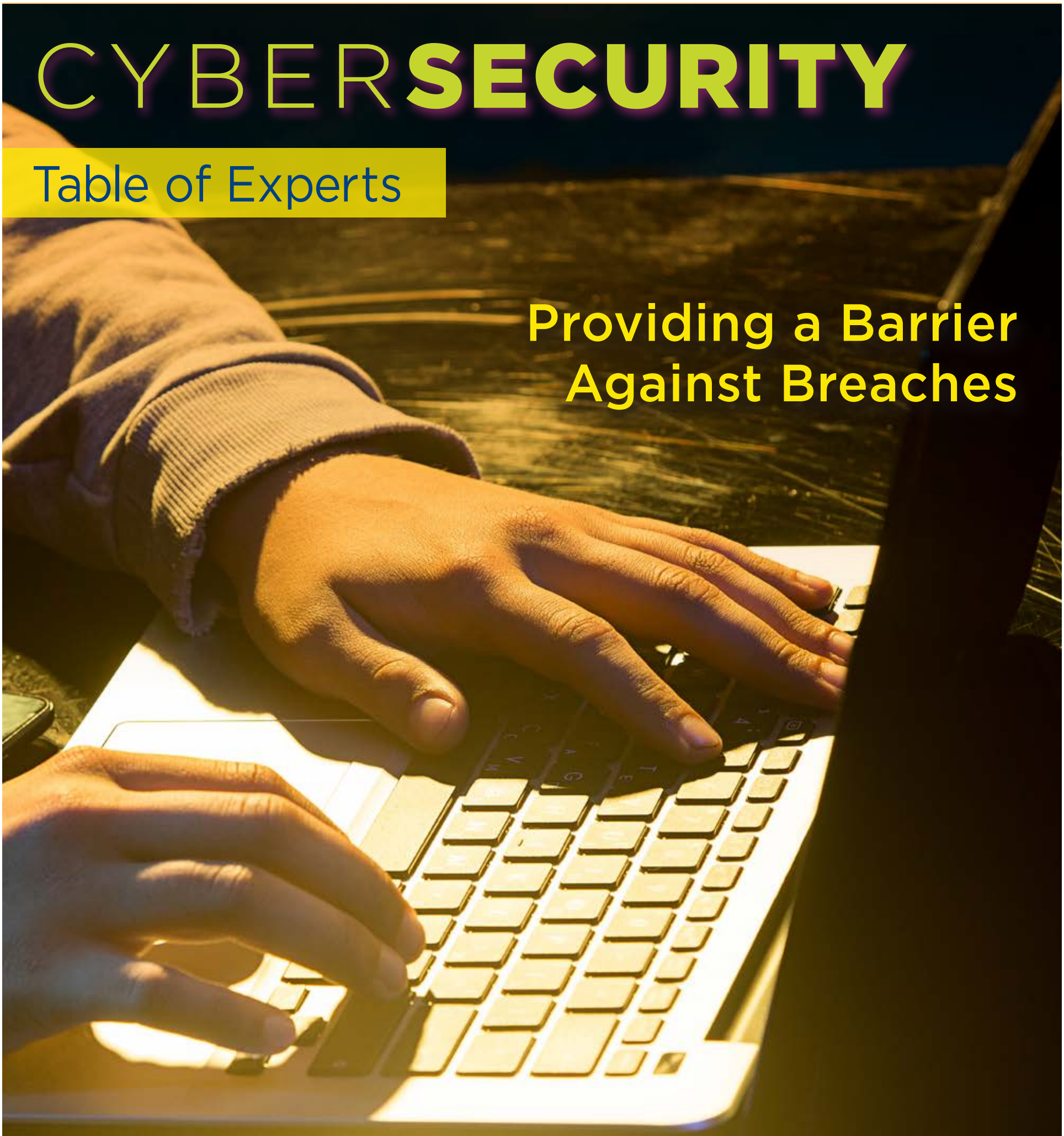
ADVERTISING SUPPLEMENT TO THE PHOENIX BUSINESS JOURNAL

CYBERSECURITY

Table of Experts

Providing a Barrier Against Breaches



Sponsored by

Accountabil IT

INFINITY INSURANCE PARTNERS

Insight

PERKINSCOIE COUNSEL TO GREAT COMPANIES

University of Advancing Technology UAT Learn. Experience. Innovate.

