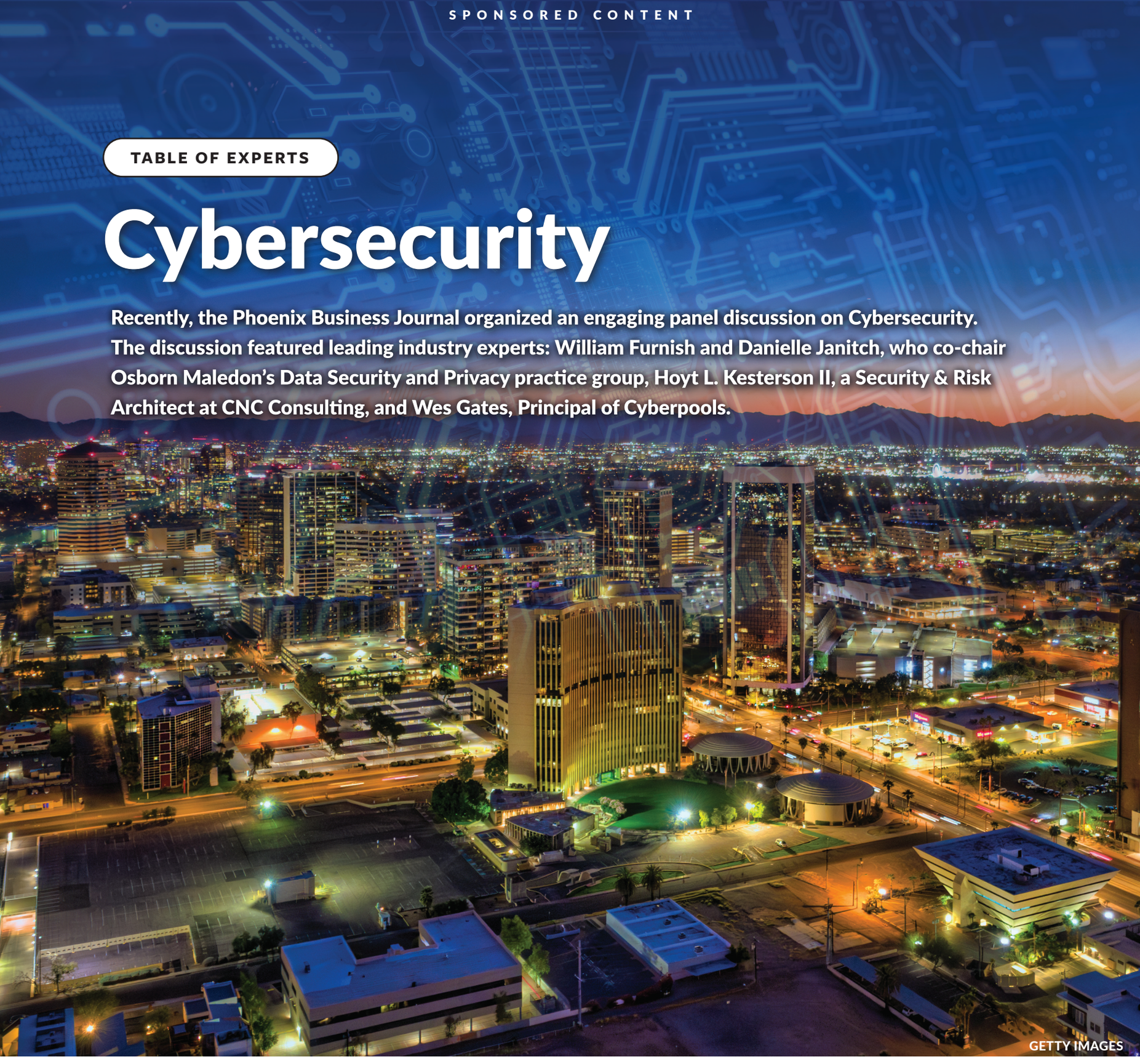
TABLE OF EXPERTS

Cybersecurity

Recently, the Phoenix Business Journal organized an engaging panel discussion on Cybersecurity. The discussion featured leading industry experts: William Furnish and Danielle Janitch, who co-chair Osborn Maledon's Data Security and Privacy practice group, Hoyt L. Kesterson II, a Security & Risk Architect at CNC Consulting, and Wes Gates, Principal of Cyberpools.



