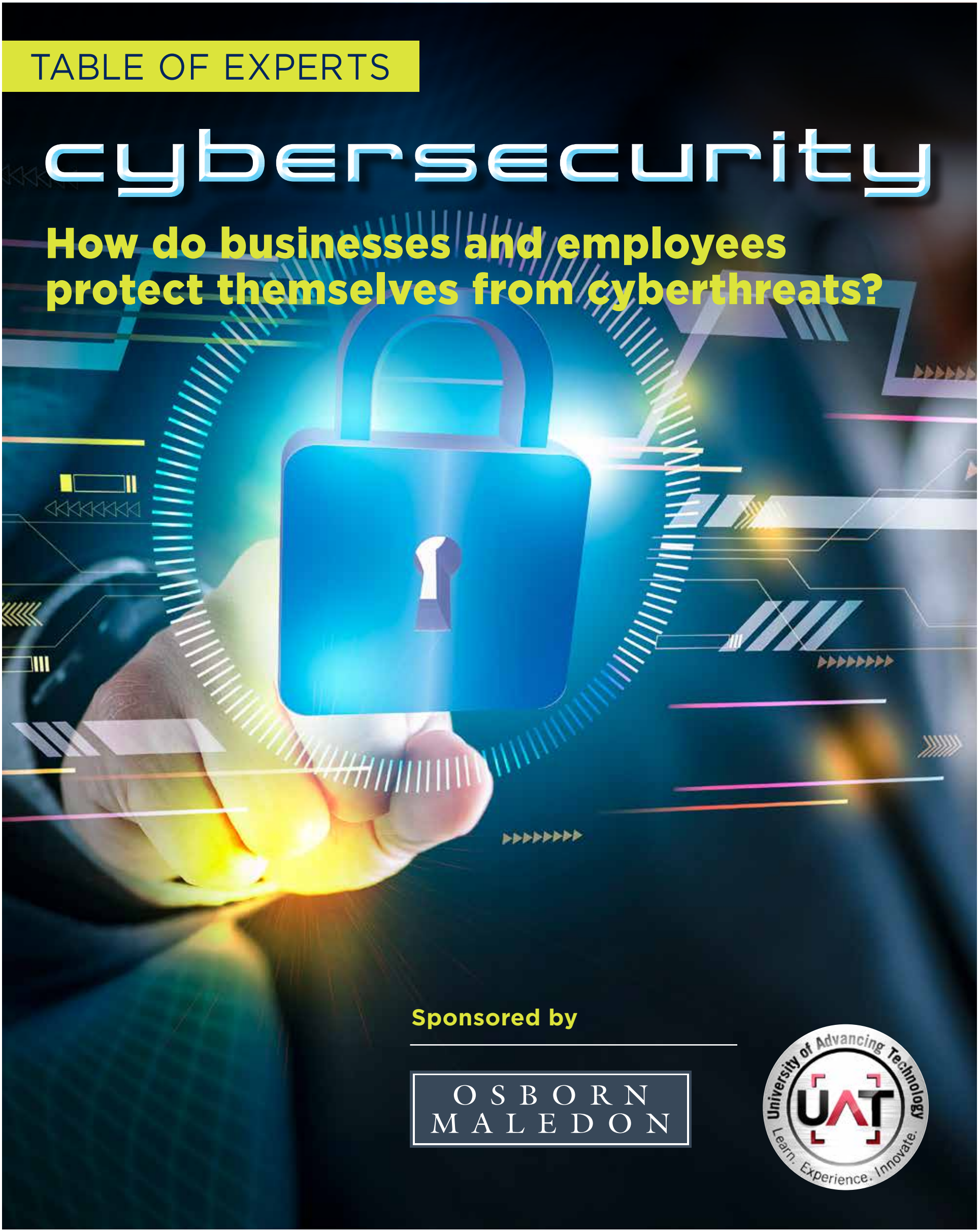
ADVERTISING SUPPLEMENT TO THE PHOENIX BUSINESS JOURNAL

TABLE OF EXPERTS

cybersecurity

How do businesses and employees protect themselves from cyberthreats?