ADVERTISING SUPPLEMENT TO THE PHOENIX BUSINESS JOURNAL

KARIN ALDAMA

Partner

Perkins Coie LLP

Karin focuses her practice on complex insurance recovery matters, including successful London arbitrations under the Bermuda Form. She also has extensive experience with complex commercial and appellate litigation, as well as with managing privilege law issues including in international and cross-border contexts.

In her representation of fortune 500, large and mid-size companies and governmental entities, Karin counsels clients operating in a wide range of industries, including the utility, aerospace, semiconductor and online real estate industries. In addition to her extensive experience in state and federal courts, Karin provides representation in alternative dispute resolution, with an emphasis on international and domestic arbitration. Karin also frequently represents indigenous detainees pro bono in immigration court as well as before the BIA and appellate courts.

Karin serves on the boards of the Herberger Theater Center, Act One, and the Arizona Women Lawyers Association and on the Maricopa County Bar Association's Diversity and Inclusion Committee.

Table of Experts Panel (L-R) Paul Zalewski, Dr. David Bolman (Moderator), Jessica Loomis, Curt Cornum (not pictured, Karin Aldama)

Dr. David Bolman: Talking about cyber security, insurance is a place people don't normally think about, but it does reflect how cyber security and keeping information secure is part of everybody's life.

Jessica Loomis: One of the biggest things is we ask, "How are you protecting your data?" We don't care if you're a construction company or a hospital. And a lot of the time they say, "Oh, well, we don't need that. We're not going to get hacked, we're not going to lose the data."

Dr. David Bolman: Has the insurance industry had many attacks?

Jessica Loomis: Not from a property and casualty standpoint, but from a healthcare standpoint, Blue Cross Blue Shield has been hacked, and there's been a few other healthcare carriers that have been affected by cyber hacks and attacks.

Karin Aldama: Cybersecurity really should be a concern to everybody these days. That includes both data such as Social Security numbers or bank accounts, for both clients and employees, and confidential business data. What that means is that essentially any business is a potential target for hackers.

Dr. David Bolman: Are medium and smaller organizations equally as vulnerable, or targeted?

Jessica Loomis: I would say one in five small businesses are affected. Medical offices are probably one of the largest. Financial planners are another that is largely affected.

Karin Aldama: If they have confidential or personally identifiable information, absolutely. Maybe not with the same type of organized, well-planned attacks launched against large healthcare providers, financial institutions, or retailers, but definitely as a target of opportunity.

Dr. David Bolman: Are we seeing much ransomware in Arizona?

Jessica Loomis: I've had several clients basically open an email from a client and then their systems are frozen and it's costing them several thousand dollars, probably in the $30,000 to $40,000 range, to try to fix things and recover their information.

Dr. David Bolman: What do you recommend individuals and companies do to protect from these kind of hacks?

Jessica Loomis: Education is the biggest thing. We send information constantly about what types of new cyberattacks we're seeing. We try to get them to educate their employees, even have seminars with their employees to let them know what's happening. Testing their employees, sending out phishing emails to see if they open them. These are the types of things that we recommend our clients doing.

Karin Aldama: Assess and reassess their security protocols in terms of technological and business developments. Train and retrain employees — including management and senior management — on security issues. Put in place an incident response plan that identifies who will do what in the event of a cyber incident, run drills on that plan, and keep it updated. In terms what to do about it, get appropriate insurance coverage.

Dr. David Bolman: Curt, in your world, what are the biggest issues you're seeing with cyber security?

Curt Cornum: There's three buckets. One is, how are our clients engaging their customers. In other words, what security do they need to deliver that kind of client experience that they need to be relevant in the market. The other one is around workforce enablement. What are our clients doing to enable their workforce so they can provide that differentiated experience to their customers. The third bucket is around infrastructure optimization. That is all the things the end users don't necessarily see, like the servers and the storage and all the switches and those types of things that are in the background.

Dr. David Bolman: What trends are you seeing in their awareness of what it takes to train the staff, have the infrastructure securely architected, and things like that?

Curt Cornum: I think Jessica mentioned the training component is a big deal. Whatever number you apply to it, whether it's 10 percent or 20 percent of the breaches that happen the way Jessica described, with somebody clicking on a rogue link or attachment. If you could reduce that number without applying technology — by educating users — there's a huge benefit in doing that.

Dr. David Bolman: The motion towards cloud services has different set of security issues and concerns. How do you talk to your clients about that?

