Table of Experts:
Insights into Cyber Security

A SPECIAL PROMOTIONAL SECTION IN THE NASHVILLE BUSINESS JOURNAL

AUGUST 26, 2016

SPONSORED BY

Bradley

Bradley Arant Boult Cummings LLP

Cybera

TEKLINKS®

We Make IT Work for Business.

Meet the Experts

Paige Boshell

Partner, Bradley
pboshell@bradley.com
205.521.3639

For more than twenty years, Paige Boshell has advised and counseled clients on a variety of privacy and information security risk assessment and mitigation processes, including the identification of, protection from, detection of, response to, and recovery from data security risks. She drafts and negotiates SaaS, cloud, software licensing, and other information technology and service provider contracts. Paige frequently advises clients on privacy and security issues related to the FTC Act, the FCRA and FACTA, the GLBA, the COPPA, and the TCPA. She advises clients that have suffered a data breach in connection with the resulting investigation, including coordination with fraud investigators, technology service providers and law enforcement and the ensuing mitigation effects, including preparation of customer notices, negotiation of vendor contracts, and coordination with consumer reporting agencies.

Cliff Duffey

President and Founder, Cybera
1.866.429.2372
cybera.net/company/contact.html

Cliff Duffey has served as Cybera's President since founding the company in February, 2001. As President, he has been the architect of Cybera's growth and emergence as a leading security technology company. Prior to Cybera, Duffey served as Senior Vice President of Corporate Development at Covad, managing the acquisition and integration of BlueStar Communications. Duffey was Senior Vice President and Chief Technology Officer at BlueStar Communications, where he managed technology strategy, business development, product marketing, and the rollout of BlueStar's network of 450 U.S. data centers. He also held management positions with Ascend Communications up until its acquisition by Lucent, and Intermedia Communications. Duffey holds a B.S. in Computer Engineering from Clemson University.

Aaron Lancaster CISSP, CCSK

Operational Team Leader, Teklinks
alancaster@teklinks.com
865.545.5086

Aaron Lancaster is a trusted results-oriented Certified Information Systems Security Professional (CISSP) and operational team leader. He has over 15 years of cyber security experience gained from diverse organizations in healthcare, federal government, software, energy and defense industries. Aaron specializes in vulnerability management and systems security architecture, and uses leadership and influence to shape organizational security culture. Aaron is co-founder of the East Tennessee Chapter of the Information Systems Security Association (ISSA E-TENN) and has presented at several security conferences. In addition to CISSP, Aaron has attained Cloud Security Alliance's Certificate of Cloud Security Knowledge (CCSK).

Connect with Aaron at www.linkedin.com/in/aarondlancaster or on Twitter @aarondlancaster

Bradley
Bradley Arant Boult Cummings LLP

Cybera

TEKLINKS®
We Make IT Work for Business.

Cyber security advice from the experts

Transcribed and edited by Andrea Williams

In today's complex threat landscape, what should a business's biggest security concern be?

Paige: I think what we would counsel now is what we've been counseling for the past five years, which is that a plan and continuous planning is critical. What we've really seen more recently is a shift from a specific incident response plan, that's much like a business continuity plan in this context, to more overall, overarching data security planning. So your response and your resiliency to an incident remains key, but even more important is the up-front planning. The culture is very important—to have your culture top-to-bottom, and across horizontal departments, be in tune with these critical concepts of privacy and security, so that any time the business wants to offer a new product, or a new service or a new method of delivery, or any time the business wants to sign up with a new vendor or a new business partner—you understand how it will affect your so-called 'crown jewels,' or your most important proprietary and consumer information.

Aaron: I think one of the biggest threats is the employees within the workplace. So, how are we educating our employees? How are we training our employees to use technology in a way that's smart and doesn't create additional vulnerability for those crown jewels that we're trying to protect? Is that happening on a yearly basis? Is it happening on a bi-annual basis, or a quarterly basis, and what topics are being covered along the way? Is it just phishing? Is it a spear phishing or wire fraud attempt being highlighted? Related to phishing, it's become such a problem, specifically in the area of wire fraud attempts, that the FBI put out an advisory this year saying everybody needs to be cognizant of this because organizations are taking the bait left and right and losing, on average, $150,000 per incident to these wire fraud phishing attempts.