GETTY IMAGES

SPONSORED BY:

OSBORN MALEDON
ATTORNEYS AT LAW

MEET THE EXPERTS:

HOYT L. KESTERSON II
Security & Risk Architect
CNC Consulting

Hoyt L. Kesterson II is a Security & Risk Architect with CNC Consulting in Phoenix, Arizona. He has more than 40 years of experience in information security and related technologies. For 21 years he chaired the international standards group that created the X.509 digital signature certificate. He is a founding member and co-chair of the Information Security Committee in the American Bar Association. He is a testifying expert. He holds the CISSP and CISA certifications. He has three articles published in The SciTech Lawyer—What's Quantum Computing Got to Do with It? in the Spring 2022 issue; Cryptocurrency: A Need for Integrity in the Summer 2023 issue; and The Synergy of SciTech and the RSA Conference, co-authored with Ruth Hill Bro, in the Fall 2024 issue.

WILLIAM FURNISH
Partner and Co-chair,
Data Security and Privacy practice group
Osborn Maledon

William Furnish is a partner and co-chair of Osborn Maledon's Data Security and Privacy practice group. A recognized thought-leader in cybersecurity and data privacy, he regularly advises businesses, educational institutions, and professionals across diverse industries. William holds CIPP/US certification from the International Association of Privacy Professionals and is a frequent presenter on law and technology topics.

DANIELLE JANITCH
Partner and Co-chair,
Data Security and Privacy practice group
Osborn Maledon

Danielle Janitch helps Arizona businesses grow by managing their day-to-day legal needs, focusing on cybersecurity, data privacy, and intellectual property. She serves as general counsel to large and mid-sized companies, offering legal solutions for licensing, data protection, distribution, trademark prosecution, and more. Danielle also advises businesses on launching new products and services, including contract negotiations and market testing, while providing training for IT teams when needed.

Before joining Osborn Maledon, Danielle clerked for Judge Roslyn O. Silver of the U.S. District Court, District of Arizona. She holds a J.D. from Stanford Law School and a B.S. in Chemistry and Biology from MIT. Danielle is a U.S. Army veteran.

WES GATES
Principal
CyberPools

Wes Gates is the principal of CyberPools (dba Gates Consulting), which has been providing IT services to clients for over 25 years. His firm contracts with educational institutions to provide cybersecurity services to school districts, including developing the cybersecurity services offered to educational institutions and spearheading cyber claims/cyber incident response efforts.

Wes has over 35 years of IT experience, with 21 of those years working with educational institutions. He has worked in various roles, including chief information officer, developer, chief information security officer (CISO), and network engineer. Wes has a full stack of development skills, network administration, and cybersecurity training.

GETTY IMAGES

Wes: Let's kick things off. Hoyt, we'll start with you. What is third-party risk? And why should I care?

Hoyt: I think third-party risk should be looked at two different ways. One of them is what we call supply chain in which companies use other companies to provide software. The other type of third party is when you offload some functions for your company to a third party. The Target data breach where they were infiltrated through HVAC controls is an example of this.

You will have to grant access to third parties. The question is how good of a job are you doing controlling that access? You must realize that if you let them into your system, you have to be really careful about what their own security controls are.

Wes: Agree, third-party audits are increasingly important as organizations continue to outsource services and business functions. And then the other part of that is if you delegate your data to a vendor and they're the custodians of your data, then you have another set of controls to consider.

William: A business may be able to "push down" contract terms on third parties and obtain indemnification. But if you're not performing audits or if you're not taking steps to verify that those third parties are performing the way they are supposed to, that indemnification may be of limited value.

Hoyt: I think of contracts as essentially alleviating damage. It's almost like insurance because if the third party doesn't do what they're supposed to do, then we have things we can fall back on; we can sue you. Well, that's nice, but that's not protection, right?

Hoyt L. Kesterson II SUBMITTED PHOTO

"We've been building systems to help businesses protect themselves because we realize as a nation our businesses are our strength. It bothers me to see these systems shut down without evaluating first what they contribute."

HOYT L. KESTERSON II
CNC Consulting

William: The key takeaway is that you cannot assume the level of sophistication and safeguarding being done by third parties you allow into your systems. You can have all the indemnification in the world, but if that third party is not financially solvent or around to actually indemnify you for a mistake they have made, then you have little protection. My colleague Danielle Janitch knows a lot about clauses that can assist with managing third-party risk.

Danielle: Most companies are aware of the need to include a basic security clause that obligates the vendor to implement appropriate and reasonable administrative, technical, and physical security measures that conform with then-current prevailing industry best practices, as well as provide notification in the event of any security breach.