Curt Cornum: There's the cloud-first mentality that's out there and there's a mobile first mentality out there. Now, there's also the Internet of Things piece out there as well. The cloud-first mentality is when you have a business that needs to make a decision, "I need this application," either for, like I said, workforce

enablement or better client engagement.

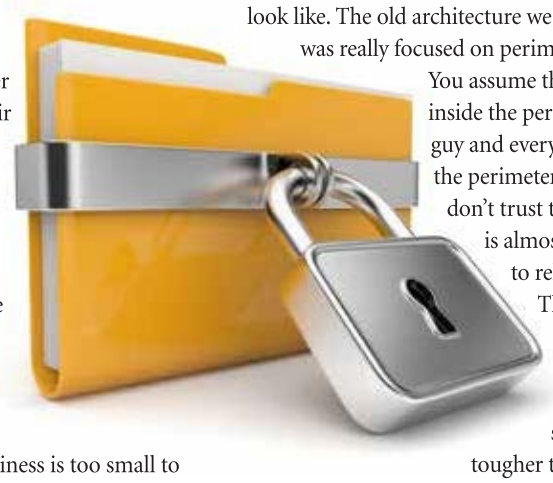
So, a lot of folks have adopted a cloud-first strategy for those applications. Then you combine that with the mobile-first strategy, where users want access from anywhere and from any device. Those two dynamics, cloud-first and mobile-first, are radically changing the environment that we see.

Dr. David Bolman: Do you encounter that, and how do you work with that?

Jessica Loomis: We try to educate our clients that is just because it's in the cloud, doesn't mean it's necessarily safe. And sometimes they don't realize that they're still liable for that data, even though it's in the cloud. We come to them and we're saying, "Okay, yes, it's in the cloud, it's safer in the cloud, but you're still responsible and liable for that data, whether it's in the cloud, whether you're processing payments and you have a payment processor, you are still liable." A lot of the smaller and medium-sized companies don't realize that it doesn't matter who's storing the data, they're still responsible.

Dr. David Bolman: As you're talking to those kind of customers, if you had to give them the short list of things to know and do, what would it look like?

Jessica Loomis: Make sure your cloud-based company has its own cyber liability and they have their own insurance to protect your data in the event that there is a loss. Read your contract and read those indemnifications, and see who is responsible for your data once it's in the cloud. And get your own cyber liability and data breach insurance.



Karin Aldama: No business is too small to think about cyber security and cyber coverage. When you look for cyber coverage, keep in mind that there are not yet any standardized policy forms, though standardization is definitely increasing. When you purchase cyber coverage, read all the fine print and beware of warranties and exclusions. Also, carefully assess both deductibles or self-insured retentions and policy limits – you want the right amounts for your business. Brokers and coverage counsel can help with all of that. If and when you experience a cyber incident, involve coverage counsel sooner rather than later.

Curt Cornum: I think you mentioned ransomware, Jessica, and it's probably the most insidious, because it is the most direct line from the breach to somebody collecting money from you. And when they're using cryptocurrency, there's this anonymity that's going on as well that makes it very tough to track the hackers down. If you look at the numbers, there has been a huge explosion in ransomware, and a lot of that is because of the dark web and cyptocurrency.

Dr. David Bolman: Do you typically recommend that people pay the ransoms?

Curt Cornum: I wouldn't recommend they pay the ransoms. I would recommend that they have backups and that they have a plan in place if they do get attacked by ransomware. You know, the story goes as soon as you pay a ransom, then you're on another list of folks who pay ransoms.

Dr. David Bolman: So, one of your suggestions to prevent a ransomware attack or to respond effectively, is to have backup data. Are there other steps you'd recommend companies do to protect themselves as best as possible against ransomware?

Curt Cornum: There are best practices that we recommend, without going into the weeds, around what the network architecture should look like. The old architecture we used to build was really focused on perimeter security. You assume that anybody inside the perimeter is a good guy and everybody outside the perimeter, well, you don't trust them. And that is almost impossible to rely on anymore. The definition of the perimeter has changed quite a bit so it makes it tougher to defend. If you can't get to a zero-trust architecture, you should at least adopt a zero-trust mindset.

Dr. David Bolman: Are either of you seeing any shifts where businesses are moving away from having transactions occurring over email to some other medium to prevent this kind of attack?

