TABLE OF EXPERTS

Battling the Ghost in the Machine

Local business leaders discuss cybersecurity risks, possible solutions

Although tales of early email fraud have made a meme of Nigerian princes, online scams are no laughing matter. In 2023, Gallup Research concluded that in the previous year, 8% of American adults had been tricked into sending money or providing access to their bank account. With AI on the horizon, the threats are becoming much more sophisticated. With millions at stake, the risk is potentially devastating to small and mid-sized companies. Problems this massive require robust solutions, sometimes within a constellation of professionals across different industries.

To that end, the Austin Business Journal recently hosted a panel discussion with business leaders from the fields of banking, insurance and cybersecurity. Participating in the discussion were Rich Perez, VP of Innovation, Texas Bankers Association; Shane Gronniger, CEO, GCS Technologies, Sumera Riaz, Senior Director of Cybersecurity, Bluewave; and Mike Draeken, Risk Management Executive, Watkins Insurance Group. ABJ's Market President and Publisher, Abby Mellott, served as moderator.

MEET THE EXPERTS

MIKE DRAEKEN
Vice President, Shareholder
Watkins Insurance Group

Mike is a highly successful risk management professional with 20+ years of experience. He helps companies manage their risk profile so that they can focus on growing their business.

Prior to joining Watkins, Mike spent 13 years as a commercial banker focusing on the technology space and almost 8 years as an insurance agent working with middle-market tech and services companies. He has a strong understanding of the VC and PE community as well as financial statements and cash flow analysis. This experience has allowed him to transition to the risk management side by helping companies design proper risk management programs with a focus on management liability and cyber lines. Mike holds a Bachelor's degree in Finance from California State University – Chico.

In his spare time, Mike enjoys spending time with his family, fishing, and coaching his kids' tackle football and baseball teams.

SHANE GRONNIGER
CEO
GCS Technologies

Shane Gronniger is the Chief Executive Officer for GCS Technologies, a locally owned and operated managed cybersecurity and IT services provider. GCS manages cybersecurity for many well-known Austin brands across a wide variety of industries, including healthcare, finance, and other critical infrastructure sectors.

Shane has been consulting with small and mid-sized businesses in the Austin area for over 20 years and brings a wealth of knowledge and real-world experience to the table. He helps businesses better understand their cybersecurity posture and positions the right tools, people, and processes in front of them through the various services that GCS offers. He and the team at GCS have crafted a very successful and effective approach to managed cybersecurity and IT that is easy to understand and consume for most business owners. In 2025 the GCS team will celebrate their 25th year of serving the Austin area and surrounding markets.

RICH PEREZ
VP of Innovation
Texas Bankers Association

Rich Perez is the Vice President of Innovation at the Texas Bankers Association, where he leads the Community Bank Innovation Magnet program. With 15 years of experience, he specializes in delivering innovative digital solutions that drive profitability and growth. Rich works closely with community banks to implement cutting-edge technology, focusing on digital transformation, cybersecurity, and customer experience, ensuring they remain competitive in an evolving financial landscape.

SUMERA RIAZ
Sr. Director of Cybersecurity
Bluewave Technology Group

Sumera Riaz is a highly experienced cybersecurity professional with extensive experience in designing and managing cybersecurity strategies for large enterprises and global managed service providers like CapGemini. She holds a Master's degree in Applied Sciences and is a Certified Information Systems Security Professional (CISSP). As a former Chief Information Security Officer (CISO), Sumera has a solid track record of implementing robust cybersecurity controls and processes.

In her current role as Sr. Director of Cybersecurity at Bluewave Technology Group—an advisory and sourcing partner transforming how companies acquire and manage technology solutions—Sumera brings a wealth of expertise and a passion for making cybersecurity approachable and practical. Her leadership has been instrumental in developing and maturing security frameworks for critical infrastructures, including healthcare, finance, and oil and gas. Her efforts have resulted in resilient practices that stand strong in today's ever-evolving threat landscape.

Abby Mellott: From your perspective, what do you see as the biggest challenges that business leaders face today when it comes to cybersecurity?

SHANE GRONNIGER: Managing an ever-expanding workforce is still a challenge, despite the pandemic being four or five years in our rearview mirror. We're now squarely living in the new normal. Empty offices are everywhere, and we still see a lot of our clients hiring people in remote geographies or roles. So, from a cybersecurity perspective, managing the sprawl of people, devices and data is a big one.

