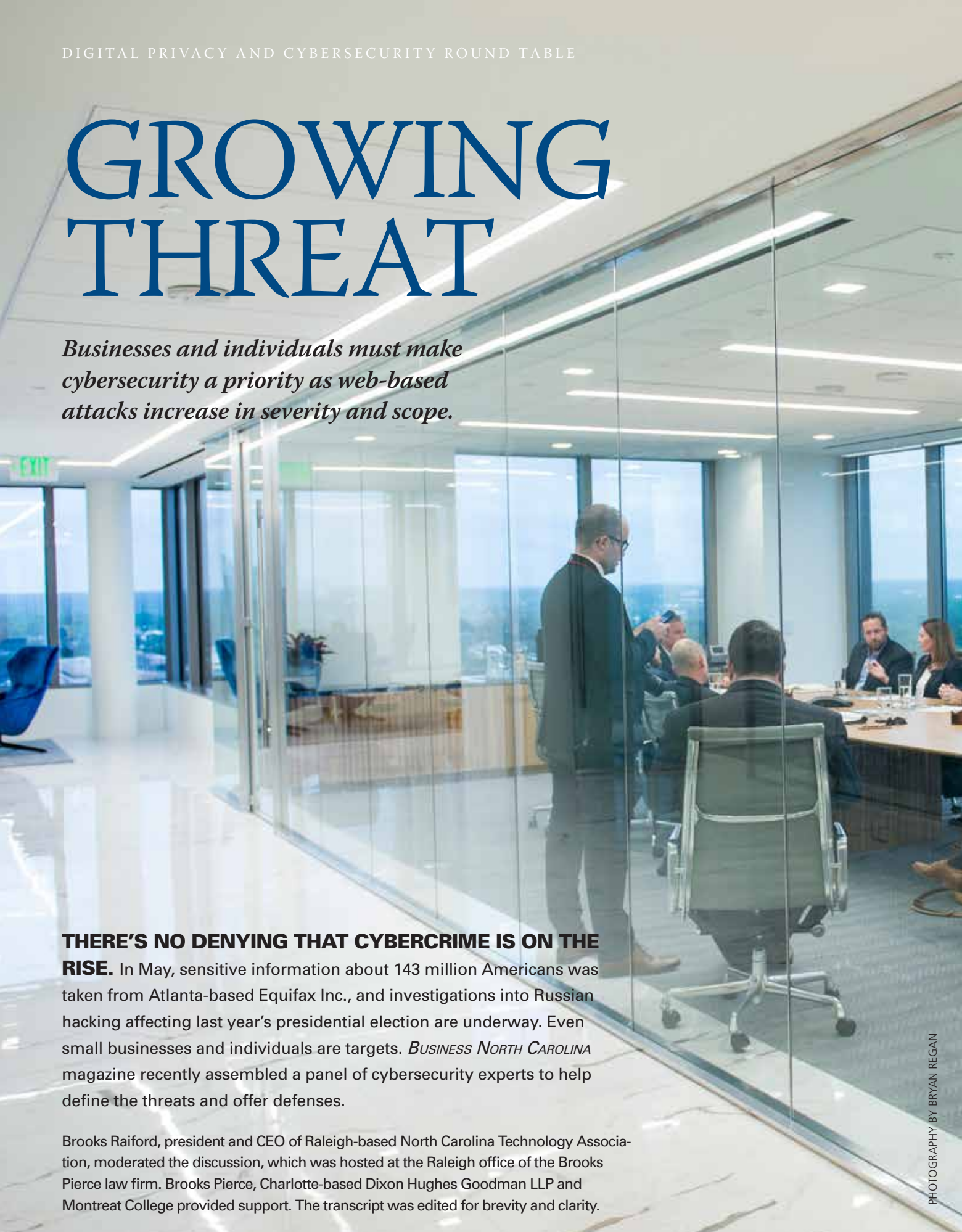
GROWING THREAT

Businesses and individuals must make cybersecurity a priority as web-based attacks increase in severity and scope.



