



TABLE OF EXPERTS

Cybersecurity

PHOTO BY MICHAEL THOMAS

Left to right: Jason Gotway, Anders Technology; Hannah Ji-Otto, Quarles; Todd Chollet, Laken Insurance.

Cyberattacks have become an exception in modern business. Yet many businesses still rely on outdated protections that leave them vulnerable. Are antivirus software and firewalls enough? How can companies prove that cybersecurity investments are actually reducing risk? And what happens when AI becomes both the weapon and the defense?

Three St. Louis experts recently joined the Business Journal's Table of Experts to discuss how mid-market companies can strengthen their defenses, from building real incident-response plans to tightening vendor oversight and updating their cyber insurance to fit the fast-moving nature of today's threats.

Robert Bobroff, publisher of the St. Louis Business Journal, moderated the discussion with:

- Jason Gotway, Partner and Technology Practice Leader, Anders Technology
- Hannah Ji-Otto, Partner, Quarles & Brady LLP
- Todd Chollet, CIC, CLCS, Senior Risk Advisor, Laken Insurance

ROBERT BOBROFF: Jason, what are the biggest blind spots companies face when relying on traditional IT security?

JASON GOTWAY: The keyword there is "traditional." It's a false sense

of security if you're using traditional methodologies, like antivirus and two-factor authentication on email and having a firewall.

But historically speaking, people feel like if you have those things, you've done enough. And that's just not true anymore — we have to go with a more modern approach.

Yes, you still have to have your antivirus and two-factor authentication. You have to have a firewall. But there are new things, like zero trust, protecting identities, and authentication.

These are a few of the things that prevent adoption — people ask, "Do I really need to have a security professional

monitoring all of my alerts 24 hours a day?" The answer is yes.

You know, it's not just your email anymore. It's not just your computer anymore. It's across the board. Anywhere an attacker finds value, those are the areas where we have to have security monitoring continually.

Blind spots turn into overconfidence — and my friends not in IT remind me that there's no shortage of overconfidence in technology. But I think a way to combat those blind spots is to join peer groups where you're finding out what other people are doing and staying up to date.

HANNAH JI-OTTO: I think traditional IT security will lead to a false sense of

THE EXPERTS

**HANNAH JI-OTTO**

Partner
Quarles

L. Hannah Ji-Otto is a partner at Quarles & Brady LLP. She advises clients on data privacy, technology transactions, and the use of emerging technologies, including AI. She guides companies through information governance and data breach response, with expertise in ransomware and BEC.

Hannah serves on the board of the International Women's Cyber Alliance and holds multiple privacy certifications, including CIPP/US/E/C/A, CIPM and FIP.

Quarles

**JASON GOTWAY**

Partner and Technology Practice Leader
Anders Technology

Jason is a Partner and Technology Practice Leader with more than 15 years at Anders guiding organizations in strengthening their technology and cybersecurity strategy. He is known for identifying modern methods to defend against evolving cyber threats and regularly speaks to

educate leaders on practical protection. Since joining Anders in 2011, he has continued advancing his expertise through VMware and Veeam certifications and holds a B.S. in Computer Management and Information Systems from Southern Illinois University Edwardsville.

anders

**TODD CHOLLET, CIC, CLCS**

Senior Risk Advisor
Laken Insurance

Todd Chollet is a Senior Risk Advisor at Lakenan. He guides business leaders on insurance and risk management with expertise in cyber and professional liability. Todd is also on Sunstar Insurance Group's Transactional Advisory team where he consults on the

insurance complexities of mergers and acquisitions. He holds CLCS and CIC designations.

Lakenan
INSURANCE • BENEFITS • RISK MANAGEMENT



PHOTO BY MICHAEL THOMAS

security and overconfidence. It's good at guarding the "front door," but it often misses what happens inside the house: insider activity, cloud and SaaS settings, and weaknesses in vendors and partners. Regulators increasingly expect companies to see and manage these risks. As a privacy counsel, I often see basics being overlooked: companies don't know where their data are. They have ad hoc vendor review systems and incident-response playbooks that never got tested over the years. Those gaps turn a technical issue into a legal one.

BOBROFF: Hannah, why is robust data governance increasingly critical in today's business landscape?