People are also using so many different cloud services now, so that has become a real challenge as well for many security teams. It's become increasingly difficult to understand where everything sits, and how it's being governed. The challenge is further compounded by not having the right tools, or not having the right people or processes in place to manage those tools. We see a lot of businesses approaching this problem through a single pane of glass or solution, which can provide a false sense of security. As the saying goes, when all you have is a hammer, everything looks like a nail.

SUMERA RIAZ: I echo everything Shane just said. You don't know what you don't know. Lean IT and Security staff in companies are fire fighting everyday. They have very little time to research emerging threats. For business leaders, building out the right security posture for their organization within budget is a challenge. Leveraging companies such as Bluewave can be a real asset to help bridge these gaps.

MIKE DRAEKEN: Sumera and Shane articulated the issues perfectly. It's a lot easier to get insurance than it was three years ago, but it's a challenge for these companies who don't even have an IT group established. I'll just be honest–if you don't at least have multi-factor authentication (MFA) in place, you're

not going to get insurance.

RICH PEREZ: One thing I would add is that because of the industry we're serving, we've got a lot of bankers who are wearing a lot of different hats. You might have a COO or CTO that is also operating as a CIO or a CISO. Because we've got these banks that are running so lean–and naturally burdened with regulatory compliance issues–they end up relying heavily on third parties, so there's additional risk in their doing that as well, right? They must now take additional steps to ensure they aren't taking on additional risk with the absorption of a new supply chain.

Abby Mellott: Tell me about some of the more significant threats that you're seeing. What responsibilities do we have–as leaders in business–in terms of preparing for these events, or dealing with the aftermath of a breach?

SUMERA RIAZ: There's been a huge uptick in ransomware. I was reading an article by Sans Institute that ransomware attacks increased by 73% between 2022 and 2023. Internal vulnerabilities such as lack of patching and successful phishing attacks seem to be the resonating reasons. The responsibility we have as leaders is to ensure that we protect our customers and our employees. In preparing for potential attacks, I would strongly recommend security awareness and training for all employees, a bi-annually tested disaster recovery plan, an incident response plan, and cybersecurity insurance.

> "I'll just be honest–if you don't at least have multi-factor authentication (MFA) in place, you're not going to get insurance."
>
> **MIKE DRAEKEN**
> Watkins Insurance Group

MIKE DRAEKEN: Cyber deception is a real threat, too. The social engineering of cyber deception is sometimes very sophisticated, and that's where we're seeing a lot of claims from an insurance perspective. So employee training is very important–making sure people know what to look for so you can eliminate some of these threats from bad actors.

SHANE GRONNIGER: I would agree with Sumera–ransomware is definitely the most prevalent attack we're still seeing, and the most devastating as well from a productivity and financial perspective. Email phishing attacks are still the most common attack vector we see that lead to eventual ransomware incidents. Mostly because these are coupled with inadequately patched systems, a lack of multi-factor authentication, and many otherwise easily mitigated attack surfaces.

Today's threat actors are now capable of casting much wider nets due to innovations such as AI, which is enabling them to quickly comb through massive sets of data and launch more sophisticated and automated attacks. Staying one step ahead is becoming harder and harder, which is why AI will and must be at the forefront of our tools and approaches as well.

RICH PEREZ: Yes, identity spoofing is really prominent now. When somebody calls and says, "Hey, this is your bank president. You need to wire a million dollars to this routing number right now." What steps are we taking to make sure that we're safeguarding that? It's too easy now, with AI voice cloning and other deepfake tactics by bad actors.

SHANE GRONNIGER: Right! There's voice cloning, but also video. There was a pretty convincing case of that in the news recently. This is really scary stuff, and this is just the tip of the iceberg.

SUMERA RIAZ: Sixty percent of the companies that were ransomed from last year are not here today. It's sad and life-altering for so many people.