Beyond this basic clause, asking for the right to terminate early in the event of a breach is always worth asking. Additionally, given the rise of AI use by vendors, consider asking for restrictions or controls around the use of AI and how it uses your data.

Wes: Okay. All right. If we can, we'll move on to the next question. Why are K-12 and higher ed targets of threat actors?

William: There are several reasons. One we have already discussed—K-12 and higher education are using a lot of third-party vendors to provide services to them. They also, because they're both employers and hosts of student information, potentially have some very, very high value, information on hand.

Wes: Yes, they have a lot of PII (personally identifiable information) and often other types of sensitive information.

Hoyt: You guys are discussing the goals of security. You know, a lot of people focus on confidentiality and integrity. The one they don't pay enough attention to is availability. I think that school systems are great targets, not just because of the information held, but because cities and municipalities have a lot invested in delivering education to their citizens. This denying of that ability is, to me, is a classic example of what ransom is.

Wes: On that point, children's PII can be monetized for an extended period of time, because until they turn 18, nobody has a reason to look at credit. So, I would agree with you, it may not be primary, but there is an incentive to capture this information. We have started to see in the breach notices that parents are informed on how to freeze their kids' credit, which is helpful information.

We've already talked around this a bit, but why does a business need cyber insurance?

William: Because the costs of a data breach or a cyber incident are far reaching and extremely expensive for businesses. It impacts things that folks might not even think about, like hardware, investigation costs, business interruption, everything that you would need to try to make your business whole after an event. It can also impact how attractive a business is for investment purposes.

Wes: So, it's not a matter of if you're going to get hit by a cyberattack, but when. And then the question is, are you prepared to respond to a cyberattack? Do you feel prepared to handle a breach without insurance, without vetted vendors? Do you know who you're going to call? It's not the Ghostbusters.

William: The insurance application process

Continued on next page

"Most companies are aware of the need to include a basic security clause that obligates the vendor to implement appropriate and reasonable administrative, technical, and physical security measures that conform with then-current prevailing industry best practices, as well as provide notification in the event of any security breach."

DANIELLE JANITCH
Osborn Maledon

SUBMITTED PHOTO

William Furnish

> "If we are looking at trends, what we'll see is likely a step back from federal government leadership and enforcement and states stepping in, if they have the resources. Every state at this point has a data breach notification law, many have data privacy and AI laws, and there's no national action on data breach requirements or data privacy."
>
> **WILLIAM FURNISH**
> Osborn Maledon

Continued from previous page

will in some ways force you to think about the issues we've been discussing that increase risk, like what third party vendors am I working with? What terms do I have with them? Who has access to what information?

Wes: Moving from a private solution to a public solution, what impact are you seeing on data security from changes at federal agencies from the current administration?

Hoyt: We've spent a phenomenal amount of time over several administrations, Democrat and Republican, putting controls in place. We've been building systems to help businesses protect themselves because we realize as a nation our businesses are our strength. It bothers me to see these systems shut down without evaluating first what they contribute. I know people who work at the National Institute of Standards and Technology who are very focused on trying to help businesses, governments, and the military protect themselves from cyber-attack. I'm concerned that systems are being shut down without evaluating what they contributed and, when we right the ship, it will take much work to put it all back in place and repair the damage.

William: If we are looking at trends, what we'll see is likely a step back from federal government leadership and enforcement and states stepping in, if they have the resources. Every state at this point has a data breach notification law, many have data privacy and AI laws, and there's no national action on data breach requirements or data privacy.

Danielle: I expect more state laws on AI regulation for both those offering AI to customers and the customers using these AI offers. To prepare for these laws, companies should be reviewing their employee and customer agreements to consider what rights are being granted to enable use of data from these constituents to be inputted into and used with AI tools – taking into account privacy obligations to the same and privacy laws.

William: There are existing laws on the books that are flexible enough to apply to AI practices—consumer fraud laws for instance. So just because there's not a law that is specific to AI doesn't mean that it is a free pass.

Wes, I was going to ask you is, if you are the victim of a ransomware attack, should you pay the ransom, and, if you do, are you potentially breaking the law?

Wes: Good question. You should never pay the ransom unless it's a very last resort. There are circumstances where if you don't have a backup and you can't recreate the data and you might go out of business. Under those conditions you might have to consider paying. And that goes back to the question of having a solid cyber panel and do you have insurance that's going to help you understand if it's even legal to pay the ransom to this particular threat actor? Ultimately, you are negotiating with a criminal hoping for a positive outcome, which is far from a reliable solution.

