TABLE OF EXPERTS

SAN ANTONIO BUSINESS JOURNAL

cybersecurity

Considering the current world events, companies need to be diligent to protect their data. We all have increased cybersecurity risks and malicious actors will take advantage of these events for social engineering attempts. They will commonly instill a sense of urgency and/or play on our emotions to get you to divulge personal or company information.

Jimmy Holmes, Market President, and Publisher of the San Antonio Business Journal, met with executives to discuss this on March 11th to get their counsel on what businesses should do.

SPONSORED BY

DEF-LOGIX inc.

UTSA ALVAREZ College of Business
The University of Texas at San Antonio

GETTY IMAGES

Jimmy Holmes: With recent breaches all over the news, what are some of the top risks that companies face right now?

Nicole Beebe: The two top risks are still the same as they've been for several years now, unfortunately, ransomware and phishing. In fact, most ransomware is delivered by phishing. Phishing is where somebody sends an email designed to trick a reader into clicking a link or doing something that would give someone a foothold into their network. There are several types of phishing. We've got phishing. We've got spear phishing. We've got whaling. We have smishing. We have all these different variants of phishing that are targeting different people using different technologies, but the point is subterfuge, social engineering the reader, taking advantage of them going through their email too quickly and not fully attending to the message and clicking on a link or clicking on an attachment, opening it up, infecting the machine with malware, which then leads to the second threat, which is ransomware. A lot of times, clicking on a link launches a ransomware attack. Ransomware is where an actor cryptographically blocks and locks all of your information and data and holds that data for ransom. If you pay the ransom, then theoretically, and most of the time, they'll unlock your data and give you back access to it. Data availability is one of the most important things to most people and most companies, so it's a very, very effective attack. If you don't pay this ransom, you don't get your data back. Remember, hacking and intrusions are big business. It's not like it was back in the '90s when Paul and I started in this business. Back then, it was a lot of what we would call script kiddies, a lot of people doing it for conquest and to see if they could do it. It was often an intellectual hobby.

Now we are talking organized crime and nation-state actors and folks who are making a living from this kind of activity. Ransomware and phishing really are two of the biggest threats.

The move to massive remote work through the pandemic has, in my opinion, introduced a couple of new threats too. They are threats that I think are really emerging and are only going to get worse. One is attacks on virtual private networks. Unfortunately, we continue to put much of our protective focus on the perimeter, but once somebody gets in, they have full permissions. So, with all the remote work that's going on since the pandemic, there's a false sense of security that if I just VPN into my organization, my organization is then secured. But now think about where people are VPNing from. They're VPNing from their home. They VPN from the coffee shop. They VPN from a lot of environments that are not as secure and so now if an attacker can attack the VPN, they can then get into the organization and have free reign. That's not to say stop using VPNs. It's the same as virus detection software. People say, "Well, virus detection software doesn't detect everything, so what's the point?" Well, the point is it's going to block a lot of it, right? It's like saying, well, I can't keep from getting any kind of sickness or illness, so I might as well just go lick the handrail in a public environment, right? That's crazy. So, the same thing. You have to have the basic protections of virus software and you have to have VPNs, but now VPNs are becoming a significant target to threat actors.

I think IoT is another emerging threat because of its interconnection to those environments, but we can talk about that maybe a little bit later. So, I guess the conclusion is the biggest threat to organizations has always been and continues to be the person, the human, because at the end of the day, it's a person or employee that's clicking on that email, that's infecting the machine with malware, that's getting up ransomware. It's a human or an employee that's going to an insecure website that causes malware to be installed on your machine. It's a human that's creating bad passwords, writing down passwords, or reusing passwords. It's a human that's choosing not to install patches. At the end of the day, the human has been and continues to be the weakest link.

Paul Rivera: I'd like to second that. The remote worker right now is the additional dimension and a new risk to organizations these days with the push to remote work. When all of this began, a lot of companies didn't have the infrastructure to adapt to this remote work. So, what they did is, they migrated to the cloud to provide that infrastructure because it was quick and easy. Now, some of the challenge in going there is that there are a lot of potential risks doing work in the cloud, and if you don't have the experienced technicians to put the appropriate safeguards on that, that leaves the organization open to other types of vulnerabilities when migrating your infrastructure to the cloud.

I guess, especially with the recent political climate lately, some of the companies and corporations that are probably going to be big targets, especially coming up this year, are your infrastructure companies and financial companies. There's a lot of talk about these institutions and how they really have to up their game on security because of all the things going on right now in the world.

Jimmy Holmes: Paul, what cybersecurity measures should be a top priority for companies to protect themselves from these risks that we just talked about, as well as other technology threats?

Paul Rivera: It's the basics, right? You'll be amazed at how many companies don't do just really basic security and a lot of things today have been made easier to implement two-factor, multi-factor authentication, right? Many software clients provide that solution. It's just turning it on, right? Another thing, is backups, right? Backups will save a lot of heartache, especially with ransomware being one of the largest or one of the significant risks. Today, it's still growing. It's been around for a while and it's still growing, and backups can do quite a lot in mitigating that type of damage due to ransomware. Even practicing restoration to perform a backup is important. A lot of organizations don't practice a scenario in which they have to actually restore these backups. If you're not adept at making sure that your backup is able to work and restore or you don't exercise that, then they're worthless.