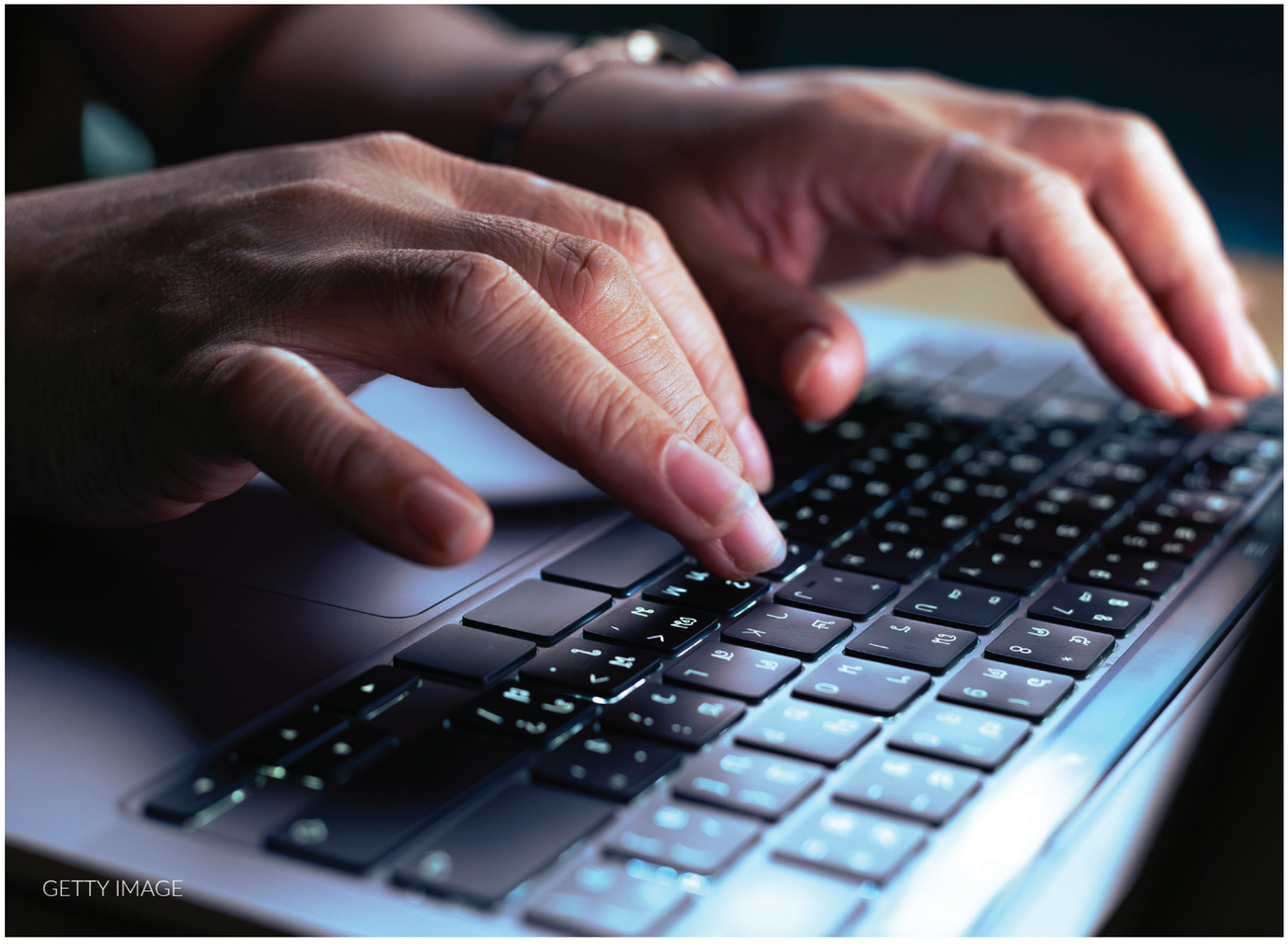
Abby Mellott: Clearly, we have a need for skilled professionals in this space. Can you guys talk a little bit about what it takes to build and maintain a strong cybersecurity team? How can we foster a security-conscious culture in the workplace?

SUMERA RIAZ: Honestly, it's nearly impossible to have an internal security team that's up to date on all the potential threats that are out there globally, and at the same time trained in emerging tech and security software. Companies should leverage MSSPs with a strong security bench to be an extension of their security team. Security is not a technology, it is a practice. A security-minded culture is a top-down approach and has to be driven by leadership.

SHANE GRONNIGER: I agree. There's definitely a lack of talent right now in the marketplace, and that's been going on for a long time. I think one challenge we're seeing is that a lot of the certifications and training programs are somewhat stale by the time they're mass-adopted. If you're building a team internally, we encourage willingness to train on the job, and at the same don't be afraid to outsource where it makes sense. There are many partners out there (like GCS) that will not only help you fill the immediate gaps but will help you build a team as well through a collaborative approach that helps your team learn and improve. We've worked ourselves out of a job several times by doing this but it always feels rewarding, and there's always another business at our doorstep needing the same kind of help.