I know we're going to get back to phishing a little bit later on, but this is a huge problem. And it starts with the user.

Cliff: I think what we see happening on a general basis is very consistent with what Paige and Aaron said. I think the three trends that we notice more than we may have seen a couple years ago is that, first and foremost, we see security being weaved into the fabric of the business. It's no longer a separate department, or a bolt-on. Security now depends on creating awareness with every single employee, every process. Every step of the business has to have security as a portion of the decision-making tree. The second thing we see is data and systems for analytics, and in reaction to the Target [company] breach, we see the world shifting a lot, so that identifying and knowing that there's a breach is not good enough. We see companies taking a much more proactive set of initiatives to prevent or isolate the data that may be exposed. Finally, I think a few years ago, most businesses were looking at security as something they had to do, and there were compliance factors in a lot of businesses that were the driver. But the third thing that we see happening is, in today's world, compliance is not enough. Most major corporations have woken up and realized that they need to truly take actions. It has to be strategic to protect their proprietary data and information, and compliance is too low of a bar.

> "It's no longer a separate department, or a bolt-on. Security now depends on creating awareness with every single employee, every process."
>
> **Cliff Duffey**
> **President and Founder, Cybera**

So as you're talking about that, and you're talking about being more proactive rather than reactive, what's the best way to educate employees?

Cliff: We may have a little bit of a different view because our business is in security software and technology. We definitely see the education policy and employee awareness. But a technology trend that we see much more often now is that corporations are putting in much tighter access controls, and they're doing that with new software systems and technology. And essentially, they're making it harder for there to be multiple employees or resources that can access data that they shouldn't have access to. So employees or users, all systems and their roles are being more tightly defined, so that if there is a breach or a weak point with any system or user, the damage can be isolated to a limited set of data or systems that that user or system had access to.

continued on page 26

"We're seeing a lot more traditional phishing emails but also those that include a Doc or a PDF attachment, rather than a link to a site."

Paige Boshell
Partner, Bradley

Aaron: Like Paige was saying, a lot of this comes back to your planning, and I think training's got to be an integral part of your plan. And, secondly, prevention is important—and that's an ongoing process of managing and maintaining the technology and continuing to build on that foundation of training that you have set with your employees. Then there's remediation, as well, on the back-end of that. So if you run a phishing campaign on yourself—and I would recommend every business run a phishing campaign on themselves, to take a temperature of what their company looks like—ask yourself if you have high-risk employees. I have very close friends and colleagues who are professional penetration testers and run phishing campaigns on companies for-hire on a regular basis, and they are just amazed by some of the bait that some employees will take. They will send an email out to a list of publicly-available email addresses for a particular organization, and the email will say, "Do not click this link," and there will be a link right next to that, and they'll still get a 20% click rate.

So, if you've identified a risk, then there's due diligence, due care that needs to be exercised in that area. And, certainly, we've seen a precedent with cyber insurance policies that state that if you know of a risk, and you're not doing anything about it, they won't cover that. They basically can come back and say, "We don't insure stupid." And for the small and medium businesses out there, if you don't have the bandwidth or resources to identify those risks, then maybe you need outside help. That's where using an outside service provider or a consultant can be a very big value-add for a business.