There are simple things to do. A simple thing that we've actually implemented recently, where we were like, "Okay, why didn't we do that earlier?" was just a simple external email tag. When you're receiving email, a lot of times they can be spoofed. Sometimes the email looks like it's from an internal co-worker/employee. Having that external tag, you'll say, "Okay, this is actually outside the organization." So, now you can be a bit

MEET THE PANELISTS

Nicole Beebe

Melvin Lachman Distinguished Professor
Director, The Cyber Center for Security & Analytics
Professor & Chair, Department of Information Systems & Cyber Security, The University of Texas at San Antonio

Nicole Lang Beebe, Ph.D. previously served for five years as the Director of The Cyber Center for Security and Analytics at UTSA. Dr. Beebe's research interests relate to cybersecurity, cyber analytics, digital forensics, and data analytics with applications to insider threat detection and analysis, IoT security and forensics, and cyber threat hunting. She has published approximately 50 peer-reviewed articles in top journals and conferences that have been cited over 1,500 times. Her research has been funded by the National Science Foundation, the Department of Homeland Security, various Department of Defense agencies, several industry partners, and has resulted in a patent-pending cyber search algorithm and multiple software platforms.

Paul Rivera

Co-founder of CyberOps Training Academy
President/CEO of Def-Logix, Inc.

Mr. Rivera has 20+ years of cybersecurity experience in the government contracting industry. He attended the University of Texas at San Antonio, the leading university in cybersecurity, where he obtained a bachelor's and Master's degree in Computer Science and Information Technology/Information Assurance Concentration. He is an expert in Information Technology specializing in red/blue team tool development, and computer and network security. As president and CEO of Def-Logix, Inc., Paul has earned recognitions in the cybersecurity industry and has led the organization to multiple awards as one of the fastest-growing companies in San Antonio, TX (2019 & 2020).

more cognizant on clicking on any links in that email. Lastly, and again, the big thing is the human element that Nicole has mentioned. Educate the employee on being aware of these two types of techniques that could breach security in the company and try to have some type of regular reminders. Maybe a monthly type of reminder of, "Hey, let's keep in mind that these are some of the things that we need to be careful with to safeguard the company's infrastructure."

Nicole Beebe: I completely agree with everything Paul said. I agree that external tagging on email is very important, but Paul has the luxury of working with lots of smart security people as his colleagues, right? Organizations need to remember and not have a false sense of security that they may have a lot of non-security-minded people. What happens in a large organization is one person on the inside gets their account hacked and then their email begins sending messages internally to everybody else. So, one of the things I'm concerned with is that the external tagging gives employees a false sense of security that if it's from the inside, they can trust it. You can't trust your fellow employees when it comes to email security because their account may be hacked. That's one caution.

On the backups, I can't agree more with Paul, and it's an unfortunate thing because if I want to put students to sleep quickly, I'll just start talking about business continuity planning and disaster recovery planning and talk about backups. They think it's just the most boring topic in the world, but it's so very important because you don't have to pay the ransom and you can just get your data back. You're like, "Okay, fine. I guess I'm upset that you have a copy of my data and maybe I have some intellectual property concerns therein, but I can operate." However, we have to start reconsidering how we do backups because the very thing that makes backups reliably done is that they're online all the time.

Now ransomware writers are getting smarter and they're ransomwaring the backups, and so you must have a layer of defense between your data and the backup itself. I think that's important.

Another thing I would throw in there from a defense perspective is checking web links. It's something that I don't see being done enough. You can have rules on your network that before your employee can open or can click on a link, it has to be tested, and nine times 99% of the time, that testing is done as the email comes in before you click on it. It's very rare that you're going to sit there as an employee and wait for the system to check the security of that link, but that really helps to make sure that your employees aren't clicking on links that they're going to drive by malware.

The last thing I'd mention is an area where more research and development is needed. We really need to move to zero trust networks, zero trust network technology and zero trust network policies and perspectives. I'm getting back to my first point. We have this continued perspective of perimeter security and trusting you once you get inside. We can't do that anymore for lots of reasons, for technology reasons, for insider threat reasons, for third-party vendor reasons. There are a lot of reasons you shouldn't necessarily trust the person who's on the inside or the machine that's on the inside. Zero trust networking is an ideal and a design framework where you continuously verify all identities and don't simply trust a user or machine request just because it's coming from the inside.

It says let me approach everything as if I can't trust anything and protect my network from that perspective, but the problem is zero trust networking is just emerging and it's not there yet, and we need companies like Def-Logix to keep doing the things that they do to make that a technology in reality.

Jimmy Holmes: Now, I'm going to ask a series of back-to-back questions to each of our panelists that relate to their specific expertise. Nicole, we're going to start with you. How has the Internet of Things changed the cybersecurity landscape?