Jessica Loomis: No. I think people still feel safe doing these transactions over email. It's easier. Now we're getting into electronic signature. And if they're in your system, they have your electronic signature. I think we're getting more towards electronic versus doing things more manually or over the phone.

Dr. David Bolman: A topic you hear about often, or guidance that's being given in protection against cyberattacks, is some form of dual authentication. How quick are your clients to picking that up?

Jessica Loomis: It's hard enough getting a signature, and the information you need when you're sending the first request, to get a second authentication, I think is going to be quite difficult because people just want to be able to sign it, or do what they need to do, and be done and not have to worry about it.

Dr. David Bolman: I think that's where the crux of everything happens in the business space. On the one hand, we're trying to get things done, and we're being very efficient, we're moving relatively quickly it's part of our business strength, using technology, but if you've got that, then it's very easy for someone to get the, "By the way, please click this link to approve this UPS package on your desk." And someone goes by super quickly and clicks. And it takes a fair bit of training to get past that.

Curt Cornum: I think there is some promise there. Because it hasn't been cheap to implement, especially for small and midsize business, and it hasn't been without some complexity. For example: are you carrying a fob? Are you doing it with some software on your phone? I think we are making headway by making it easier to adopt these technologies. I think if you're not looking at or already doing two-factor authentication, you need to be. Just in terms of the user access control and being able to engage your clients. When people walk into your place of business, a lot of times, the first thing they ask is, "Can I get on your WiFi?"

Dr. David Bolman: You earlier mentioned cryptocurrency. Which is bitcoin. Can you talk briefly about what those are and where they're headed?

Curt Cornum: It's true bitcoin specifically has enabled a lot of the cyber criminals today. Even though you could potentially track down somebody that's using it, it's fairly anonymous even though it's an open ledger that you can see. The upside to things like bitcoin is there's about 2 billion people in developing countries that aren't as privileged as a lot of us. They don't have access to credit cards and checking accounts and

CONTINUED ON PAGE 30

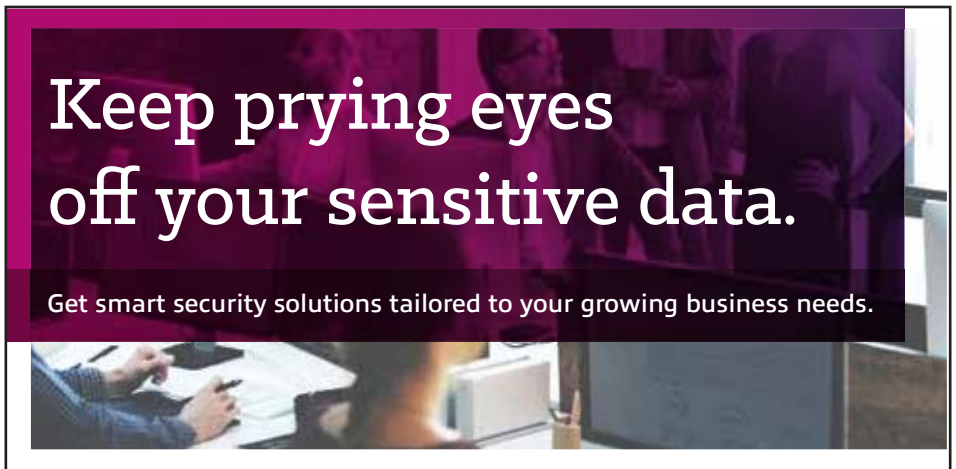
DR. DAVID BOLMAN

Provost

University of Advancing Technology

Provost Bolman has focused his career upon addressing the profound need within Arizona and the nation for a substantial and diverse creative class workforce. As its long standing provost, Dr. Bolman has built the University of Advancing Technology (UAT) into a unique all-STEM institution that marries the best of traditional small private college learning with the genetics of innovation that come with agile technology organizations.

Dr. Bolman has grown UAT from a single classroom of 13 students into a STEM private college campus that is unique not only to Arizona but also the country. UAT and its community are dedicated to advancing society through students who learn the tools, techniques, concepts, and responsibilities of applying technology in ways that lift up human society. He is an alumni Valley Leadership and currently serves as its past board chair. He is also an alumni of the FBI Citizens Academy and serves on the AZPBS community board.