Sponsored by

OSBORN MALEDON

University of Advancing Technology
UAT
Learn. Experience. Innovate.

ADVERTISING SUPPLEMENT TO THE PHOENIX BUSINESS JOURNAL

WILLIAM FURNISH
Partner
Osborn Maledon P.A.

William Furnish is a commercial litigator and partner at Osborn Maledon P.A., where he co-chairs the firm's Privacy & Data Security Group. In this capacity he regularly advises businesses, educational institutions and government entities on compliance with, responses to and litigation involving trade secret, document management, data security and privacy matters. He is currently involved in groundbreaking litigation on Arizona's Automobile Dealer Data Security Law, pending in federal court. William represents clients in both state and federal courts, as well as in arbitrations, mediations and administrative proceedings.

He is a co-author of the Bloomberg Law: Privacy & Data Security profile for Arizona and regularly presents and writes on data security and privacy matters for publications, including the "Phoenix Business Journal."

Before he joined Osborn Maledon, William's practice involved advising and representing Big Four accounting firms, pharmaceutical manufacturers and other institutions in connection with securities, professional liability, intellectual property and commercial litigation.

He has been honored by Southwest Super Lawyers as a Rising Star, Business Litigation, 2020, and by Best Lawyers®, in its "Ones to Watch" category for 2021.

His community involvements include participation in the Arizona Technology Council, the Federal Bar Association Board, and the Phoenix Public Library Foundation Board.

Ray Schey: Businesses have been working remotely and trying to do what they can, but how many will do so in the foreseeable future? And what steps should or could businesses take to make sure their employees are practicing good computer hygiene and how can they prepare for possible security incidents? And what does it mean for the business culture regarding security, where the staff is now working remotely rather than in one place?

William Furnish: I'm an attorney and partner at Osborn Maledon. I'm in, among other groups, our cybersecurity and data security practice group. And we've been working remotely effectively since March.

A big part of working remotely has meant educating people about what might seem to us in our fields as no-brainers, but simple stuff like, don't click suspicious links because now you're always connected to work. I think a big part of that has been changing the mindset. When people go home, they're not used to thinking, "I need to maintain all of this information confidentially as attorneys." Certainly, other industries have these obligations as well, but we have professional obligations to maintain security over the information we have.

The first thing you can do is, if you're working from home, make sure your router is up to date. There's firmware that comes out regularly for your router. It may seem mundane but updating security updates is crucial.

If you're working outside of the home, try to avoid using public networks at all costs. And if you have to use public networks, make sure you're using a virtual private network or some other form of secure data transfer on those public networks. Make sure that you have some form of password for your home Wi-Fi, if you're using Wi-Fi.

Aaron Jones: One thing I stress for individuals is not only how are you responsible for the business's data, but you're also responsible for your data, your family's data. We're essentially each having to become our own IT team that is the first line of response, the first line of defense. I also see individuals reaching out to me and saying, "Hey, I've seen something," or, "Hey, something feels odd," or, "I don't feel right about something." They've never had to be their own IT team.

The responsibility for information security for protecting data for individuals who work in health care, who have to worry about HIPAA now, and they have to worry about it from home, even though they are working using something like a VPN to connect back to a system 25 miles away. What used to be a morning commute now becomes a press a button and dial in and have to be concerned about all of these items.

One thing I'm telling people is you need to put yourself in the safest position possible. Number one item is open communication. Be ready to pick up the phone because nobody in your IT team is going to be mad if you pick up the phone and say, "I don't feel comfortable about an email I got." But they are going to be worried if you say "Hey, I got this weird email and I double-clicked on the attachment."

The next order of business is secure your mobile devices. We don't have to just worry about the bad guys. We have to worry about accidental things like children, leaving your computer available and a kid, getting ahold of it and dumping everything into the trash. Or an incident that I did see was an individual who was issued a computer and he allowed his children to use it. And they got the computer infected by going to a webpage that was for children.

We don't just worry about the shady guy that's targeting us from overseas. We also have to worry about the accidental things that can

happen in our own home.