Nicole Beebe: It's changed hugely. Back in the 90s, when Paul and I got into this space, it was like the Wild West of computing and everybody was doing all these classic things wrong. No offense, Paul, but software developers would hardcode passwords in their software. They'd create back doors that would make it beneficial for developers to go in and do things. They would just do all these things that were just bad security and we spent about a decade or so getting away from those things. All those bad security practices in product design seem to have crept back in with today's Internet of Things technologies. We're back to where we were in the 90s. IoT devices, because of their short-lived nature, are quickly developed and time-to-market is key. Companies think we have to get them out fast. We know there are security vulnerabilities. We'll fix them on the next revision. But nine times out of 10, they don't get fixed because consumers aren't demanding it. Consumers aren't savvy enough.

We're just now beginning to see marketing where people are using security as a differentiator. There are certain cellphone companies out there that are marketing that their network is more secure than another. Finally! That's wonderful! Until we have that across the board, however, manufacturers of IoT devices are going to continue to push devices out in a known insecure fashion with all the classic security mistakes that we had in the 90's. Now, think about the fact that there's going to be... I think we're up to 25 billion IoT devices right now. They're projecting 65 million IoT devices in the next three years. 65 billion devices.

What is Internet of Things? It's things that are connected to the internet and then interconnected amongst themselves. Now, you add 5G on top of that. Now 5G is enabling all these IoT devices to communicate with each other in a very effective manner. So, now you have IoT devices, like my Nest Thermostat, my Ring doorbell, and my SimpliSafe alarm system, or whatever it is at home all connected to my home network. I then use my UTSA laptop to connect to my home network, and I then VPN into UTSA. Do you see how easy this is? If I can attack an IoT device that's very vulnerable and use that as a hopping off point to get into the computer, to get into the network, to get into the university, that's a much easier way than trying to attack the university's front door.

So, with the huge explosion of IoT devices, the fact is that we're connecting everything to everything, and the fact that we have so many of them, the fact that they are so vulnerable, and the fact that 5G is now interconnecting the world is a huge security threat. It's increasing the attack surface, in my opinion, like you've never seen before, and it's connecting them at a speed, to be perfectly frank, that humans can't keep up with. If we don't increase our use of artificial intelligence and machine learning to help us with security to create active defenses, we're not going to be able to keep up with the detection, much less the response.

Jimmy Holmes: So, in a nutshell, you're only as good as your weakest link.

Nicole Beebe: Yes, and humans were weak and now IoT devices are weak. Very well said, Jimmy.

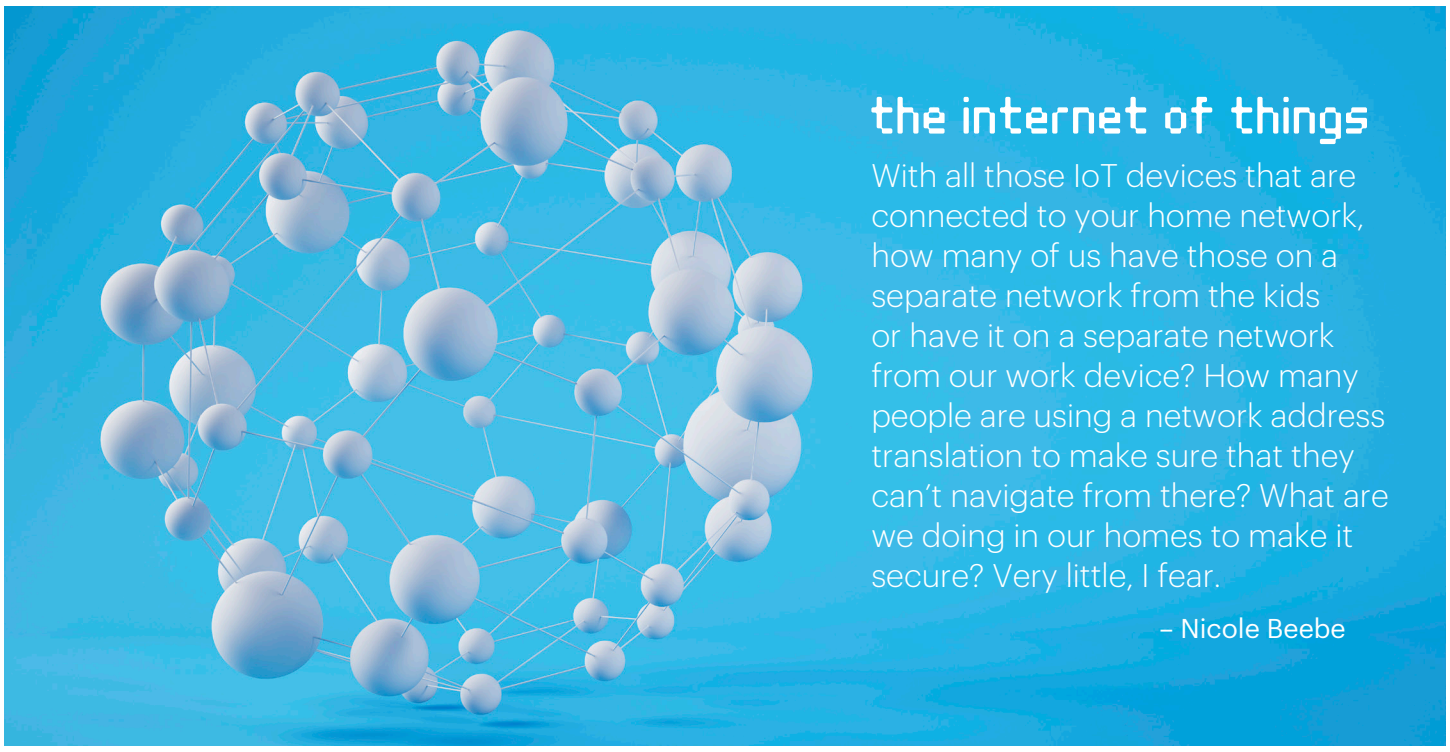
Jimmy Holmes: So, what is the impact of increasing prevalence of IoT devices and 5G networking on our personal business security? You touched a little bit on that, but anything you want to add?