PHOTOGRAPHY BY BRYAN REGAN

THERE'S NO DENYING THAT CYBERCRIME IS ON THE RISE. In May, sensitive information about 143 million Americans was taken from Atlanta-based Equifax Inc., and investigations into Russian hacking affecting last year's presidential election are underway. Even small businesses and individuals are targets. *Business North Carolina* magazine recently assembled a panel of cybersecurity experts to help define the threats and offer defenses.

Brooks Raiford, president and CEO of Raleigh-based North Carolina Technology Association, moderated the discussion, which was hosted at the Raleigh office of the Brooks Pierce law firm. Brooks Pierce, Charlotte-based Dixon Hughes Goodman LLP and Montreat College provided support. The transcript was edited for brevity and clarity.

HOW DO BUSINESSES AND INDIVIDUALS VIEW CYBERSECURITY? HOW ARE THEY BEING ATTACKED?

QUICK I represent small to midsized businesses. Many wonder what they can do when large companies with seemingly endless resources, such as [Minneapolis-based] Target Corp. or Equifax, are breached. They wonder if they should do anything, which is even scarier. We suggest solutions to those who ask, but there are probably just as many not asking.

NYE The businesses targeted continue to evolve in which virtually all sectors are a target. Now, new and emerging techniques are being used on the back end. Many attacks originate from phishing campaigns, which use an email to target an individual. The subject hopes the recipient of the email will trust the validity of the email and click on a link or an attachment that contains malware. The FBI investigates insider threats, business email compromises and email account takeovers. We're seeing a rise in real-estate fraud, where cybercriminals manipulate homeowners during closing, providing the buyer with new wiring instructions that reroute money.

KOTYNSKI Criminals are learning company processes such as vendor payment. They inject themselves in the middle, where they have access to financial information or money. We're a public entity, so many of our processes are accessible to the public. That makes us a bigger target.

DILLARD Many small to midsized companies are leaving themselves wide open for an attack by having nonexistent or minimal cybersecurity infrastructure. That also leaves little usable forensic data after a breach. The coverage gap is mostly due to a lack of awareness of the risks. Some don't believe they are a target. That changes after a breach, especially when they face a huge bill to clean up the mess.

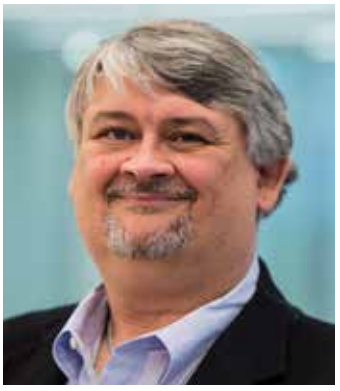
THOMPSON Many top executives believe the answer is simply hiring a corporate information officer. But there needs to be more behind the scenes than up-to-date technology. They need tools to communicate with their technology team and whoever comes to help after a breach.

SAINE State government is the largest repository of residents' data in North Carolina. It's our job to protect residents. Our challenge is improving interaction between residents and their government. We must remain transparent through both, which can be difficult. We don't want to telegraph our weaknesses, particularly to segments that want to harm us.

HOW DOES CYBERSECURITY AFFECT BUSINESSES?

SAINE It's a cost factor, especially for small businesses. They are handling more digital interactions, such as point of sale, which create more exposure. A data leak could close their business. I'm

CLAYTON DILLARD
president, Holly Springs-based Legion CyberWorks LLC



ANDREW KOTYNSKI
director of information security services, Raleigh-based N.C. State University

JESSICA NYE
special agent and cyber squad supervisor, Raleigh office of Washington, D.C.-based FBI

S. WILSON QUICK
lawyer, Raleigh office of Greensboro-based Brooks, Pierce, McLendon, Humphrey & Leonard LLP

BROOKS RAIFORD
president and CEO, Raleigh-based North Carolina Technology Association

REP. JASON SAINE
N.C. House of Representatives, District 97 — Lincoln County

DAVID THOMPSON
Montreat College adviser and CEO, Matthews-based EdgePoint Ltd.

chairman of the [N.C.] House's Information Technology Appropriations Committee. We brought together appropriations chairpersons to better warn of risks and share solutions. We consolidated the IT department for similar reasons. Last session we worked on limiting liability for IT vendors.