Ray Schey: Aaron, we're going to stick with you. There's a term called sandboxing. Can you explain what that is and how it can help a business?

Aaron Jones: Sandboxing is important because we want to reduce the threat profile our users have to deal with. What I would recommend you do is go out and do your investigation once you have these terms and you have an idea of what to go out and search for, but there are companies like Proofpoint as well as Amazon that offer the ability to provide a remote desktop for your users to work on, but they continue to control the system. Your users will sit down and log into the Proofpoint browser, and all of their web browsing is conducted on a system that is remote even though to the user, it's completely transparent.

They use the computer as they normally would, but all the communication is done somewhere else. And a user who may be potentially eavesdropping on the network or somebody attempting to exploit that user's browser remotely, your use is insulated against these things.

Ray Schey: And that's a benefit to the business just because of the safety aspect of it.

Aaron Jones: It is, and as well as the control because now you can audit what they're doing without asking them to install things on the computer. Obviously there's a balance that you have to strike between the trust that you have for your users and how much you want to be able to look at what they're doing on their home network. By having them work on a system that you have access to remotely, now you can audit everything.

Ray Schey: William, as a corollary to working from home, there's so many children that are getting homeschooling now as a result of a lot of schools that have not reopened. But schools also maintain large numbers of files on their own networks too. What risks are involved there and what steps can parents in the schools take to protect themselves?

William Furnish: This goes back to Aaron's point and our earlier discussion about this sort of culture of working remotely: You don't necessarily think of your kids as a potential conduit that could impact your business. But to the extent you're sharing devices, that absolutely is a possibility.

As a result of data breaches, there can be the loss of Social Security numbers, student information, a lot of personal information. Now, schools are required to comply with federal law called FERPA that imposes security requirements on them. Arizona state law requires the security of student records, but that's not a guarantee. I think the short answer is, as a parent, you're pretty reliant on the steps the school has taken to protect its own systems.

To the extent possible, monitor the news and make sure if there is a breach, you're aware of it, because there are reporting obligations, but you may not hear about that.

Ray Schey: That raises another question, in how good are school districts and government when it comes to protecting their own data?

William Furnish: I think they do the best they can with the resources they have. My firm has advised school districts and charter schools and all sorts of networks on data security issues. There is no completely hardened system that is impervious to breaches.

Some government systems do contain very valuable personal information. I'll just give you an example in the education space. There's an organization that collects donations for schools called Blackbaud. There had been a data breach because Blackbaud, which has all this financial

information, is viewed as a very target-rich environment.

If you're sharing information with other entities, if they're vulnerable, then you're vulnerable too.

Ray Schey: We're going to throw a term to you Aaron: cryptojacking. How concerned should people be?

Aaron Jones: I'd really like to back up William's statement on the education part and making sure you're talking to your children about these things because back in 2010, around February 2010, there was a lawsuit out in Pennsylvania in which a school there was using the laptop webcam issued to the kids to spy on children and take photos of the insides of their homes and things like that. One thing I will tell parents is if somebody gives you a device and you bring this device into your home, you can be appreciative of the device but you should also be cautious of said device. Tell your students or children take the device, put it away at the end of the night.

Don't leave it open facing towards the bathroom or something like that. You never know who could potentially be using that device, especially when these schools have become a little overzealous in trying to monitor what's being done with their tools.

Going back to cryptojacking, if you are a business or a company, you may have experienced issues with individuals who come to you and tell you, "Hey my computer's moving very slowly. I'm unhappy with the performance of the network". You may find it's not your system, it's individuals attempting to abuse your network by looking to mine cryptocurrency. Cryptocurrency, being things like Monero, Bitcoin or any of the other cryptocurrencies that are out there.

One issue we have is it's surprisingly easy to include a bit of JavaScript into a webpage.