Nicole Beebe: Again, it goes back to attack surface, and let me point this out. So, with all those IoT devices that are connected to your home network, how many of us have those on a separate network from the kids or have it on a separate network from my work device? I'd say probably 98% of us don't, right? How many people are using a network address translation to make sure that they can't navigate from there? What are we doing in our homes to make it secure? Very little, I fear. A lot of times, the routers that we buy that connect these things together aren't secure and so what you're doing is just increasing the attack surface. Any hacker is going to go after the easier way to get in, right? Furthermore, they'll go after the way to get in that has less logging. There are fewer detection mechanisms. They're very small devices with not a lot of memory and not a lot of processing power and so they don't have detection or defensive mechanisms in and of themselves. So, it's like leaving a door on my house open with a sign up saying, "Come on in, burglar, and oh, by the way, I don't have any cameras."

Jimmy Holmes: I'll put you on the spot here. So, what should universities be teaching those in the cybersecurity field?

Nicole Beebe: We need to be teaching all these different technologies. But a challenge is that we have to both educate and train. We have to teach foundational knowledge and functional skill. One of the great things about American college education is that it's designed to create critical thinkers and in a wide range of areas, right? We don't just take somebody in and teach them 120 credit hours of cybersecurity. While that would make for a very well-trained cybersecurity person, it doesn't necessarily create the same critical thinker or problem solver, and that's one of the strengths of American education.

The downside is it only leaves me with 30 or 40 credits to teach them cybersecurity, and then if I must introduce them to all the fundamentals, it's hard to teach them all the latest technology. So, it's a challenge. We have to teach them the latest and greatest technology. We have to teach them the latest and greatest tools, but we also have to teach them the fundamentals.



GETTY IMAGES

I think another thing that universities teaching cybersecurity need to do is help students perform in the workforce with the inundation of data that they're experiencing. What we're doing at UTSA to address this problem is we're launching a new applied cyber analytics degree in the fall of 2022. In one degree, students will obtain a solid foundation of knowledge and skill in modern analytics to be able to deal with massive amounts of data with machine learning, as well as obtain our world class cybersecurity education. They then learn how to integrate the two through cyber analytics. This is a first-of-its-kind degree truly addressing a next gen problem and workforce need.

Think about it. As you interconnect 65 billion IoT devices with traditional IT networks and with operational technology networks, the volume and variety of data is just... It's debilitating. You cannot throw enough humans at the problem and that's what our security operation centers are still doing today, "Oh, we have more data. Let's hire more people." Even if you could hire enough people, people, no offense, are slower than the attacks. We're slower than the bits and bytes that are traversing the network. We need machines to do some of that low level processing and then put a human in the loop. I'm not suggesting we have completely AI-enabled defense systems, but you use machines to do what machines can do well and do fast, and you give that data at higher level abstraction to the humans who can then discern what the motive is, what they're after, and how to best thwart that attack.

Jimmy Holmes: So, as security needs grow, what must be done to fill the skills gap in cybersecurity?

Nicole Beebe: I think one of the things that we need to begin to do is to realize the size of the cybersecurity field and that there is no one-size-fits-all. One of the things I fear that we're doing in American education, particularly post-high school with regard to cybersecurity, is we're all taking a one-size-fits-all approach. The field of cybersecurity has, depending on how you want to count it, over 15 different subdomains. You have people who are going to be technicians versus people who are going to be the highest most technical malware reverse engineer. We have to begin to create programs that are differentiated from one another. If I want to do this in cybersecurity, I should go to this school in this program. If I want to do that in cybersecurity, I should go to that program in that school.

We are treating cybersecurity education like we can teach everybody everything. Cybersecurity is so big and broad and deep and huge. Nobody can know everything, so we have to specialize and we have to begin to differentiate our program so that students will know where to go to meet their specific needs and interests. A great benefit of a large program like UTSA's is that there are enough choices and paths that someone who doesn't yet know exactly what they want to do in cyber can figure it out without changing schools.

Jimmy Holmes: Well, yeah, it's like a business school. Different degrees, finance, accounting, marketing, and cybersecurity is a relatively new thing at universities. I see what you're saying. The ability to specialize is a very complex subject.

Nicole Beebe: It is.

Jimmy Holmes: So, is there anything you want to add to what she just said, Paul?