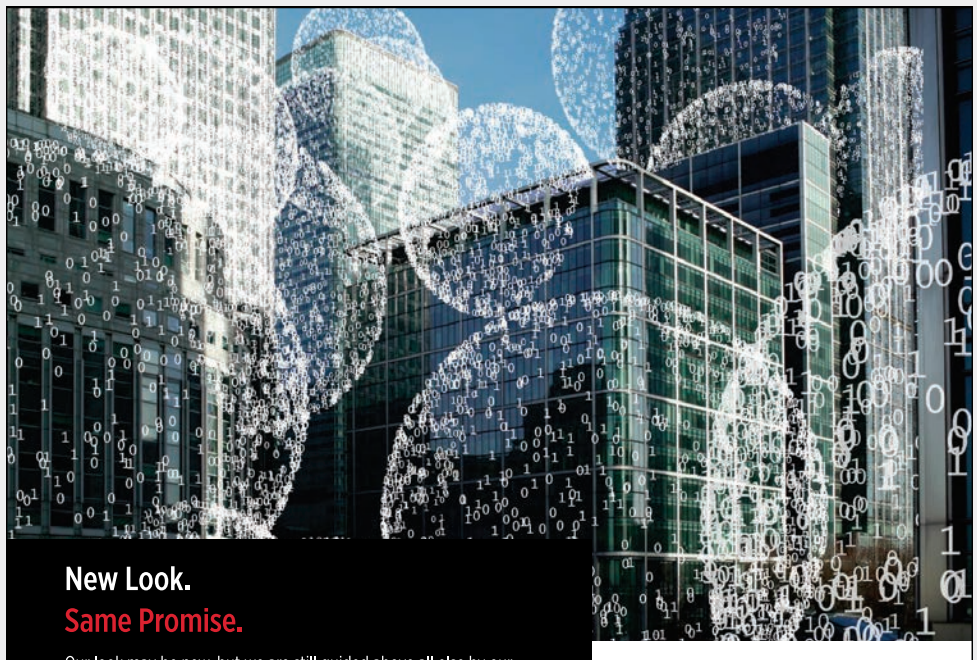
Paige: I agree with the concept of training and campaigns. Coming from the law firm side, we are often asked to engage in client-specific training. For example, for a bank or for a hospital, they'll send us a set of supplies or a set of requirements, and everyone who works with or touches that particular client will engage in the training. I have found, as a trainee, that what is really effective is ongoing and continuous training for a variety of perspectives and new employees—for example, maybe a phishing module, or maybe a network security or physical security module. But just weave that training into the employees' everyday employment life, if you will. We have found campaigns—particularly pop quizzes with phishing—to be very successful, because you don't want to get caught having opened a phishing link, but if you've done that in a training exercise, it is a really great learning opportunity for the employee. It keeps us from becoming complacent.

And to wrap up, I'll mention a company, Phish Me, which is a leading phishing intelligence security tester and provider. They offer free webinars, free employee training modules that include these pop quizzes. So a smaller company that might not have the capacity to put a security vendor on retainer has options like Phish Me, where they can engage in some level of free training for their employees.

You all have mentioned phishing quite a bit, so, clearly, this is a topic that's top-of-mind right now. What else do people need to know about that in order to protect themselves?

Paige: I think that Aaron raised a really significant recent trend, which is the wire transfer fraud emails. And those are referred to generally as "business email compromise" or BEC attacks. And that's not your traditional phishing, because there's no link or attached document. Those are emails that purport to be from someone within a company who has the authority to order wire transfers from someone else within the company who has the authority to actually initiate a wire transfer. And we've seen this at very large companies like Mattel, as well as very, very small clients, and from large dollar amounts to small.

The FBI and InfraGard have been releasing a lot of reports and updates and alerts on BEC. As of early summer, federal law enforcement has estimated over $2 billion in lawsuits.



They're warning, in particular, of account activity in Beijing, as accounts residing in Beijing have been a hub of this activity. So you're seeing it more on the international landscape, but they're also seeing this as a more sophisticated level of phishing attack, where the attacker has gotten to know the company. They know who the people are. They know who the players are, and they know to whom to send the email and from whom.

Additionally, we're seeing a lot more traditional phishing emails but that include a Doc or a PDF attachment, rather than a link to a site. Folks have become much more educated about clicking on unknown sites, but we click on PDFs and Docs every day. And we're seeing that through those sorts of attachments, once they're downloaded onto a system's network, they can infect the entire network.

Aaron: I'll add to what Paige was saying about these targeted wire fraud attacks, where someone has spoofed the CEO's email address to make it look like it comes from the CEO, going to the CFO and saying something like, "Hey, I need this wire done today to pay this bill. It's $75,000, and I need it right now." There are a few things there to consider. First, the phisher is going to masquerade as somebody who has the power or influence to put pressure on somebody that can actually carry out this process, and then also, the request will typically be a rush and outside the normal process of how things are done.