QUICK Many small businesses can't afford a cybersecurity expert. Many are running 10-year-old systems that haven't been updated or had software patches installed. That makes it near impossible to assess their risks or identify when a breach has happened. Know your customer notification requirements before a breach, because they are different in every state that you do business. Every company should have a data privacy task force that includes top executives, IT folks, human resources and representation from every facet of the business.

DILLARD Notification law is where businesses, especially those with a limited budget, can quickly fall into serious trouble by, for example, notifying the wrong people at the wrong time. You need to know your first step after an intrusion. Who do you call? How were your business and customers exposed? Don't make IT solely responsible. It can't see every risk. Businesses need to identify and prioritize their risks and then mitigate them.

THOMPSON N.C. State and Montreat are members of National Center for Academic Excellence Program in Cyber Defense, which is jointly operated by National Security Agency and Department of Homeland Security. Montreat is looking at ways to help the community by leveraging its resources. As students learn skills, they can work with businesses in the community. Not only does that give students great work experience, but it also could provide a less expensive cybersecurity option to businesses that can't afford a consultant.

KOTYNSKI We use many interns from the Poole College of Management. They eventually will be business owners. We try

to give them a taste of what we see day to day. When we talk to businesses, it's less about who they need to notify after a breach and more about opening their eyes to the fact that someone does want their information.

NYE It goes back to awareness. Look at the most valuable assets manufactured and owned by your company. What would someone want to steal? Once you have that defined, you can educate your employees, especially those outside your IT staff, about protecting it. Companies regularly hold fire drills, so why don't we rehearse for a cyber incident? In the event of a cyber incident with your company, you'll be better off if you create and practice your response.

WHAT TYPES OF CYBERCRIMES HAPPEN IN NORTH CAROLINA?