At the core, data governance is the operating system for a company's data and technology. You want to have clear rules, policies and processes for what you collect, how the data is classified, who can use or share it, and when it is retained or deleted. It matters significantly because regulators and consumers now expect data to be handled in a secure way, and cybersecurity and privacy issues are more likely to be a board-level issue. The complicating factor to establish a good data governance system is that your data now increasingly lives across different software, apps and vendors and AI tools.

That's the business landscape, and in the legal environment, there's now

a patchwork of international and domestic data privacy and cybersecurity frameworks, which has made compliance really difficult for businesses. When things go wrong, as we see a lot during breach response scenarios, costs can add up quickly. You're dealing with everything from forensic work and notification to regulatory scrutiny and class-action exposure, not to mention reputational damages.

Practically, data governance means knowing your people, data and vendors. That would mean assigning accountable owners, inventory your data, only keep the data you actually need and manage your vendors. Then, we want to set simple, enforceable rules for access, retention, deletion, cross-border transfers and breach cooperation. Most importantly, we want to pressure-test them with tabletop exercises.

If we do it well, data governance lowers regulatory and litigation risk, reduces the cost of compliance, strengthens customer trust, improves data quality, shortens sales cycles and turns incident response from a scramble into a timely evidence-based process.

TODD CHOLLET: I think about a couple of things you mentioned when it comes to insurance claims. What often drives claim costs higher is this misunderstanding of what data you have

and where the data is. Why are you saving data that's unnecessary or ancient? Could you mitigate the cost by just purging it? From a claim severity standpoint of understanding what you have and where it is, those management tools can mitigate the cost of a claim.

BOBROFF: Todd, can you talk a little bit about cyber insurance variations, standalone coverage vs. sub-limits, endorsements and exclusions?

CHOLLET: There's a lot of misunderstanding about what cyber insurance is. The smaller the organization gets, the more misunderstandings there are about cyber insurance. We still talk to people on a regular basis who say they have cyber insurance, and find it's an endorsement on a policy that covers maybe \$50,000 worth of data breach costs. That's not going to get you very far in a claim.

So, I think there's still just this misunderstanding of what cyber is, and cyber isn't a prepackaged one-size-fits-all thing. It really needs to be tailored to fit what the organization needs. And that could take a lot of different forms — even if you carry a standalone cyber policy, there are sub-limits, exclusions and endorsements that can be added on or removed. You can manipulate the policy to respond how the organization wants. It's important to realize that there's no right or wrong coverage; it's what the organization is comfortable with and whether it will respond as they expect in the event of a claim.

One of the hot issues right now is dependent business interruption. If a vendor or an IT provider of yours goes down because of a cyber-breach or system failure, is your business set up to withstand that type of impact? Is your cyber policy structured to respond to those risks? You really have to understand the nuances of a policy.

GOTWAY: That's why when we're first introduced to organizations, one of our questions is, "Do you have cyber insurance?" We know what a big deal it is, because the odds aren't in your favor if you don't have it. In these situations, we ask that clients have a good relationship and an ongoing conversation with their insurance broker, because a lot of them

just treat it as "yes" or "no." There's so much more to it after the fact.

CHOLLET: And it's a constantly evolving situation. Cyber-insurance is a pretty young insurance product, relatively speaking. In the past five years, policy forms have evolved quite a bit, and there has been more consistency from carrier to carrier, but there's still a lot of proprietary language and variations out there.

JI-OTTO: And like you said earlier, \$50,000 really doesn't go very far when it comes to covering all the costs of a data breach. As a privacy counsel, I've seen the costs for responding and mitigating a single breach may include engaging forensic firms to come in and take a look at what happened, notifying individuals and regulators according to state breach response laws and providing credit monitoring to affected individuals. If it's a ransomware breach, we also engage ransomware negotiators and consider whether a ransom payment is necessary. On top of that, you often need PR specialists to help craft clear communications for employees, customers, partners, or the general public.

And that's not the end of the story. After the breach, companies often face a whole new wave of problems. We see companies that were breach victims getting sued after the breach including class action lawsuits, which can be really expensive. We've seen state attorneys general step in to investigate and demand answers for consumers. So, when you consider all these risks and potential expenses, it really makes sense for companies to weigh them carefully against the cost of maintaining robust cyber insurance coverage.