William: So, better to put yourself in a position where you have backups and taken steps to ensure that you're not in a position where paying a ransom is essential to the continued existence of your enterprise.

Hoyt: One of the most critical things that you just mentioned is the Office of Foreign Asset Control. They want to make certain if you're paying ransom, you're not paying it to, for example, North Korea, which they consider to be a terrorist country. You should never be making this decision without the advice of counsel. You need good legal advice, not just technical advice when dealing with an attack like this.

Wes: On that point, should a business report every cyber-attack? And are there situations where it is better not to report?

William: If it meets the statutory or regulatory definition of an attack that requires notification, then yes. But not every cyber-attack is an event that requires a report.

Wes: Yes, that's a question we hear a lot. I would submit that 100% of businesses with an internet-facing presence have and will continue to be attacked. So then it becomes a question of when does a cyber-attack become a reportable event.

William: Wes, I know because you work with a lot of businesses and education institutions, I imagine you have numerous, basic steps that folks can take to reduce their risk.

Wes: We often get questions about how do I make my system secure? What one thing can I do? It's not one thing. You have to have an organization that values having a cybersecurity system and plan and prioritizes putting those appropriate protections in place. But what we have seen over the last dozen years, is that there are some common controls that you can put in place that will dramatically reduce your risk of a successful cyberattack. You can have the most secure systems in the world, but your employees are often your weakest link. And if they click on that link, they will allow the threat actor to come in and take whatever they want.

William: Never underestimate human error.

Wes: One thing with that that is helpful is to not make phishing and training punitive for your employees. You know, give some positive rewards. We've seen a significant uptake in engagement with gamification and rewards for participation.

Another effective control is multifactor authentication (MFA), which has drastically reduced the frequency of account compromise. If a phishing email, account gets compromised and then the threat actor moves laterally through the network, game over. MFA very often stops those things from occurring. Vulnerability scanning helps too. You know, checking

the doors and windows of your systems to make sure they're locked, monitor any external, assets you have on the internet, just making sure those are locked down. The bad guys are doing that on a regular basis. And one thing to keep in mind is this is ongoing and not a one-and-done because systems are always changing. New vulnerabilities come up.

An active cybersecurity program also includes endpoint detection response (EDR) software. Again, that's something that can stop a ransomware attack, potentially. It's not an end-all, be-all. Sometimes, some threat actors can get around certain systems. They target those. But it's again its defense in depth that's having layered controls in place. Install software patches.

We also can't overstate the importance of software patching. We've seen patches that have been out for a year and a half, compromising servers that, if installed, would have prevented a claim. We know that's not always an easy ask, but usually the risk is worth the additional protection it provides.

Wes Gates

SUBMITTED PHOTO

Hoyt: And the other thing, of course, is that we have too many people who are running systems that are end of life. Standards require you to be up to date on patches. However, some systems that hit end-of-life years ago; there are no new patches from the vendor. Old software that's past end-of-life is essentially an open wound and will certainly be exploited by attackers. It is imperative to mitigate these risks if these EOL systems must be kept in production.

William: All of these points really stress that you need to have a good overall plan and guidance within your organization along with a consistent and deep data security plan ahead of time.

"We often get questions about how do I make my system secure? What one thing can I do? It's not one thing. You have to have an organization that values having a cybersecurity system and plan and prioritizes putting those appropriate protections in place to having a solid cyber panel."

WES GATES
CyberPools

Your account is expired.

Click here to reactivate your account.

You wouldn't fall for it, but Chris in marketing just clicked the link.
Now they're in, you'll find out about it in a couple months.

One of the best ways to mitigate the effects of a data breach is to respond promptly. You need an incident response plan. We help clients minimize potential legal exposure at the front end by drafting corporate contractual provisions, company policies, and employee agreements. Then, after a breach, our cybersecurity response team can quickly and efficiently investigate the breach and seek appropriate judicial relief and protective orders on an expedited basis to minimize the harm.

You need to be prepared for when your system gets hacked. We help you develop a plan so if the worst comes to pass you have a strategy and procedures to act quickly and mitigate problems.

OMLAW.COM

OUR DATA SECURITY SPECIALISTS:

Danielle D. Janitch
(602) 640-9381
djanitch@omlaw.com

William Furnish
(602) 640-9341
wfurnish@omlaw.com

OSBORN MALEDON
ATTORNEYS AT LAW