So I think one of the great ways that businesses can protect themselves against this is to put manual verification processes into place. Think about your retirement or investment accounts. Will your investment manager or financial advisor do a transaction by email? No. They're going to pick up the phone; they're going to want you to sign something and fax it, or email a scanned copy, or come to their office and sign it right there. Or it might even have to be notarized. So two-step verification processes can be really helpful. We see that starting to come into play in technology, as well, like with logging into critical accounts like email or iCloud or other services that are considered now to be core to people's workflow and to their lives and their identities. Facebook and other social media accounts are starting to have these two-step verifications. Do that in your business. A simple phone call can save your company tens or hundreds of thousands of dollars in a matter of hours. And advise your comptrollers and other people that have access to those systems to not be pressured by something outside of normal process.

Ok, great. Let's talk about networks and the cloud a little bit.

Cliff: I think cloud is one of the biggest fundamental shifts in IT infrastructure that we've seen since the late '90s when the internet came forward. Another trend we see is the Internet of Things, and almost every electronic device imaginable is now being made network-capable. And the third, which is where we've really focused our technology and business, is the trend of network and security evolving from closed appliances and closed systems made by big companies, into software-based systems—a lot of which are open-sourced. Companies are now being much more active in setting up and managing, and even using, open-source components throughout their business.

In particular, we're seeing that, where businesses used to just build a big network, now, they build that big network; they connect it to the cloud; and then they connect their users into that network. So this is where all three of these major trends cross, and that's actually a recipe for disaster. If anyone ever gained access into that, then they could have far-reaching access to a great deal of proprietary data.

So what we see happening is businesses are building networks within networks within networks, and they're adding encryption

continued on page 28

"...one of the great ways that businesses can protect themselves against [wire fraud attacks] is to put manual verification processes in place."

Aaron Lancaster
Operational Team Leader, Teklinks

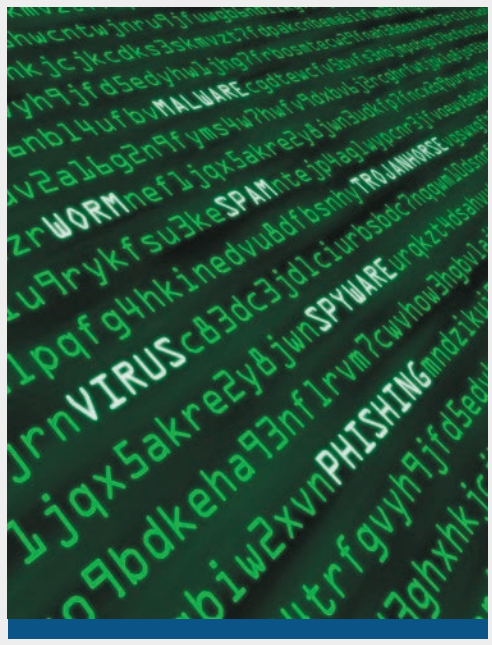
Cybera's award-winning technology is currently installed in over 60,000 business locations in 23 countries. And although we are a leading provider of secure, software-defined WANs to major enterprises around the world, we proudly call Nashville our home. Our locally-designed technology eliminates the complexity that global enterprises face when deploying secure payment networks and enterprise applications to remote locations that have no on-site IT staff.

Focus on your core business and leave the security to us!
Securing your remote locations does not have to be time consuming, complex and costly. Cybera's cloud-managed, defense-in-depth approach makes it easy to deploy highly secure networks to all of your remote sites at the lowest possible cost. So you can now focus on growing your business rather than worrying if your remote locations are secure.

We are the proud recipient of the NBJ Best in Business Awards and proud members of the Nashville Technology Council and the ISSA Middle Tennessee Chapter. To learn more, contact us at www.cybera.com or 1-866-429-2372.

Cybera®

9009 Carothers Parkway Suite C-5
Franklin, TN 37067



"It's really important to have contractual provisions in place with your cloud provider, ensuring that they meet certain levels of security..."