CHOLLET: The tools to identify what limits are necessary have gotten better, too. I think historically, there was a lot of guesstimating based on the cost per individual record. Now, there's more claim data to base it on, and there are modeling tools that can give organizations a better idea of what limits they should carry.

BOBROFF: Jason, how is AI changing both the threat landscape and defensive strategies? Further, how is AI leveraged by attackers, and how can you utilize AI to stop attackers?

GOTWAY: Whenever we're talking about how AI is impacting organizations, we say that from the highest level, you're being scanned all the time. No matter if you have a very good security posture or not, you're being scanned all the time. Then, if a weak spot is identified, it may gain further attention from an attacker, again potentially using AI to accelerate the process. Go down another level, and someone will evaluate how easily your vulnerabilities can be exploited and the how valuable you are as a target.

AI is increasingly used after those scans to help attackers interpret what software or versions you're running and whether known vulnerabilities apply. If something looks exploitable, AI can help an attacker analyze possible attack paths faster. That's how I want organizations to think — not to make them paranoid, but to be matter-of-fact that this is happening. As it relates to your own scans, periodic penetration tests aren't enough anymore. This initiative has to be a constant scan, just like you're being scanned by automated systems. That's the way I feel AI is working against us.

Now, how we can stop it is by looking at vendors. Every organization has a ton of vendors. I'm zeroing in on the ones doing cyber, and I'm asking those vendors, "What AI are you baking into your software to make my life easier and make us more secure?" A lot of times, they can give you very specific answers. So, it's important to focus on selecting vendors that are doing that work for you and leveraging AI. Ultimately, AI defense functions provided by vendors may identify and review issues faster than what would formerly have been performed by a human security team.

CHOLLET: I think the barrier to entry for these attackers is so low now. In the past, you may have had to be this wizard who knew how to move around, but nowadays, you just have to buy a ransomware-as-a-service application and you're armed with the tools you need to exploit any business you want. That's the scary thought for me.

GOTWAY: Yeah, and then there are very simplistic ways — you know, we used to be able to spot a fake email by



FINDING NEW WAYS FOR YOUR BUSINESS TO THRIVE

As a team uniquely composed of CPAs, financial thinkers and specialists across many industries, we have the specific expertise to engineer a plan to match your ambitions.

 **CALL US** (314) 655-5500

 **VISIT US** anderscpa.com



misspelled words, bad grammar, and all. Now, an attacker can throw it in ChatGPT and ask for an email in the perfect dialect for the right area.

JI-OTTO: Speaking of that, a few years ago, I learned threat actor groups were aware that their English was a problem when it came to making their phishing emails look legitimate, so they hired more English speakers to improve their customer service. Now with AI tools, they can polish up their emails so much more effectively.

BOBROFF: Hannah, as artificial intelligence becomes more deeply embedded in business operations, which governance models are proving most successful in balancing innovation with regulatory compliance?

JI-OTTO: In today's rapidly evolving regulatory environment, organizations need to adopt an agile AI governance framework to remain both innovative and compliant. From a legal perspective, the federal government has not enacted a comprehensive AI regulation and is taking a lighter-touch approach, but individual states, including California, Colorado, Utah and Texas, have implemented their own AI statutes. On the international level, the European Union has a very comprehensive framework governing AI and data use. China also has a targeted requirement for AI implementation and deployment.

In this shifting regulatory landscape, businesses that want to remain compliant need to have AI governance that's broad enough to cover the fundamental requirements across different jurisdictions, yet flexible enough to adapt to changing regulations. I think the most effective governance models need to balance speed and compliance through clear, risk-tiered controls and defined ownership. A cross-functional team is also essential, as it is important involve legal, IT security, privacy, and business representatives establishing an enterprise's standards. Then you want to have embedded AI product owners responsible for applying those standards across different use cases based on assessed risks.

I think one practical takeaway for



PHOTO BY MICHAEL THOMAS

AI adoption is the importance of vendor diligence, like Jason touched on previously. Vendor diligence includes managing intellectual property risks, data rights, and IT security. A well-defined AI use policy clarifies organizational expectations and boundaries.