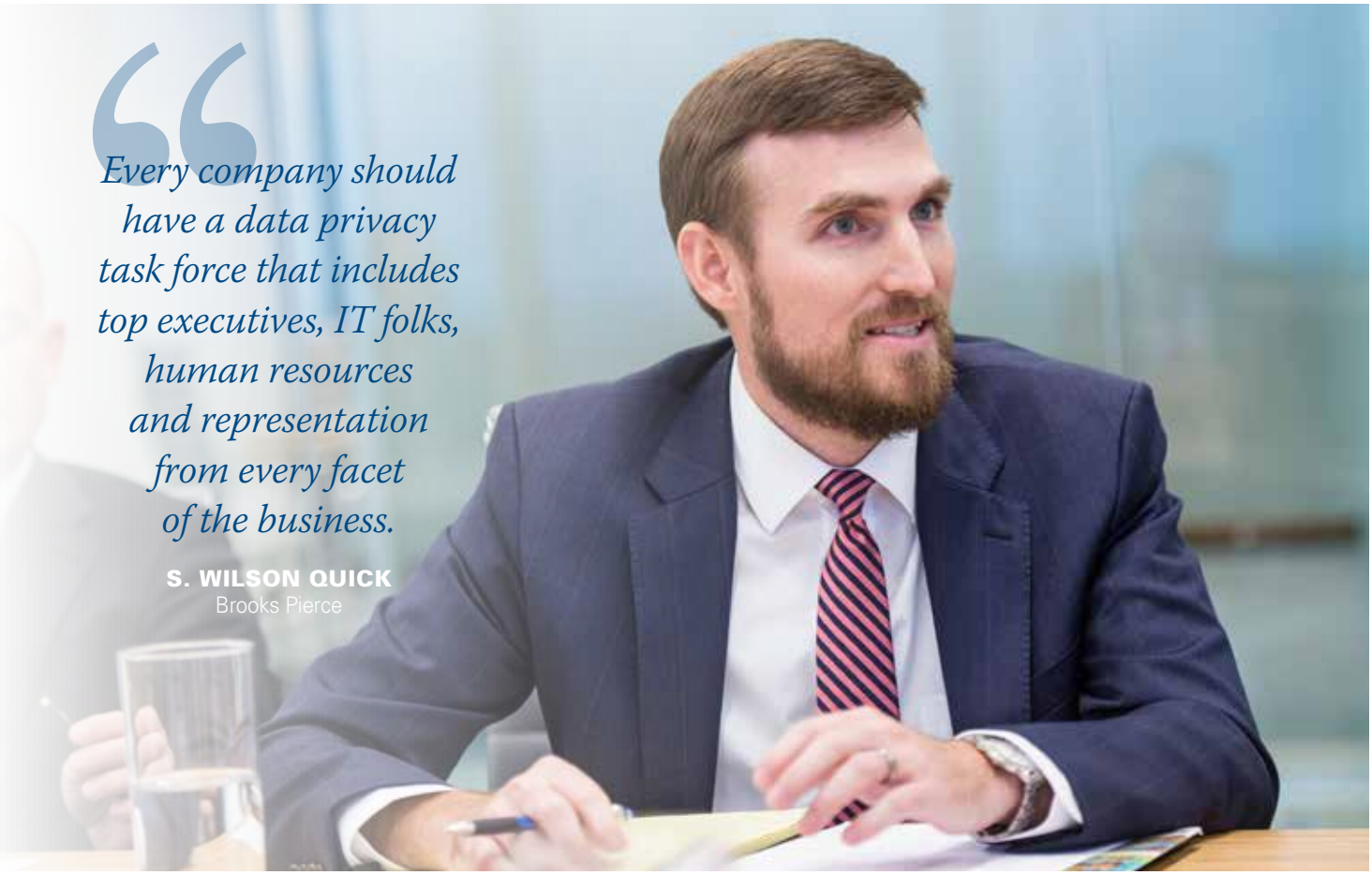
NYE We see everything, because North Carolina is a leader in many industries — financially motivated hackers to hacktivists hacking for socioeconomic or political causes to insider threats to state-sponsored intrusions to cyberterrorism. Cyberterrorists have disseminated lists of personal identifying information that include North Carolina residents and ask for lone wolves in the U.S. to attack them. North Carolina has world-famous educational institutions. Research Triangle Park is a global center for technology and business. Charlotte is a leader in the finance industry. We're assisting with awareness and discussing the threats, but more needs to be done. Cyber intrusions and cybercrime affect everyone. The target could be monetary funds or intellectual property or personal identifying information, which could be sold on the dark web for a profit. Most people don't recognize the demand for their information. Cybercriminals are after everything right now.

WHAT IS RANSOMWARE AND HOW IS IT BEING USED?

NYE Ransomware encrypts a user's important files, documents or even their entire computer, making all of that information unreadable until a ransom is paid. In theory, the data is returned or computer unlocked once a ransom is paid. However, that is not always the case. These attacks have increased and become more and more sophisticated, to include attacks on Internet of Things devices, because criminals have created a very profitable marketplace. The cybercriminals behind this generally are asking for ransom amounts that are in line with a business' or individual's ability to pay. The FBI's policy is not to pay the ransom because payment only encourages the criminals to continue this activity. If an individual does decide to pay, the cybercriminals may ask for more and more money ultimately never decrypting the data. And there's no guarantee that your data will

If I'm a small or mid-sized business deciding between storing data in-house or with a large company, I would lean toward the latter. They have teams dedicated to making sure protection is up to specifications.

DAVID THOMPSON
EdgePoint Ltd.



Every company should have a data privacy task force that includes top executives, IT folks, human resources and representation from every facet of the business.

S. WILSON QUICK
Brooks Pierce

be returned or usable after payment. In an attempt to circumvent the problem, we encourage regularly backing up your data. Then in the event of a ransomware attack, a user can restore their infected machine with a backup instead of paying the ransom. But what if the ransomware attack also includes the release of the encrypted data to the public? In talking about creating a response plan in the event of a cyber incident, companies should include ransomware attacks and extortion in that plan. That response plan also should include contacting law enforcement to assist if you are the victim of a cyber intrusion.

HOW DO YOU CONVINCE A TECHNOLOGY CHALLENGED EXECUTIVE THAT CYBERSECURITY IS NEEDED?