CURT CORNUM

Vice President of Services

Insight

As Insight's chief architect and vice president of services, Curt is responsible for developing new solutions that help clients navigate the changing technology landscape. By understanding emerging trends, client requirements and the strategic direction of the tech industry's top vendors, he helps business and IT leaders develop frameworks and reference architectures that put technology to work.

Curt joined Insight in 2008 through the Calence acquisition. During his Calence tenure, Curt helped clients, including Wells Fargo, Intuit and PayPal, develop enterprise-wide secure network architectures. Prior to Calence, Curt was a sales engineering leader for Bay Networks where he specialized in designing virtual private networks (VPNs). He has also held internal IT positions at financial services and high-tech manufacturing companies, and has been designing secure network solutions since the early 1990s.

A Phoenix native and a former U.S. Marine, Curt earned his bachelor's degree in business from Arizona State University.

CONTINUED FROM PAGE 29

those kinds of things and bitcoin is enabling them to get paid for services using their cellphones.

Dr. David Bolman: For most U.S. businesses, it's really pretty much on the fringe.

Curt Cornum: It is. But the underlying technology behind bitcoin – blockchain - that is really where the power lies. It's very secure, and it's because of the blockchain technology. And what you're seeing is a lot of financial institutions using private blockchain technology. So they take that public technology and they're going to move it internally. And there's some very good reasons to do that.

Dr. David Bolman: Blockchain, at the top of the year, was listed on most lists as one of the top 10 most-influential emerging technologies in the country.

Curt Cornum: Yeah, it's really not about currency, it's about trust. And how do I apply trust in an open environment. You see a lot of companies today, where they use third parties for escrow and those types of things, that's really what blockchain can do, it creates a platform that provides trust in a peer-to-peer way.

Dr. David Bolman: As you're working with your clients, what are the top couple of things you're saying to them right now?

Paul Zelewski: Really the top thing is customers and enterprises need to develop a security program. A security program is many-faceted, but it needs to address the preparedness of the environment as well as how you react when an incident occurs. What we observe many times is customers or enterprises purchasing technologies, but then not really being prepared to manage them.

Dr. David Bolman: For most small and midsize businesses, that isn't in their wheelhouse.

Paul Zelewski: I think from my perspective, they need to reach out and find service providers that can assist them along that path. I think alternatively, they need to pursue training and education and make sure they have resources that are following that program, that path. You need a chief information security officer, you need those kinds of things in your mix.

Dr. David Bolman: In your experience, what kinds of activities are best done by the company and what are best done by service providers like yourself?

Paul Zelewski: I could make a case for going to a service provider for all of those things because they are the best equipped and most knowledgeable of best practices. However, in midsize businesses and small businesses, that's not always a practicality. I believe that, really, companies need to initially focus on the basics. And the basics are currency and patching.

Dr. David Bolman: Let's say I'm a small business. And I approach a service provider like you and I say, I want you to do all of it. What guidance would you give me on how I would interface with you? What skills would I have to learn without becoming an IT professional, because I'm busy running a business?

Paul Zelewski: It is an interaction where, via the initial assessments that we might perform, due diligence on what their environment looks like, and charting that path to really, what's a sustainable, maintainable environment. A big part of security is training and pushing training

to all of the users.

Every company, as part of their security program, needs to have a security awareness training. If you're PCI and HIPAA and those kinds of things, but just knowledge of what is it a phishing attempt? And, what to do when you're not clear.

An example in my own company with IT professionals who have been in the industry 30 years. One recently responded to a phishing email, where this was the CEO of my company, responded to a phishing email that was requesting a $15,000 payment. It actually was our CFO. And he had no reason to doubt it because it was a request from the CEO and he was out of the office, requesting this check to be sent to a particular place. Fortunately the interaction occurred after we had gone through a lot of security awareness. Before that transaction took place they said, well, they have a process where they pick up the phone and talk to each other and now they actually have a pass phrase they use.

Dr. David Bolman: Explain what phishing is.

Paul Zelewski: Phishing is where an email comes across as though they're impersonating another person from your organization. And they're typically requesting some sort of cash transfer to a particular bank account. If you really observe it closely, the impersonation is not exact, but they've done sufficient research on your company such that they know who the players are, they know who the executives are and they know the structure so that it appears to be a reasonable request.

Dr. David Bolman: What is the protection against that?

Jessica Loomis: Probably a phone call. Because if they have access to signature, if they have access to all of that information, your account numbers, everything, I would say a phone call or something to just confirm that it's truly the person that's requesting it.