BOBROFF: Todd, talk to us about cybercrime, specifically the fraudulent transfer of money.

CHOLLET: This is the most frequent claim happening right now. Ransomware makes the headlines, but fraudulent transfer of money — whether it's through social engineering where you have somebody in the organization that listens to an instruction from a third party and transfers the money themselves, or you have a threat actor that's acquired credentials to log into a bank and transfer the money — it's just happening very frequently. So, putting policies and procedures in place to combat that is important. One of the simplest things you can do is just pick up the phone and call wherever that money's going. Have a predefined number to call and ask, "Hey, did you send me an email and ask for this money?" Don't use the same form of

communication that was used to request the money.

There are other things you can do — working with someone like Jason to make sure your technical protections are up to date and making sure you have a good partnership with your banker. Don't count on your bank to fix everything, but you should work them to familiarize yourself with their fraud protection tools.

GOTWAY: I see attacks all the time. Whenever you see one, you think, "I wonder if the companies that handle my data are thinking about cybersecurity like I do."

The last couple of attacks that I saw involved token theft, where somebody clicks on something they shouldn't and an attacker gets access to a token. I don't know how many people know about that yet. It's a part beyond passwords and two-factor authentication that people need to know about to protect themselves and their organization.

CHOLLET: Yeah, certainly none of these are going to prevent 100% of cybercrime. I think that'll be a never-ending battle.

That's on the front end — preventing it — but you also want to make sure your policy responds to these sorts of scenarios on the back end.

Most policies will have a sub-limit — even if you buy a million dollar policy — on the transfer of monies to \$100,000 or a quarter million. And a lot of these transfer claims are for \$500,000 or \$600,000. In industries like real estate and construction, it's not unusual to be wiring half a million dollars to a vendor. Now there are options to build up towers in excess of the sub-limits to add more layers of protection. It goes back to understanding your policy.

JI-OTTO: If a business has already wired \$1 million to a threat actor, the legal counsel is often asked, "How can we get this money back?" Unfortunately, the chances of recovering those funds are extremely low. Many threat-actor groups operate outside the United States, making it very difficult to trace the money and bring these groups into the U.S. court system.

BOBROFF: Hannah, what trends are we seeing in cyber-incidents and the costs

associated with mitigating those risks?

Jl-OTTO: Lately, we're seeing that threat actors are increasingly using AI to carry out their schemes and attacks. IBM's current Cost of a Data Breach report for 2025 which came out this summer, reported that one in six organizations experienced breaches linked to AI-driven attacks, and the most common types of AI-enabled techniques include phishing and deepfake impersonations. Shadow AI was also involved in 20% of data breaches. I also learned from my forensic friends that some of the threat-actor groups have started using AI chatbots to take ransomware payments. It's ironic that their business is doing so well that they need to implement an AI chatbot to manage ransom payment.

The costs associated with these risks are substantial. There are direct costs, including containing the breach, but then there are the costs of forensics, notifying individuals and regulators, credit monitoring, and PR. Downtime is also a major factor, along with system restoration. According to the same IBM report, the average breach cost for United States organizations hit a record high of \$10.22 million.

GOTWAY: If you're sitting in the room during an incident response, there may be a couple of attorneys, there's the response team, the IT people, the breach coach and the insurance people. You can just feel the meter running, so it's no surprise how much it adds up.

CHOLLET: That's why understanding the data you have and doing the tabletop exercises and the incident response planning can make such a difference in the claim cost. And having somebody in the business who will be able to make decisions and not have to leave the room and take that information to a decision maker, then come back — that's a lot of wasted effort.

Jl-OTTO: Exactly. Some companies don't have a process in place beforehand. So during the breach, they have to scramble and figure out whom to call. Sometimes, if it's a ransom breach, all the systems are down, so it's not easy to get in touch with leadership. That's why it's really important to make those decisions ahead of time.

CHOLLET: I think that idea is really hard for people to grasp, that I'll show up in my office and won't be able to do anything. So, even when you present the idea, they'll say, "Oh, I'll just go get another computer and start fresh." But that doesn't take into consideration all of the simple steps of what would have to be done. Even your phone numbers are integrated in technology. Nobody remembers phone numbers anymore. So, when you're in a panic in an emergency situation, having simple things planned out can make a big difference.