Paul Rivera: Yes. Actually, on filling the skills gap, I agree that we have done a one-size-fits-all approach and , as a high school dropout, I think college has its place, but then I believe there are certain skill sets in cybersecurity where you really don't need a college education. One of the things that I've noticed with current employees is that the skills that are developed come from hands-on experience. So, I think there should be some programs developed that allow people who may not be interested in getting a four-year degree in college to basically learn the specific skills and actually get hands-on work to develop those cybersecurity skills, right? So, as Nicole said, maybe it's a school where, hey, this is network intrusion detection and all you learn is that, right? Another one may be analyzing system logs and where the individual gets a hands-on, deep-dive experience into that particular tool or set of tools for that aspect of cybersecurity.

Nicole Beebe: I couldn't agree more.

Paul Rivera: Maybe this is a shameless plug, but at Def-Logix we created a subsidiary where we are basically building a six-month training course where we teach these basic skills, but I think that it's going to be an essential part with the growing need. You can't wait four years to send someone to go into the workforce to fill in these huge gaps and skill sets.

Nicole Beebe: Trade schools.

Paul Rivera: Yeah, trade schools, exactly. I think that is going to be an essential part in the future for meeting these skills gaps.

Nicole Beebe: I completely agree.

If I could throw in one more thing. Depending on what study you read, there's a four-million-job shortage gap in cybersecurity, right? So, if you don't do what Paul is saying, which is to create skilled tradespeople in this area, and you rely entirely on college education, you're not meeting the need, right? Everybody doesn't need a college education, just like Paul said, but the other thing we have to do is we have to reach populations that are typically not in this field. We will never close the workforce gap if we continue to only have representation from the white male community. Just considering the numbers alone, we must tap into other demographics. Cybersecurity remains a very white male-dominated field. If we don't get females involved in this field, if we don't get underrepresented minorities involved in this field, we will never close the job shortage gap.

Furthermore, we need diversity of thought and experience to solve complex problems. Cybersecurity has some really complex problems and if we all come from the same background and bring our same ideologies to the table, we're not going to have creative solutions through diversity of thought to solve these big problems. So I agree. We need the trades. We also need to get a lot more underrepresented populations involved in cybersecurity to meet the job needs.

Jimmy Holmes: I know the pipeline is starting to get a little bit better as far as different programs in high schools. There are a lot of different ways you can feed a career and generate interest. We need to recruit from all different areas. Cyber attacks are crimes that we cannot have. The public sector is going to have to help manage

this and all different companies need to adopt certain policies. It's not just the IT department fighting this battle. Do you have any further thoughts on education for career readiness in this field?

Nicole Beebe: This is a little bit of a tangent, but you made me think when you were talking about high school students and younger. I also feel like we have a lot of young people who get engaged in this kind of activity because it's exciting and it's fun and it's cool, right? We need to have very early education and provide challenging, ethical outlets for these students. I joke to people about using their powers for good and not evil, but I mean it very sincerely. There are students who are underchallenged. They have these skills. They have these interests, but they don't have an outlet and, unfortunately, the outlet they find is on the dark web side. If we can find those students and both corral their ethics and give them the challenge, give them the challenge on the good side, that's a very powerful thing.

I've known some people in the government who have offensive cyber operator jobs and they ask, "Why do you keep doing that? Because you could make so much more money in private industry," and they say "Because I couldn't have this kind of fun on the outside, right? The things that I get to do are so intellectually challenging. There's no way I could do this on the outside or I'd be put in jail. So, those kids who have that kind of knack and that kind of interest when they're young, we need to harness and direct them in a very positive way early on.

Jimmy Holmes: There are a lot of high-paying jobs that that are on the defense side rather than the attacking side.

Nicole Beebe: Yes, sure.

Jimmy Holmes: Paul, let's discuss a term I've never heard before, homomorphic encryption. What is it and why is it important?

Paul Rivera: This is a recent research area that we are exploring and to be honest, it's a recent term I heard just a few months ago. So, basically, doing this research, I was shocked. I was like, "Okay, this is something that's been being worked on for the last, I guess, 10 years," and now that computers are getting more powerful now, there are some practical applications to this type of technology. So, with regular encryption, usually, when you work on data, you have to unencrypt it, do the operation, and then re-encrypt it, right? During that process, you can expose this data especially if the data is privacy sensitive. So, what homomorphic encryption does is basically allow you to encrypt.

Let's say, for example, it's a query, right? You're looking for a particular email address in a database and it's encrypted. The search for that, let's say, is ABC@yahoo.com. You can go ahead and check for that email address in that database and that query is encrypted, and also the search is encrypted. So, you skip that whole process of unencrypting the data and so there's no point in which that data is exposed to a privacy breach. So, where this technology is really looked at to be applied to is data that's in the cloud. Since a lot of people have been migrating to the cloud and they have a lot of this data in the cloud and, going back to zero trust, when you have your data in the cloud, you have to really depend on the security measures that the cloud provider has to protect your data.

So, if you're unencrypting your data in the cloud to do these operations, you may be exposing privacy sensitive data. It could be medical records. It could be financial records, things of that nature, and you have to worry about some of the regulations that these industries have whether it's HIPAA, PCI, SWIFT, etc. This technology allows you to do this work when you may not trust that cloud provider, but since your data is always encrypted, you can do these operations without sacrificing the privacy of the data. In a nutshell, that's what it is and where it could be applied to and why there's a big move toward using this technology because of corporations moving this data into the cloud.