CONTINUED ON PAGE 20

AARON JONES

Professor

University of Advancing Tech

Aaron Jones, the lead Cyber Instructor at the University of Advancing Technology, is a software developer who currently creates applications for law enforcement. He is also an AZ POST certified general instructor as well as a public speaker. He earned a B.Sc., in Computer Information Systems from Park University in 2013 and an M.A. in Intelligence Analysis with a focus in Cyber Security in 2014. He has been the recipient of recognition from the El Paso Police Department, State Of Texas, Texas Military Forces, Chandler Police Department and others.

Aaron is also active in the community as the founder of the Phoenix Linux Users Group Cyber Security Meetup and regularly teaches members of the public a myriad of topics related to cybersecurity. His audience includes students, teachers, law enforcement, military, government officials and concerned members of the public with a strong desire to learn what is going on in the world of technology.

When Aaron isn't teaching, working, or spending time with his family, he enjoys relaxing at the pond with a fishing pole while not catching fish, operating a pistol at the shooting range or reading books. He owns a Sega Saturn and a Sega Dreamcast and his favorite video games are Panzer Dragoon, Road Rash, Phantasy Star Online 2 and Power Stone.

CONTINUED FROM PAGE 19

For a while, it was projected to be the future of advertising. Instead of serving ads that people were using ad blockers for to block anyways, they were going to use the resources on your computer to mine cryptocurrency while you viewed a webpage. As you're reading the news, they take your excess processing power on your computer. And they conduct what's called mining, which essentially is just the process of supporting that cryptocurrency by confirming transactions.

In the event that something like this happens, one of the first things you're going to see is very high CPU load on your system. We see this on servers, we see it on desktops, laptops, we see it everywhere because the idea is to do a shotgun approach. Infect as many systems as you possibly can do as much mining as you can before they fix it and try to make as much money as you can before the golden goose dies and you can't get the egg anymore.

The idea here is take the steps necessary to protect your systems, both at work as well as at home. Juicy targets are kids, lots of laptops are issued to children. If you could get them to go to web pages that allow you to cryptomine while they're on those webpages like games, you can use those resources to essentially mine for free. And those are some of the issues that we've seen. We've even seen these kinds of infections end up in places like 911 centers.

Ray Schey: William, Arizona's data security and data privacy landscape is policed by the attorney general, and the attorney general's recent lawsuit against Google based on deceptive and unfair practices is maybe another enforcement tool. Is there anything this lawsuit might be able to tell us about how the attorney general views its role and whether we can expect lawsuits from individuals against businesses for use of data moving forward?

William Furnish: To take a step back a little bit, unlike the European Union, the United States has a patchwork of laws regarding data security. At this point, all states have a data breach security notification law. It's generally, at a very high-level, regulated by the Federal Trade Commission and some other federal agencies, but there's no data-specific entity. And there's been a lot of discussion about a national data security law. It's been a growing discussion, but at this point every state's doing their own thing.

Arizona has a data breach notification law, which imposes some financial penalties if a data breach isn't reported under certain circumstances. Part of that data breach law involves the concept that you don't have to notify people if you conduct a forensic audit and determine that there's no risk of loss of financial information. And if you're sandboxing, it's a lot easier to audit what's happened. If I'm running a company, and I have a data breach and I don't notify people, the individuals can't sue me for failing to notify under the data breach notification law. Instead, what happens is the attorney general sues me and there's some monetary penalties.

There's also a very broad law in Arizona that's used for all sorts of sales of goods and consumer sales, which is a consumer fraud act. What is interesting is that the Arizona attorney general has sued Google for deceptive and unfair practices regarding Google's tracking of individuals and not really explaining how they track those individuals in connection with the use of Google smartphones and Google applications. The interesting thing about that is in addition to the attorney general's ability to sue under that act, that does have a private right of action.

The point I want to share is what I would call a legal hook for individuals to sue businesses; that's where liability can really explode. The data breach notification law has capped damages. The consumer fraud act does not and there is a potential for punitive damages. I think one thing businesses need to be aware of – and why I'm personally watching the suit carefully – is to see if there's something that

can be gleaned about what potential liability under this act means. The question, in terms of data privacy, is whether individuals could potentially sue businesses based on what they view as deceptive practices in how businesses use their data.