Dr. David Bolman: Would two-factor authentication help? You mentioned pass phrases.

Jessica Loomis: Absolutely. If it's a phone call, a pass phrase, having that type of relationship with your banker, your financial planner and the people in your office to understand if this is a request that I'm asking of you.

Curt Cornum: I think that's the point — to create some other channel. The acronym was PUT: pick up the phone.

Dr. David Bolman: What are some of the things they should look towards the next 12 to 24 months?

Curt Cornum: Businesses should look at developing their security operations infrastructure. It's what I call moving from SIEM to SOC. SIEM stands for Security Information and Event Management. I think everybody is probably there to some extent, or they feel like they are. They may not have a full-blown SIEM platform, but they're at least trying to understand what's happening in their environment. They probably don't understand it totally, that's why there's this move to being more offensive, which is where the SOC or Security Operation Center comes in. Building a full-blown SOC is beyond the scope of a lot of companies, so they may do some taks internally, but the 24-7 aspect for example, maybe they let somebody else do that.

Paul Zalewski: Most small, and even medium- and large-size businesses are ill-equipped to select what tool set, what methodology, what approach they're taking. And when they can find a service provider that provides SOC services that are bundled with SIM and vulnerability management and other kinds of assessment tools, that enables them to engage and frequently at a price point that's much different than if you had to do all of that yourself.

Dr. David Bolman: I'm going to use this as a vague advisory moment, because my space is higher education, and UAT has graduated more cyber professionals than probably any place in the country. If you had to give me guidance on what they would like in a cyber-trained workforce, what would you tell me?

Jessica Loomis: From our aspect, I would just say that we continue to talk about how we can prevent these attacks from happening, but they're going to happen. And, so then what next steps after it's happened do you take? And a lot of these companies don't have the understanding that their business could basically be crushed, and they could lose everything from one simple hack. And so they don't have the insurance in place to protect those liabilities and protect their clients, their loss of income

Curt Cornum: With the transition we're seeing, I would start with the why. In other words, why are these hacks happening? Who's doing them and what's their motivation? It's much more of a criminal operation today and it's not like they're all super organized. There's folks that

can just go download malware from a platform that a hacker created and then the hacker takes a cut of anything this person gathers. So, they're not all super professional, but the tools are there to enable others. So, first it's around getting cash. Second is around corporate espionage. Number three is for the notoriety.

The most valuable thing is for folks to understand the tools, what's on the horizon in terms of tools that are being brought to bear to handle this. Things like machine learning to look at data traffic and anomalous user behavior, those types of things. I think we need to rely on machines and analytics tools to do that.

Paul Zalewski: I think, a graduate today, of course these are educational paths that didn't exist when I was coming up. I don't think there was any curriculum around security when I was graduating. And I think a graduate needs to understand that day one you're probably not going to be the chief information officer at a company. Sometimes you start in the mail room, but the opportunity to gain experience is in those SOC kind of environments and working with.

Karin Aldama: The cyber workforce should stay aware of technical developments and revise their security plans accordingly. They also need to stay abreast of legal and regulatory requirements. But security is really not just the task of the cybersecurity workforce, it's everybody in a business.

Dr. David Bolman: There's this other side of security, which I think is growing faster than we realize, which is the small business version. Which are the kind of skills that are involved in securing an architecture, making sure that protocols are in place, you know, and that data is being handled properly, and things like that.

On another topic, we're seeing more IP violations going on. Could you describe a bit what that would look like to a business that probably hasn't thought of this before. You know, the idea of this theft occurring in digital space. What does that look like?

Curt Cornum: Well, it looks like an employee that's exfiltrating data as we like to say, and that does happen and it's an area that most small and midsize businesses don't really focus on.

Dr. David Bolman: Kind of the current millennium's version of stealing the Rolodex.

Curt Cornum: Exactly, and for a lot of small and midsize businesses, that is their customer base. And because it impacts their ability to transact, they literally lose their ability to run the business.

Dr. David Bolman: Is that the kind of thing that as a provider you protect against and you insure against?

Jessica Loomis: Yes, loss of income, theft of data. Third-party liability for in the event the insureds clients' data is stolen. As well as expense reimbursement that includes attorney's fees, notifications, as well as forensics. There are a lot of exposures that can be covered under cyber insurance.

Dr. David Bolman: My last open question was the next 12, 24 months what are the big trends?