Abby Mellott: Mike, is it a rarity to have cybersecurity as a coverage option at this point, or is it pretty widespread?

MIKE DRAEKEN: In a sense, cybersecurity is still in its infancy. In the late 90s, Pixar had AIG put up the first


GETTY IMAGE

policy. But a lot of companies won't buy cyber until someone tells them to buy cyber. In other words, if they're working with a large enterprise company, and the coverage is contractually required, they'll do it.

On the flip side of that, you have companies that just don't think they're vulnerable at all, right? So they don't think about it until an attack occurs–which is obviously not the ideal timing. We've talked about the risks already, and claims are on the rise right now. In the midst of the Russia-Ukraine conflict, we're seeing a lot more incidents. So it's not a matter of if an attack will occur, but when.

Abby Mellott: Rich, you guys are a membership organization. How are you able to support your community banks or regional banks that may not have internal resources?

RICH PEREZ: We have a few unique programs focused on supporting our members, like our innovation magnet. As you say, a lot of these businesses can't afford some of the top tier services that are available, so we aggregate those and provide best-in-class solutions in creative ways through our strategic partners that lower the cost of entry and provide managed services.

> "Today's threat actors are now capable of casting much wider nets due to innovations such as AI, which is enabling them to quickly comb through massive sets of data and launch more sophisticated and automated attacks."
>
> **SHANE GRONNIGER**
> GCS Technologies

Abby Mellott: Does anyone else have advice for companies who struggle with a limited budget for cybersecurity?

SUMERA RIAZ: Bluewave partners with our clients to design technology solutions that focus on goals and outcomes. We typically start an engagement with a Technology Portfolio Assessment, which is a cost analysis on spend for technology and security. On average, we identify 23% + savings buried in tech debt. If we can help find that money, it can be repurposed for security and transformational projects.

Abby Mellott: In light of the spike in cyber attacks this year, how do you help clients define the right security posture for their companies?

MIKE DRAEKEN: On the insurance front, there's not just one cyber policy. Each carrier has their own policy, and it does evolve. It depends on the market swings. Today, it's a soft marketplace, so you're going to see more favorable terms. It tends to be extremely broad. So it will cover phishing, network and security and business interruptions, generally speaking. That said, there are supplements you can add in. What a company needs will be specific to each entity.

SUMERA RIAZ: It starts with a company's risk appetite. When I speak to the leadership at various companies large and small, I ask them this question: "How many days can your company stay alive without generating revenue?" Every company has its own DNA, and the right posture for security is different for each company, as are regulatory and compliance requirements depending on the industry. The right security posture is defined by the level of risk a company is willing to take on.

SHANE GRONNIGER: Threat actors know where the bigger pots of gold tend to be, right? So they do absolutely go after those types of organizations. However, there's been a lot of money made off smaller companies, and those are the ones you don't read about every day. For every big story we read about in the news, there's are dozens more among smaller businesses. I will say, three or four years ago maybe two one out of five customers had cyber insurance. Now I'd say four out of five have it, and it's not just limited to regulated industries, it's just about everyone.

MIKE DRAEKEN: I had an incident where one of my client's vendors was hacked, and they sent an invoice saying, if you pay it early, we'll give you a 10% discount. It was over a million dollars.

My client did the right thing by doing a callback. The callback was AI generated, and because this vendor was in Taiwan, she had never heard that person's voice before. They got it all back, though!

RICH PEREZ: That's crazy. Shane is right. We tend to focus all of our attention on big news stories about these mega breaches, right? But we've got nearly 400 banks in our membership, and many of them are being compromised. Because it's 10s of 1000s of dollars instead of millions, the FBI is not going to spend time to assist in aiding "small" breaches.

We use the power of our community to ask important questions and make sure people are feeling heard, especially when they are not necessarily being seen. We ask them, "Who else has gone through something like this? Did you find any help?" That's where we've seen some level of success–being a sounding board for our industry and their concerns, which are very real.