Jimmy Holmes: So, what sectors is this recommended for?

Paul Rivera: Any sector where you must deal with regulations regarding privacy. That's your financial. That's your medical. It could be a lot of things. I mean, personally, I don't like having my data out in the cloud. So, we have everything on premises and the whole reason why is because I don't trust the security in the cloud and although there are some good safeguards in there, if you misconfigure something, then your data is exposed, right? Homomorphic encryption allows us to take advantage of the power of the cloud without jeopardizing security and privacy of your data.

Jimmy Holmes: Where do you see this currently applied?

Paul Rivera: Again, it could be a medical record search or let's say it's a COVID database. So, who's vaccinated? Right? There may be medical entities that may need to do a search, but you want to make sure that data is kept private and, again, financial, right? You may want to find out who's investing in this other offshore company. You know the entity by just querying this database for example. You won't expose all the databases' users or records and you only get that specific query element that you're looking for. So, that's what I think it's really useful for and that's where it's really moving into. It's really the financial and medical industries right now where the technology is being used currently.

Jimmy Holmes: Do you see anything different as far as in the future for homomorphic encryption?

Paul Rivera: Well, again, as data moves out into the cloud, everybody's probably going to explore this technology and will potentially roll out in the next five years, and it may be seamless. You may not realize it's happening, but all infrastructure in the next five years is going to be built out to provide that aspect of data protection in the cloud.

Nicole Beebe: Could I add another perspective in here? As people are listening to Paul and reading what Paul mentioned, I can imagine people going, "Well, that's not going to be a threat to me because they're not interested in my stuff or the time in which it's decrypted is so small because I decrypt it, do this thing, and re-encrypt it," right? There are a lot of people who think that the threat isn't very high, but when I teach my digital forensics classes -- the point of digital forensics is to do data recovery in support of some sort of investigation, and so a lot of times when we do investigations, we have suspects and criminals that encrypt things -- my students are asking me, "How do I get around that encryption? How do I crack it?" I say, "You don't. You don't mess with cracking the encryption nine times out of 10. You simply find the unencrypted versions of the data." The way most programs work is when it's encrypted, the decryption then creates a file, temporary though may it be in an unencrypted state, and then usually developers very unsecurely delete that. From a forensics person's perspective, I can get it back because it's still there. Just because you deleted it doesn't mean it's gone. It means it's recoverable.

Secondly, for the data to be presented to the user in an unencrypted fashion, it must go through memory and so it's cached there to be represented to you in an encrypted state. So, go back to the very beginning of this conversation. All I need is to put malware on your machine that puts a hook into memory or puts a hook into the file system to then show and bring back days later maybe the unencrypted data when it was unencrypted for five seconds. So, the threat Paul's talking about is a very real threat and it's not a very skilled attacker who can capitalize on that threat. When we talk cool words like homomorphic encryption, we would think that only the most skilled hackers could thwart security mechanisms, but it's not true. These are very serious vulnerabilities that Paul is talking about.

Paul Rivera: I'd like to add that in the old days, software was valuable. Today, it's data. So, any way you can get any type of data, that stuff can be monetized whether it's legitimate or illegitimate, right? That data is extremely valuable. And today, it's the data. It's not the software. Data is the gold nugget in any enterprise.

Jimmy Holmes: How do you both see the cybersecurity landscape changing over the next 12 months as it relates to what's happening in the world today in each of your fields?

Nicole Beebe: I'm going to make a positive spin. From an academia and education perspective, I'm very excited at the number of new cybersecurity programs that are popping up all around the world. I'm excited to say that I see a lot of professional and trade-oriented cybersecurity programs. Back to Paul's point that it's not all four-year degrees. I think from a positive perspective, I really see good momentum at closing that workforce gap, and the negative side that it has nothing to do with academia per se. I think in your context of what's going on in the world today, I think we're about to be in for a wild ride, right? I don't want to turn this political, but the Ukrainian power plant that was hacked five, six years ago was an exact example of what can happen. We recently experienced the Colonial Pipeline hack. That was ransomware and it created havoc for days with automobile gas outages along the Eastern Seaboard. If we're talking about what's going on in the world today and we're talking about a very unstable situation over in Ukraine and dealing with Russia, the threat of cyber war, more specifically the threat of an economic war waged on the cyber front, to me is a very real threat.