Paige Boshell
Partner, Bradley

inside their corporate networks. They're doing multi-factor authentication on every user, on every application, on every system, to validate any device that's allowed to connect to any other system within their network. And so, with the flexibility of network and security functions becoming a software function, it's giving a lot more creative architectures for businesses to layer in security throughout their businesses. And it's really driving a need for more in-house security expertise, a lot more up-front design, and a lot more proactive interest in how they can build out their infrastructure to validate the identity of every user, and put in the access controls, so that if any individual user has a breach, that breach is very limited in its scope.

Paige: Just to the point of focusing solely on the cloud, from a lawyer's perspective, your cloud is only as secure as your cloud vendor is. So questions like, does the cloud play a role in keeping networks more secure? I have to say it depends. If you have an off-site physical storage facility, you would want to go visit that off-site storage facility. You would want to look at the physical controls, the physical environment, the temperature. And you want to do the same type of thing with your cloud service provider—which is, you need to vet the provider, both as a vendor and also as an information security provider.

It's really important to have contractual provisions in place with your cloud provider, ensuring that they meet certain levels of security and that they have certain audits to maintain that level of security, so that your company has a way to actively and continuously monitor that security protocols are being met. And, then, you have to actually monitor that security so you can catch a defect or weakness before it directly impacts your information.

Aaron: To add on to that, I would advise that, if you're going to leverage the cloud to bring more security to your network, you pay careful attention to your agreements with those service providers. Where does their responsibility leave off, and where does your responsibility begin? And what are they bringing to the table? Cliff mentioned in-house talent that can perform certain roles, and you're going to want to make sure that you have the people to perform those roles that your cloud service provider is not bringing to the table. But they should absolutely be bringing security to the table, to a degree—or at least offer that, even if that's something that you choose not to leverage.

But we're seeing some amazing capabilities come from the cloud. For example, in a cloud environment, some things are possible that are just not possible in a traditional, on premise architecture, like multi-tenant instrumentation and monitoring. So across an entire environment of services, rendered to a number of clients, in the cloud, we're now able to monitor those different environments and look at trends that are affecting individual customers—and then mitigate that threat for all of them. So, from a threat intelligence or a business intelligence perspective, that's something that cloud service providers are able to do for customers that you may not be able to do for yourself. You may not even be able to get access to that kind of intelligence-sharing information if you're in an on premise deployment model. So not only are business agreements really important, but what the technology itself is capable of delivering is important as well.

The cloud also offers a lot of flexibility in how you can adapt to changing conditions, but it can also be a threat to your security. There's a term out there called "departmentalization," and what this refers to is this: We traditionally think about our business from an on-premise perspective, in which the business's IT infrastructure didn't extend beyond the office building. The firewall was where the environment ended. Then we start adding things on, like VPNs for remote access; we start adding on other things like Outlook Web Access and SharePoint Web Access, so that we could get to business applications from off-site. Now, so many applications have moved to software as a service, which are rendered in the cloud, that a lot of that information is leaving the network on a minute-by-minute, hour-by-hour, day-by-day basis. And based on data that I've seen, most businesses don't have a very good handle on how much of that business is leaving the network. And that's a huge threat to business security.

So I would also recommend highly that business owners engage someone to help them get a handle on where their critical business information is living and where it's going, because you may or may not be aware that, for example, one of your employees is storing healthcare information on a non-HIPAA-compliant system like Google Drive, or Gmail, or Yahoo Mail. That carries direct civil penalties and is something that could have direct financial impact on your business.

Paige: If I might add and agree with that last point, it really is the foundation of any plan, that the first step you take is to get an inventory of your information, where it's housed, and who can access it—whether via internal access or external access. Because

whether you're using a cloud provider or another vendor, you are only as strong—and your plan is only as strong—as your weakest link.

Last summer, the Department of Justice released a list of about 10 or 15 best practices for cyber security, and I would recommend that to any business (it's accessible online at the DOJ site). It's just a list of basic principles, and their number one principle is: Identify your crown jewels, or your key information. It's the information from which your business derives its value, whether it's your customers' information, protected consumer information, or internal proprietary information. Identify where that information is located and who has access. And an important corollary to that inventory is, what information do you have that you don't need?