BOBROFF: Jason, what does real incident response readiness look like for mid-market companies?

GOTWAY: There are mid-market companies that are very underprepared, and then ones that have done the tabletop exercises and are able to continue, not panic, because they've adequately prepared. Organizations that are ready have well-documented incident-response plans — and not something straight off of a website. It's one that you've read and understood and tailored to how it applies to you. Essentially, you've customized your readiness plan to how you react. Every business is different. They store their data in different ways. But having that incident response plan ready to use is very important, and you don't want to be in a spot where you're learning things about your environment in the middle of a situation. You don't want any arguments about what gets restored first to get business operations back to normal.

The thing I probably hear the most is, "I just want things to go back to normal as fast as possible." And, for that to happen, you have to be ready for these incidents to occur, with an order of operations for figuring out what's most valuable to be restored. Whenever you have all of that in place, then you're set up for success post-incident.

Jl-OTTO: From a legal perspective, companies are required by state laws to notify individuals and regulators if personal data is involved in a breach. Mid-market companies face the same notification clock as big companies do, even though they have a leaner team to handle all of that. So, it's even more important that critical decisions about

how to respond to the incident are made in advance, so the company doesn't go into panic mode.

GOTWAY: Yeah, your incident response plan and then tabletop exercises to test that. Anytime you have a big change within your organization that may have an impact on your documents, those tabletop exercises are important. Beyond that, in my opinion, you should conduct them quarterly. Monthly may be slightly unrealistic. The goal should be that you are familiar with the plan, and you're not dusting it off whenever you have an incident.

BOBROFF: Todd, talk to us a little bit about best practices for cyber-controls.

CHOLLET: I think we've come a long way in the past five years. There was really a big shake-up and wake-up among all organizations post-COVID. As more people worked remotely, that came at a time when cyber incidents were growing, and that really exposed a lot of businesses. After that, insurance companies responded by telling these

companies they needed to start taking it seriously and putting protections in place. Before that, a lot of companies were just checking a box, buying cyber-insurance, and that was their incident-response plan.

Businesses have come a long way toward putting controls in place. Large organizations are doing it more than smaller ones. But even then, we still hear about attacks on a regular basis where simple things like multi-factor authentication and data segmentation aren't in place. And if they're not in place, you're not as well protected on the front end and not as prepared to mitigate claim costs on the back end.

GOTWAY: Yeah, when the attestation document comes out and the first four things — MFA for email, MFA for VPN, MFA for your cloud, all the way down the line — that's these controls. Traditionally, you might think if you've got it on your email, you're covered. But you forgot about all these other things. That's why the attestation document is a huge deal.

Jl-OTTO: We're noticing a trend

Lakenan
INSURANCE · BENEFITS · RISK MANAGEMENT

Professionally Serving Your
Businesses and Families Since 1938

**Knowledge.
Action.
Results.**

SCAN ME

(314) 721-1500 info@lakenan.com

1 N. Brentwood Blvd. Suite 700 | Clayton, MO 63105

with SaaS vendors in the last few years. More and more customers are building cyber-insurance requirements right into their contracts. Instead of leaving it vague, these agreements often spell out exactly how much coverage a vendor needs to carry. It's becoming less of a "nice to have" and more of a standard expectation in the relationship.

CHOLLET: Yeah, that's become a bigger issue in the past two years with the breach with Change Healthcare and how many businesses that affected downstream and with CrowdStrike last year and how many businesses that affected. So, there's been more focus on paying attention to your vendors and their cyber-posture, and what policies and insurance they have in place. When our clients get presented with those agreements, we always tell them to check with their broker and make sure that what they're being asked is appropriate or even attainable. Looking at the cost of the insurance and the value of the contract — do they match up? We've had situations where we've had small businesses being asked to carry \$10 million in cyber

insurance. The cost of that policy is going to outweigh the revenue they receive from the contract.

BOBROFF: Hannah, what roles does cyber due diligence play during mergers and acquisitions?

