY IN CERTAIN AREAS? ARE WE BEHIND IN OTHERS? ARE THERE CERTAIN INDUSTRIES THAT ARE PARTICULARLY STRONG IN NORTH CAROLINA THAT HAVE TAKEN A LEAD IN ADDRESSING SOME OF THE ISSUES WE TALKED ABOUT TODAY?**

SPAINHOUR There's a lot of talent here. California is a leader on certain types of law — North Carolina gets there, and we're not last. We get there. There's certainly been activity at the North Carolina legislature this year — they were looking at amendments to the security breach and security freeze components of our statutes. It didn't go anywhere, and I don't think it will this year. But, it's certainly something that our elected officials are focused on, so I expect there will be activity in the future.

MACKENZIE I agree with you that the legislature is not behind, by any means. I believe you're talking about the amendments to the identity theft protection law. HB 904 is the bill. It's putting a little more teeth into the protections. It is now starting to mandate that companies must have reasonable security controls in place. So, North Carolina, by no means, is behind in all of those things. We're not ready to adopt a [California] type of regulation, but it's well above the midpoint in keeping pace. ■