This is still working through the courts. Google recently tried to dismiss the lawsuit and that's pending. The bottom line is businesses ought to be aware of potential claims not only that the government has, but also that individuals might have against them for what businesses might view as pretty normal practices.

Ray Schey: Let's talk about spear phishing, Aaron, and how do companies protect themselves from that tactic? Can you tell us what it is first and then how do companies protect themselves against that?

Aaron Jones: What you'll hear is either the term spear phishing, phishing or a whale phishing, and they typically each represent the same thing, and that consists of sending out a message to someone in the attempt to get them to take action. When dealing with phishing in general, most of us are aware of something like receiving an email that says I'm the king of such and such country. I have $10 billion. I want to share that money with you, whatever.

Spear phishing is taking it a step further. I go to your social media. I find out about you. I get a little bit of information about who you communicate with, and I build a picture of who you are, so that I can build a message specifically for you. If you and your company only use Zoom for communication and I send you a message about your team's account being suspended. You might not care about that. You may delete it. You may think it's spam.

But if I find out on your social media that you've complained about Zoom connection issues, I can make an educated guess that you're using Zoom. And then therefore I build an email that looks like it comes from Zoom, and I communicate with you that way. So number one, speak to your employees, speak to your children about social media and its use, understand that anything that you're putting on social media potentially has value to someone, these companies wouldn't exist if the data didn't have value.

All of this has information I can use to glean. How's the company doing? Who are they doing deals with? Who are they communicating with on LinkedIn? All of this becomes valuable and then eventually becomes part of my attempt to fraud or convince you to click on something, because ultimately my job is as if I was the bad guy would be to build a sense of urgency by telling you that there's a very short period of time to get something done.

Ray Schey: William, the European court of justice recently declared that the EU and U.S. privacy shield is invalid. What is the privacy shield? Why was it important and what does it mean for businesses here?

William Furnish: The EU and the United States have, for a very long time, had data transfer collaboration. This agreement was a Safe Harbor, which permitted transfer of data between EU and the US that complied with certain requirements as being insulated from potential liability and from EU requirements. Now that has been declared invalid because the CJEU viewed it as not protecting data.

The U.S. Department of Commerce and some entities in the EU and Switzerland entered into what was called a privacy shield. The whole point was to replicate the Safe Harbor, allowing companies to apply for the program they needed to comply with its requirements. And if you were a participant, you could certify that you were complying with the EU's requirements or the European commission's requirements, or the Swiss requirements. And they were complying with our requirements, and it's all hunky-dory to share data.

Earlier this year, the Court of Justice for the EU concluded that the EU-U.S. privacy shield did not provide sufficiently adequate protections for EU citizens on government monitoring. And shortly thereafter, the Swiss administration reached the same conclusion. It did not strike down, however, what are called alternative data transfer mechanisms for controllers of data who want to use things like standard contract clauses, which basically– without getting too into the weeds on it – certify and state that you will comply with all the requirements and that you will treat data safely and securely.