DILLARD We focus on brand, reputation and ability to deliver — things that resonate with most executives. If we can show how an intrusion or breach puts those at risk, then it makes sense to them. The adoption rate is still low, but that's where we see the best results. It's sad. We talk to health care practice owners, and they are hesitant to do all of the things needed to prevent a breach and protect patient privacy. We can warn them, and we can be there for them when the worst happens.

WHAT ROLE DOES PRIVACY PROTECTION PLAY IN CYBERSECURITY?

SAINE Residents have to decide how much information they want to share. Smartphones, for example, provide navigation by locating their users with GPS. But that data also shows where they've been. That's OK if I allowed my data to be used like that, but what if I didn't or there is a breach? There are many policy questions that are evolving around privacy. Things are moving quickly on a bipartisan online privacy and data release bill that I co-sponsored. Many House members didn't have a good understanding of those terms when we first brought it to the floor because they never considered them. One member said, "I'd like to know if my employee goes to church or not on Sunday." That's not our business or the business of an employer. People need to understand the implications of opting in on data use. Sometimes they don't realize they are allowing it. Who reads the agreement when you can't wait to use your new app?

HOW IS EDUCATION RESPONDING?

THOMPSON Montreat is one of a few faith-based liberal arts colleges that offer a cybersecurity major. While most approach it through technology, Montreat focuses on the human component. We need to underscore character and ethics education

Benchmark Litigation named us "NC Law Firm of the Year."

But that's only half the story.

That's because it happened twice—in 2016 and 2017. We gratefully acknowledge this honor from the highly-regarded independent research organization. And we thank our talented lawyers who take on complex, often precedent-setting, litigation for our clients.

For more information about Benchmark Litigation's methodology, visit https://www.benchmarklitigation.com/general/research.

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

BROOKSPIERCE.COM

BROOKS PIERCE
FOUNDED 1897

People need to understand the implications of opting in on data use. Sometimes they don't realize they are allowing it. Who reads the agreement when you can't wait to use your new app?

REP. JASON SAINE
N.C. House of Representatives,
District 97 — Lincoln County

in this space from the earliest grades. We need to explain the ramifications of what's done in the digital space. No one will care if there's a scandalous online picture of you in 20 years, because I believe everyone will have one by then. But one could cost you a job right now. Faith-based institutions and service academies are the only two groups of colleges that are overtly teaching character in this space. Many people aren't discussing it. It's a losing proposition until you focus on the person at the keyboard. University of Tulsa makes its cyber program students complete a federal security clearance form. That may be extreme, but it's a way to ensure honest students are educated and bad ones aren't weaponized.

KOTYNSKI Today's students have spent most of their lives on smartphones. Everything is 6 inches from their face. Then there are faculty members, who may have retired from their industry 10 years ago, who don't want to get involved in that technology. You have to find common ground, where everyone is safe and sane. It's impossible to get some kind of adoption across the board because you'll never hit all of the right marks.

WHAT PARAMETERS SHOULD YOU PUT ON YOUR DATA COLLECTION AND STORAGE?

QUICK Every business needs to examine the information it has stored. If you're collecting scanned driver's licenses to ensure your sweepstakes entrants are 18 years or older, for example, you only need them for a short time. If you keep them and there's a breach, you'll have to notify each person. Even an old computer in the back room is a risk if it's accessible. Find out where information is stored and if old source methods have been eliminated before something happens.

DILLARD You have to know your system and the data that's on it. Only then can you install proper protective measures. If you're following your policy of encrypting data on your computers, for example, then it won't be accessible to whoever recycles them. There's no magic in it. The same fundamentals apply, no matter your data or who is managing it.

THOMPSON If I'm a small or midsized business deciding between storing data in-house or with a large company, I would lean toward the latter. They have teams dedicated to making sure protection is up to specifications. I know that I don't know very much about an attacker's likely approaches. So I want help. But even that isn't a sure thing. I lose several credit cards to suspicious activity each year. There's no pain to me. I get a new card, and my bank pays the bill. The recent Equifax breach affects millions, but I won't lose sleep over it. I'm curious to see what will make people say it's a threat to businesses and society. ■