I think most organizations think, "Well, I'm just this organization," or "I'm just this company." If you are a third-party vendor to get into a bigger organization

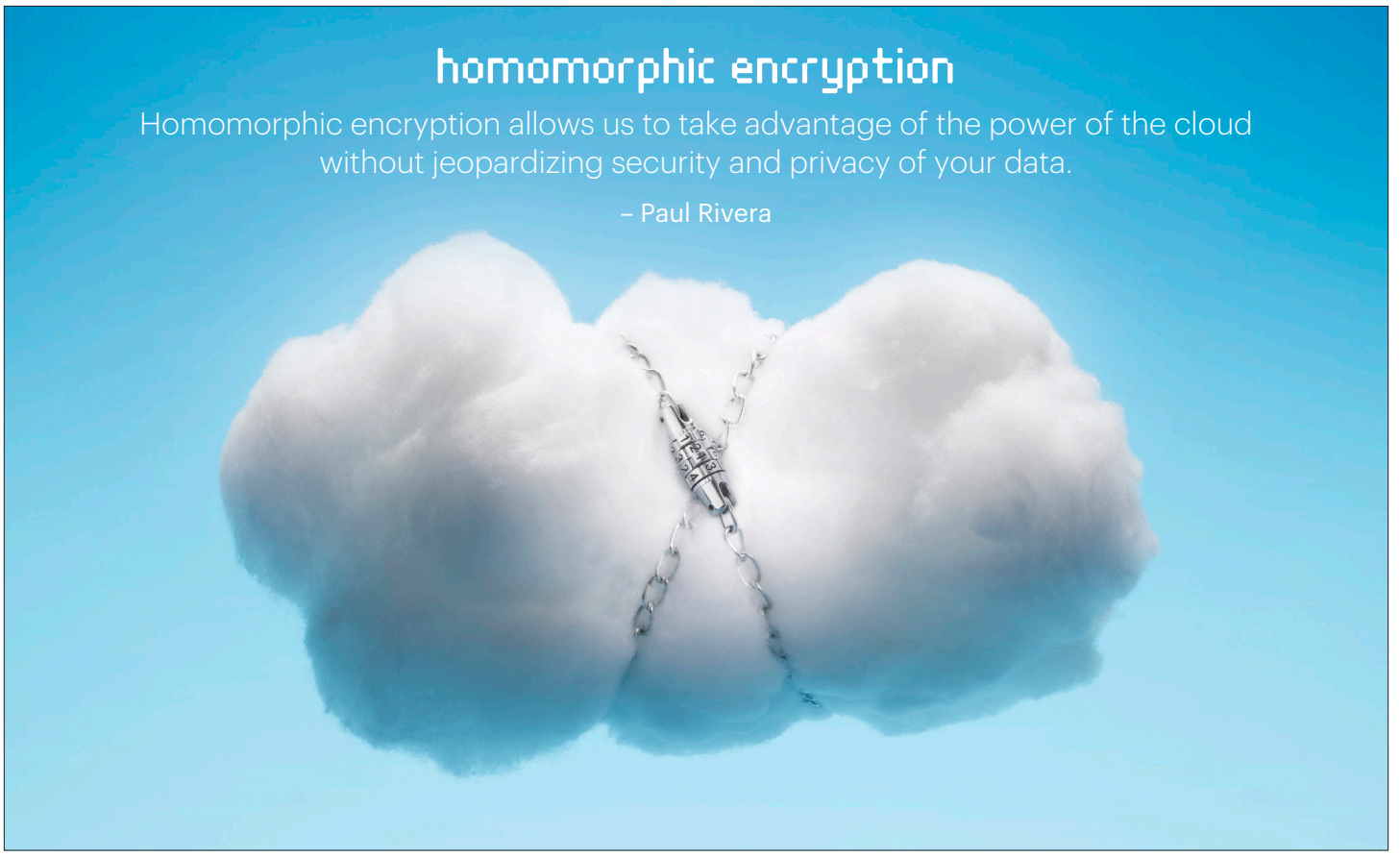
like a pipeline, just think about what can happen to our economy when critical infrastructures, transportation, energy, food supply, those types of things are compromised. Then go back to the notion of IoT and basic security. When you think of some point-of-sale systems that are still running Windows 98, which is a disturbingly large number, or food manufacturing plants that have industrial control systems that are, again, using very old operating systems, we have so much weakness in the cybersecurity posture that it's like a house of cards. The house of cards is very tall in our country of our capabilities and our way of life. Cybersecurity has some significant threats to our way of life and if we're compromised in very specific ways, it would be very bad.

Paul Rivera: Yeah, not only is it an international concern, but I also think a domestic one because of a lot of polarization with the different parties. You've been hearing a lot about certain platforms being hacked and it's due to political hacktivism, right? So, there's doxing. If you happen to have the wrong views, people may target certain platforms to get the data. Also, financial data can be threatened. There was one example I heard recently. There was some type of a funding platform that was breached and they got a list of donors and they started spreading this information, "Hey, these are the people who donated to this cause. Go get them." As a corporation, you have to be very careful not to end up on the end of a political argument. You may not have a dog in the fight with you, right? So, I think that that's going to be a factor this year, and of course, internationally, which is going to be big. I think there are going to be a lot of things with nation-state and even political activism. It will be a wild ride as Nicole just said.

Jimmy Holmes: Both of you are in the preventative trying to educate and protect businesses and educate students to learn how to protect businesses and their own personal lives as well. I don't know a person who's been on the internet who has not been hacked. What do you do when your bank notifies you or Experian notifies you that your information is on the dark web? What are you supposed to do with that information? What do you do once your data, whether it's your company's or your personal information, has been exposed?