Jessica Loomis: Sometimes I feel like we're just constantly trying to scare people. And I don't think that's what we're trying to get across. I think that more than anything, it is about education. I think that really people maybe don't realize that your insurance broker is someone that can assist. If you do have cyber liability, the

insurance carriers actually have resources. They can figure out where you need to start and then maybe guide you through the process of securing your data and in taking those initial steps.

If you could utilize the resources that you already have, that you maybe don't realize you do have, like calling your insurance broker and saying, "Hey, if I buy cyber liability, I understand that they might be able to help me with some of these."

Dr. David Bolman: Most people are probably unaware that there's cyber insurance out there.

Jessica Loomis: And that the carrier is actually there to provide services for them, to help them protect their data, because the carrier doesn't want to be liable for that loss of data either if they can help it.

Paul Zalewski: I think the education is working. I find it interesting that because I think the media promotes it that conversations I have with people like my mother-in-law, who is aware of what WannaCry is. So that part is working. But I think when I travel to some of the security conferences, they're very much right now advocating that this is a huge war and we're losing.

Curt Cornum: I agree with you, Jess. I don't really think there's an apocalypse out there, although you might think that sometimes, with what you read. And I do think that there's a lot of positive things out there. But I think we can do better. My guidance for folks is don't go at it alone.

Karin Aldama: Increasing standardization of cyber policies, and developing case law addressing specifically cyber policy language. Thus far, much of the litigation relating to cyber coverage has concerned policies other than specialized cyber policies, such as directors' and officers' policies, crime policies, or general liability policies. Those can sometimes be analogized to cyber policies, but it will be helpful to have more precedent construing the language actually contained in cyber policies. That will give both policyholders and insurers additional information helpful in risk assessment and underwriting.

Dr. David Bolman: Arizona is facing a tremendous cyber workforce gap that will affect our information security for the next 5-10 years if we don't accelerate building tech professionals. Locally, thousands of people are needed who know how to talk the language and architect information security. Unfortunately, it takes about 10 to 12 years to cook a cyber professional using traditional approaches, and even then there simply aren't enough individuals in the pipeline to meet the need. What I advocate for, and what UAT is having success with, is creating programs for high schoolers, middle schoolers, college students, and working professionals who are looking to get into a field. UAT's programs, hack-a-thons and community outreach are shaping the workforce driveline by immediately cultivating enthusiasm for cyber security among a more diverse group of candidates and fast-tracking people into the workforce.

JESSICA LOOMIS | CEO

Infinity Insurance Partnership

After over a decade in the insurance industry Jessica Loomis, founder and CEO of Infinity Insurance Partners, decided she could create an insurance brokerage that was truly focused on what the client needs. A client oriented insurance brokerage that provides amazing service, education and risk management. Jessica Loomis has 18-plus years in the insurance industry working not only with the large insurance brokerage firms but also for the insurance carriers. In her spare time, Jessica enjoys supporting local nonprofits in the Phoenix metropolitan area. Some of the nonprofits that Infinity Insurance Partners supports include Arizona Technology Council. Jessica believes "It is important to support the community which in turn supports our economy. Technology will be a huge part of that economy." Another passion of Jessica's, as a single mom, is to support her daughter in her love of dance through a local Performing Arts Studio. Jessica enjoys golfing with friends, colleagues and clients.

PAUL ZALEWSKI | CTO

AccountabilIT

Paul Zalewski is an IT professional with more than 30 years' experience providing IT customer support solutions in a wide variety of business applications and infrastructure environments.

Since receiving a BS degree in computer science in 1979, he has continually been employed in a customer support role as an outsourcing or managed services delivery team member, first with the Sperry Corporation (Unisys), then with Boeing Information Services, SCB Computer Technology, OneNeck IT Solutions, as an independent consultant, and most recently as CTO with AccountabilIT. As a result of these experiences, Zalewski has developed a keen awareness of the principles and practices that contribute to world-class solution delivery and customer support, and demonstrates a special talent for contributing, building, and maintaining world-class customer-focused technical support teams.

During the last several years, Zalewski has applied his experiences providing technical leadership working with customers on their transformational journey from private to public and hybrid cloud solutions, with an emphasis on enhancing the maturity of the customer's security landscape as an enabler of the transformation. He is responsible for providing executive and technical leadership to AccountabilIT's Cyber Security Services offerings.