> "Cybersecurity is expensive. Most of the time, companies find savings buried in tech debt. A technology portfolio rationalization can help find that money and it can be repurposed for security."
>
> **SUMERA RIAZ**
> Bluewave Technology Group

Abby Mellott: What about training? What are you guys doing to make sure your staff and clients are alert and prepared for cybersecurity risks that may be on the horizon?

SHANE GRONNIGER: Specifically, when talking to our clients, pay attention to the news, your team, and your security vendors. Get more involved. You don't need to get certified or become a cybersecurity expert, but the more you know the more informed decisions you can make. Our approach is high touch, and we very much encourage stakeholder involvement. There's no point in turning on all of these tools if we don't have the right people looking at them on a regular basis. A key component of our managed cybersecurity service is engagement. We're not just a monthly report that you receive in your inbox, or a customer portal with lots of bells and whistles. While we do have those things, we require real engagement to be as effective as we can be. For many this is a monthly or quarterly security meeting with key stakeholders. For others it's a more frequent cadence. The level of engagement can vary based on risk profiles and appetites, but the more we can stay engaged the better. Achieving and maintaining a good cybersecurity posture requires more than just a report, a portal, the tools, or even the training. It requires ongoing conversation and collaboration with the right people. It takes a village!

We may say "Hey, we've got 20 machines out there that are vulnerable and at risk, which could lead to a breach. So we spend time with that client every day, every week, every month. With other clients, we have a weekly security meeting. Those are for the very big clients that have a lot of moving parts.

The level of engagement depends on client need. But the more we can stay engaged, the better. We want key stakeholders to understand that while they need not become cybersecurity experts, the more that they know how everything works, the more informed decisions they can make in times of crisis.

RICH PEREZ: We have standing webinars, meetings, and huddles. But I think on this topic, one of the most impactful tools we offer is access to our TBA ISAO–this is a benefit for our fee-paying members. We're pulling in feeds from Splunk and IACI into a managed Slack instance, and that gives everyone another layer of threat awareness. Our members appreciate having the ability to collaborate in real-time, as they assess any imminent threats that may arise there. We have over 500 active members who are using that tool, and we are seeing new registrations every week.

Abby Mellott: Is there anything pertaining to cybersecurity that business leaders should be aware of as we look forward to the next legislative session in Texas?

SUMERA RIAZ: North Carolina and Florida are currently the only two states in the U.S. that prohibit state agencies and local government entities from making a ransom payment or communicating with a threat actor following a ransomware attack. It would be interesting to see if other states including TX follow suit. It is a great topic for debate because you can see both sides of it.

SHANE GRONNIGER: Paying the ransom has always been a gray area for us. On one hand we're supporting the terrorists, on the other hand we're trying to keep our customers alive. For example, we support many healthcare organizations and downtime can often lead to patients not receiving the critical care they might need. We still manage these types of incidents on a case by case basis, often with the help of the FBI, cyber insurance providers, and other legal counsel. Sometimes this does involve paying a ransom, but we often avoid it by having the right systems in place. In terms of legislation, we're always keeping a close eye on this.

Texas has definitely increased it's data privacy and protection legislation over the last decade or more but up until now it's mostly been focused on consumer protection and government related entities. Regulated industries aside, most private businesses in Texas are not bound by compliance or legislation when it comes to cybersecurity. The requirements around reporting a breach are ambiguous and difficult to enforce. Best-practices frameworks are out there but they are hard to understand and adopt for most. Even those that are regulated are using antiquated standards and point-in-time audits that produce a false sense of security. We see a storm brewing on the horizon and in preparation for this we're already starting to help our regulated and non-regulated clients take a more continuous approach to managing compliance, whether it be with a specific industry regime or simply their cyber insurance policy agreement. Demonstrating close alignment to a best-practices framework, required or not by law, only helps us stay prepared for any potential legislation on the horizon.

GETTY IMAGE

> "We use the power of our community to seek information and make sure our bankers are feeling heard, especially when they are not necessarily being seen."
>
> **RICH PEREZ**
> Texas Bankers Association

RICH PEREZ: It was interesting to me that IBM did a study and determined that, last year alone, 23% of all cybercriminal activity was in the financial services industry. Seeing that number behind it was pretty insane. It's gone up from 7% in 2022 to 23% last year. So that's huge. As we all know, it's not just the banks and credit unions. It's also all the Fintech folks in the middle who have access to the information. So there again, the question is–are they taking the right steps and working with the right people in order to mitigate their risk? That's the essential question.