Nicole Beebe: Well, one is to realize, unfortunately, what your identity is worth. It's a commodity. It's sold in mass quantity and you might be disturbed at what your identity is sold for. Dollars. Dollars. Complete health records may be 30, 40 bucks, right? It is an industry and so honestly, the best thing you do is clean up, patch, and move on. It's the same thing we do in cybersecurity. You have to clean up in the sense that... I know this goes back to backups. You have to be careful just restoring back to backups when the backups might have been compromised. If you were infected way sooner than you thought you were and you've got those backups with those infections in those backups, sometimes you have to do the hard, hard, hard work of starting from the beginning where you don't just say, "I'm going to buy a new phone and then clone this from that phone to that phone." Great. Now your new phone is hacked too, right?

So, sometimes you must clean up and clean up from the beginning, and the second thing is just protecting your money. It's basics of locking. In fact, I say do it proactively. Go to all of the credit agencies and lock your credit, and yes, the next time you open a credit card or buy a car, you'll have to go through the steps of unlocking that first, but you know you're unlocking it. So, those are the kinds of protections I think you must do and do your credit monitoring and that type of thing.



GETTY IMAGES

Jimmy Holmes: But once your data is out there, you can't retrieve it?

Nicole Beebe: The horse is out of the barn.

Paul Rivera: Yeah, it could be as easy as locking your credit card or getting new credit cards. You may have to do more like get new bank accounts depending on how deep the breach is, or even apply for a new Social Security number. That's going to the extreme, but once your data is out there, it's just a messy cleanup and it depends on how much of a deep clean you want to do. It could be locking your credit cards all the way to getting a new Social Security number.

Nicole Beebe: And of course, changing all your passwords, but changing them on devices that you know are not compromised. Don't just go over to your other device in the house. I'll go over to Paul's house and say, "Paul, can I change all my passwords on your computers?" It's a joke, but you can't just do it from your devices. If they're in your machine and they're watching what you're doing and you change all of your passwords, they now know all of your new passwords. So, you have to put your conspiracy theory paranoia hat on. Proceed from there.

Jimmy Holmes: Exactly and trust the professionals that they can do it for you as well because the average CEO is not versed in coding or cybersecurity, but you want to protect your business. You want to protect your employees the best way you know how. So, do you have any tips that you think a CEO could do to make sure that they're protecting their company better?

Paul Rivera: I would say hire the right people, and if you don't have the right people in your organization, go outside your organization and look for consultants who can help secure your enterprise and secure your business.

Nicole Beebe: For organizations, just like Paul said, backups, mandatory patching, password rules, password management systems, dual factor authentication, strong VPNs, those types of things are important. CEOs need to understand the term whaling. Getting back to the beginning of the conversation with phishing, whaling is when they go after the big fish, right? The "whale" in whaling is the CEO. So, that's Paul. That's you, Paul, right? They're smart enough to know to go after the big fish. You can talk to secret survey agents in town. They'll tell you about cases where CEOs were phished, sometimes through hacked accounts of their executive assistants. They'll monitor things and they'll understand when the CEO is doing a large transaction. They'll do a man-in-the-middle attack and then have that money redirected somewhere else.

We're talking millions of dollars. Why go after little employees with little money when you can go after the CEO and go after big money? CEOs, anybody in the C-suite, are increasingly a target.

Paul Rivera: I've even had some employees in my organization get texts saying, "Hey, it's Paul. Can you send me this amount of money? Can you put it on this card?" And then I'll get asked, "Hey, are you asking for money?" I respond by saying I will never ask for any money from our employees. So, they even get emails and texts.

Jimmy Holmes: Well, I am learning a lot myself, some new vocabulary, and I'm a little bit more paranoid. But I think a little bit of paranoia is a good thing to help make sure that you don't drop your guard and you are being proactive by doing the backups. You've got to verify what you're being asked to do with a good old phone call and asking them "Did you send me this?" to the person that you think sent it to you before you click on a link. We definitely have to get better at that.

Nicole Beebe: And if I could make one comment, I always hate doom and gloom talks, right? And every time we get into this kind of talk, it's a little bit doom and gloom. I think sometimes it creates the sense to the customer, the reader, the hearer, "Well, it's no use. What's the point of doing all this?" because if somebody really wants to hack me, they will. I agree with that. If somebody with enough skill wants to do it, they will figure out a way to do it even to the most secured organizations or people, but a lot of the targets and the attacks are targets of opportunity, right? Maybe I want to get into that organization, and if I want to try hard enough, I'm going to get in, but if I can't get in through Paul because Paul is better secured, I'm going to get in through Nicole if Nicole is less secured.

It's about targets of opportunity. So, don't throw up your hands and go, "Well, it's no point." If somebody wants to get in, they'll get in. Great. Well, don't you be the weakest link. Don't you be the easy target of opportunity. Don't you be the open window to get into the house when the front door is locked. These are basics.

Jimmy Holmes: That's a great analogy and example. They are going to keep moving on to another company, another person and send out that phishing email to a million people and see what happens. They might get five. All you can do is be proactive and protect yourself better, so you are not the weakest link. I think that's fantastic advice.

TABLE OF EXPERTS
SAN ANTONIO BUSINESS JOURNAL

If you'd like to participate in an upcoming roundtable discussion, contact Liz English at 210.477.0854 or LEnglish@bizjournals.com.