A lot of older companies still have information in physical files. And a lot of other companies that were new or young when the internet and computing was new and young took advantage of the endless data source supply, and have just kept everything. The important corollary to identifying and protecting the crown jewels is getting rid of outdated, old information that you do not absolutely need, or that you are not otherwise required by law to keep, because we do see a lot of breaches involving outdated passwords or outdated information of former customers or former employees that still pose a risk—and yet there was no business need to have that information.

Cliff: In reaction to what Paige and Aaron said, we're a technology company, so we're in the business of protecting the crown jewels. And we do see more and more companies adopting the zero-trust approach on all of their data, which essentially means that they're assuming that everyone's a threat, and every system and every device is a threat. So how can they validate the security and integrity of those users and systems?

One thing that we haven't talked a bit about is, what is the internet of things— with all of these network-based devises—doing to the threat landscape? And what we see happening is the threats are becoming more than just access to proprietary information. And certainly the mobile devices, guest users—all of these pose new threats and challenges to the business. But most businesses have overlooked the real risks and threats of the business decisions that they're making for new business applications.

I'll just give you a great example that I think kind of connects all these dots and highlights it: We do a lot of work in the energy sector, particularly with petroleum companies. And a few years back, there was a great idea: Wouldn't it be nice to have a cloud-based application that can monitor the fuel levels on the ground, and tell you how many gallons are sold, how many have been pumped? And it turns out that 70% of the fuel dispensers in the world have the capability to be connected to the network and connected to these cloud applications.

So, the business concept of having cloud-based applications monitoring fuel levels is great. We had a customer a few years back, though, that had a very unsophisticated young hacker gain access to 20 of their dispensers and re-program them to tell them that there was no fuel left in the ground. And then they changed the access credentials so no one else could get in. Essentially, they had fuel in the ground at the stores, but the dispenser thought it was empty, so it shut down and stopped dispensing fuel.

So you think about that—here's a business use case or threat that nobody would have thought about. Fortunately, it was a very unsophisticated attack, but this vulnerability exists, or did exist, with 70% of the world's fuel dispensing systems. A sophisticated attack could have shut down fuel dispensing in a major region, even on a national basis. And we actually presented this use case to Tom Ridge, shortly after he left as the head

continued on page 30

"...pay careful attention to your agreements with [cloud] service providers. Where does their responsibility leave off, ...and yours begin?"

Aaron Lancaster
Operational Team Leader, Teklinks

DATA LEAKAGE IS ONE OF THE MOST WIDESPREAD RISKS TO BUSINESSES WORLDWIDE, and the problem only gets worse as people share sensitive information with customers, partners, vendors, and others outside of their organizations. Citrix ShareFile makes it possible for IT to provide the anywhere, any-device data access and collaboration people need, while meeting the organization's requirements for ***security, manageability, and compliance***.

Your business could be at risk.
Contact us for more details on controlling and securing your data with TekLinks and Citrix.

TEKLINKS®
We Make IT Work for Business.

Alabama • Florida • Mississippi • Tennessee

205.314.6600 | teklinks.com

According to Osterman Research, *Dropbox has found its way into 70% of organizations*, leaving them **vulnerable to a number of data security risks** and compliance regulations.

CITRIX® ShareFile

"...making security easier to deploy means that it's much easier to weave into the fabric of business..."

Cliff Duffey
President and Founder, Cybera

of the Department of Homeland Security, and he built a practice just in consulting on energy risks. But prior to that, all the thoughts on risk had gone into utility companies. What would happen to our country if 70% of our gas stations were shut down and couldn't dispense fuel, for a day? A week? That's a real threat, and we see challenges like that all the time. Every new device that gets connected to the internet is a new risk that most companies haven't thought through.

One last question: Your customers and your employees expect to have a frictionless experience with your applications and devices —how do you do that, while still being secure?