JI-OTTO: Cyber due diligence is now a core part of M&A, because so many deals are data driven. You're not just buying the technology or the company, you're also buying the data, the data rights and the security practices that protect the data. That means it's really important to evaluate the privacy posture, and the data inventory, third-party dependencies, and how the target company manages access, backups and incident response.

An important way to appropriately allocate the risks is through the transaction documents. As the buyer, you want the representations and warranties in the Asset Purchase Agreement/Equity Purchase Agreement to cover compliance with privacy and cybersecurity laws, accuracy of disclosures, incident history, security controls, and vendor

oversight. Add practical covenants and a post-close remediation plan, and use targeted indemnities with sensible caps to backstop known issues. For higher-risk profiles, consider reps and warranties insurance with cyber-specific endorsements. The goal is to make clear who owns which risks so the business you buy is the business you get.

GOTWAY: A lot of times, too, there may be no history of a cyber incident, but you can tell that the environment is in really bad health, either from a performance perspective or cybersecurity, and you don't want an incident on day one. So, I do like having the appropriate people doing due diligence and having a plan together for a merger or acquisition to avoid introducing unnecessary risk. That way you can immediately say, "These are the changes we need you to make beforehand, or these are the changes we're going to make right afterward, so we're not putting the businesses at risk."

Typically, in any M&A transaction, one business of the two (or more) will be healthier than the other from a cybersecurity perspective. In many cases, it's the company getting acquired that's not as healthy. It may take a lot of money to bring another organization up to speed, which could change the value of the deal.

CHOLLET: The statistic that comes out every year in that IBM report is that it takes, I think, seven to nine months before an attack is even discovered in the system. So, it would not be great to make a purchase and then find out post-close that there's an ongoing attack.

BOBROFF: Jason, talk to us about how leaders can validate that their cybersecurity spend is actually reducing the risk.

GOTWAY: If you implement a cybersecurity strategy or a plan, and you start seeing fewer attempted attacks or less logging happening, where there's just less of a footprint evident, you know you're moving in the right direction. I kind of relate it back to about 10 years ago, everybody was starting to have a decent firewall with a little extra functionality. And then, when firewalls got bigger processors, you could do geographic IP blocking where you just block attacks

coming from abroad. Once that became an option, there was less activity in the logs. So, once you start shrinking that footprint, that's something I like to share. Those are the easy ways to quantify that there are fewer attempted attacks occurring, ultimately contributing to reducing your risk.

CHOLLET: I like it when clients tell us what they've been doing. Be forthcoming with your improvements, not necessarily the quantity of money you've spent, but what enhancements you've made, so that your broker can communicate that to the market and make sure you're getting the best pricing and the best terms and conditions that are available.

GOTWAY: And there are definitive, nice-to-haves that you can tell everybody you're buying. But then there are the absolute must-haves that I think insurance will be very interested in. I always get a little concerned by some of the products people are buying, thinking they're doing a good job, but there may be areas that may have a higher priority. Nothing's bulletproof, but you're improving by focusing on the must-haves.

JI-OTTO: Traditionally, I saw companies that put graphics on slides showing how year after year, spending was going down, and the spend corresponding to incidents was also decreasing. They thought this demonstrated that they were reducing risks. However, this has changed. Last year, as Todd mentioned earlier, we saw how large-scale incidents such as the Change Healthcare breach and CrowdStrike outage that affected hundreds of millions of people, triggered cascading effects across multiple industries, and led to jaw-dropping financial losses. The traditional method is no longer an accurate way to measure risks.

Benchmarking is very important. For instance, over the past couple of years, health care companies have consistently ranked number one for the highest average cost of mitigating a breach involving personal health information, with financial service companies coming in second. So, if you are a health care company, it makes sense to invest more in risk mitigation. We represent different companies across different industries, and can help you benchmark and serve as a sounding board.

When the stakes are high, you need a legal team trained for excellence.

Quarles attorneys rise to meet your challenge from a culture of high performance. We bring razor focus to each task with the right balance of skill and finesse.

With 13 offices nationwide, our diverse team is well positioned to serve clients in varied industries wherever your business leads.

8235 Forsyth Boulevard 10th Floor
Clayton, Missouri 63105

Quarles
quarles.com