Cliff: We're in this business of providing software security and technology solutions. So this is actually one of our biggest selling points. Fortunately, as we're shifting to software-based network and security, it's giving a much, much greater capability for automation of configuration and set-up, and ultimately, that leads to making it much, much easier to deploy and manage security policies.

Today, since we can automate this functionality through software, we've gone through deployments—like we did 15,000 petroleum stations for Shell, and all but five of those were plugged in by the clerk behind the counter, and it took less than 20 minutes, and he just followed a four-step pictogram on a page-and-a-half document. So if we can make security that easy to deploy and use the software intelligence that we have, we can make a near frictionless experience. And making security easy to deploy means that it's much easier to weave into the fabric of the business, and adopt common architectures and policies across the business.

Paige: Coming from a legal perspective, the frictionless experience on legal devices is really the current holy grail. I think that consumers have gotten used to scrolling through endless disclosures online, on their computers. I think they're used to legal disclosure pop-up screens. For example, when you want to sign a document online, electronically, you have to go through several screens of disclosures and consent, and agree to sign the document electronically before the document is even presented. It sounds cumbersome, but people are used to it. They're not used to that on their phone. So what we're seeing is a tension between required legal disclosures that are intended to protect the consumers' security and privacy and the ability to have a frictionless experience on your mobile device. You don't want to sit on your phone and scroll through an endless series of screens.

There is also a tension between trying to give those full disclosures and making them simplified—not just in a way that ensures a frictionless experience for the consumer, but also in a way that satisfies regulation requirements. So I think we're going to see more from the federal regulators—particularly the banking regulators and the state regulators—about how the legal disclosure experience looks on the phone. And we mentioned earlier in this discussion that simply being compliant is not sufficient.

So, I read this question about a frictionless experience as more phone-oriented than computer-oriented. And the question is more about the best practices to achieve a device experience that is both secure and frictionless. And there's sort of that tension, on the security side—which it sounds like the security developers are really on top of and working fast—and on the legal side, which includes the information you have to give the consumer before you can transact on a mobile device. And that's something that we're having difficulty with on the legal side.

Aaron: From a security practitioner's perspective, I would love nothing more than to say that security will enable or enhance the user's experience from end to end. I think there are laws—much like laws of physics, there are laws of security, in general—that can't be broken. And I think one of those unfortunate laws is that security means greater complexity for each of us. So I think it's a balance. We have to balance and look for opportunities to enable a more secure user interface—a more secure user experience—without putting undue burden on that process of using the technology and leveraging the technology to do things like deposit checks using our phones.

I think it's being recognized in the industry today that the traditional workstation, or even laptops, are going to fall by the wayside in the next five to ten years. We're going to see a much heavier lean towards mobile tablets or multi-functional devices like the Surface or something similar to that, because we want our tech to be with us wherever we go. And there's some security and privacy ramifications to that, too. Paige talked about scrolling through these disclosures, and we accept a lot of privacy invasions or give up a lot of privacy for functionality. So there's a balance there, too.

But as far as best practices go, I think we're going to encounter some friction. We have to be mentally prepared for that. Last fall, I went to a fraud summit where the FBI presented a great deal of information around fraud, and where I think this comes back to our frictionless experience is this: If it's frictionless for us to use it, it's also frictionless for somebody who wants to use it in the wrong way. So we have to understand that we have to accept a little poking and prodding, in order to make it harder for people to misuse that technology.

I think a perfect example is airport security—and I know there's a whole millennial generation of people who don't remember this time that are coming into the workplace today. But think back to before we had TSA in the airport, and what that process of going to your gate looked like, and how that looked different from what it looks like today. We have had to accept—in a post-9/11 era—a little bit more poking and prodding, for the sake of a more difficult misuse of that venue. And I think the same applies to our technology. Frictionless is the Holy Grail of user experience. Will we get there? Maybe someday. But in the course of getting there, we're going to have to realize that security brings some complexity, and that that's necessary in order to prevent people from misusing it in a way that's not desirable. So there's a balance. ■

Tables of Experts
in the Nashville Business Journal

Want to share your expertise on an important business topic?

Contact Amy Harris
at aharris@bizjournals.com