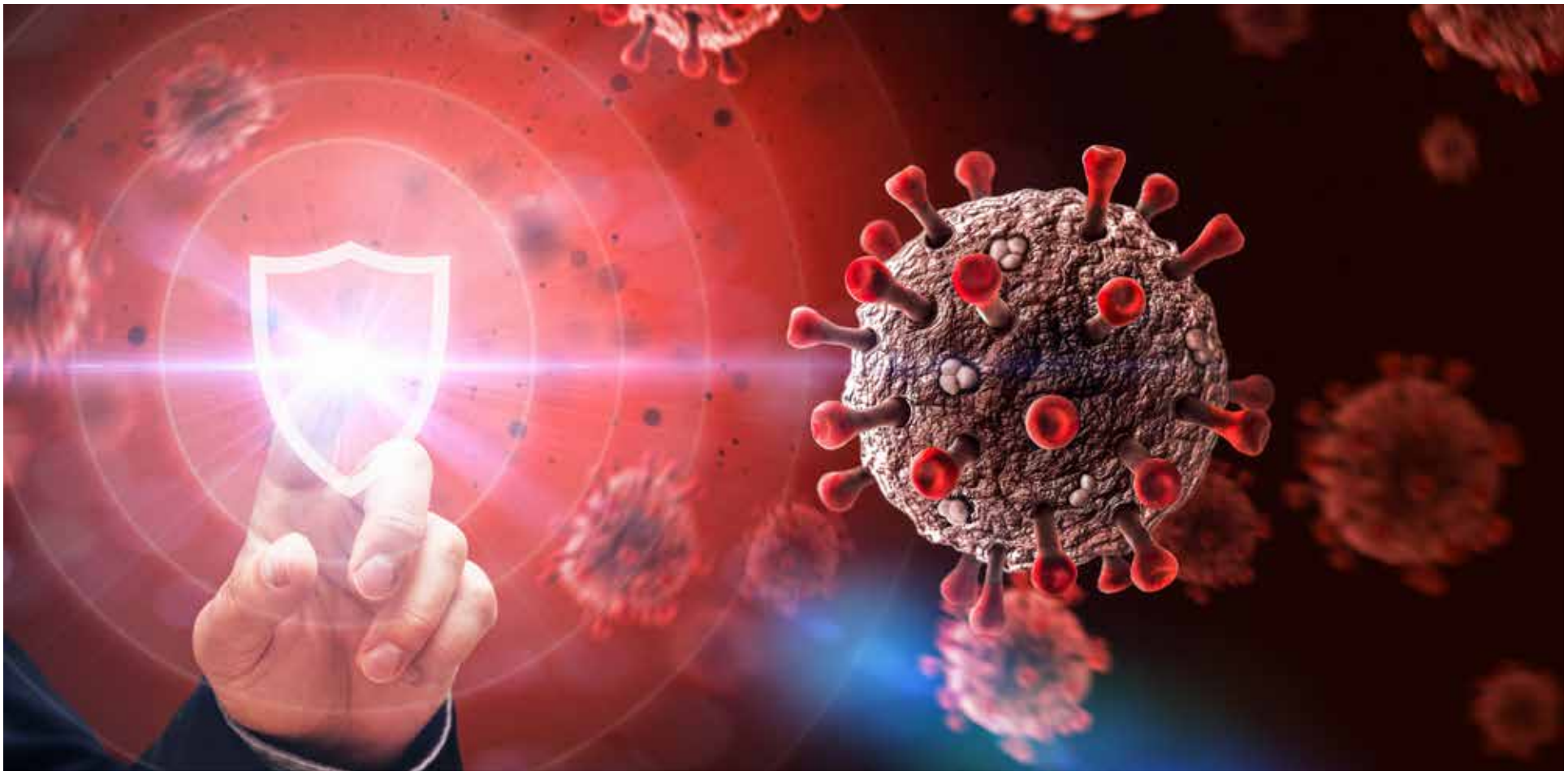
There is still a mechanism for U.S. and EU companies to ensure they're complying across the board, but those standard contract clauses still need to be audited and investigated. Now the Commerce Department is trying to keep the program going and is still certifying folks.

Ray Schey: Aaron, can you tell us what are some of the threats that business owners should look out for like in the B2B business fraud arena?

Aaron Jones: One thing we have seen is businesses receiving unsolicited bills for goods or services that were never ordered. Google suffered from this in which a third-party vendor figured out what kind of servers they typically order, and then started sending them bills for those servers and they never delivered any product. They lost a lot of money and ended up having to take that individual to court, but as the size of your business grows, and as you spend more time focusing on different aspects, one of the things you may not expect is to receive a bill in the mail for $300, $600 or something for IT services rendered or for software purchase.

The idea is to do so in a way that is similar to the way you normally do business. Another issue is attacks against paychecks and payroll. That's a big one I urge companies to pay attention to. It's very popular to get enough information through breaches or otherwise about somebody's employees and then contact and say, "Hey, I need to change my direct deposit."

Now the money is being delivered to an account where it's being sent off to mules to eventually be sent to a foreign country or something similar. So be willing to educate



your HR team.

Ray Schey: William, how has Covid impacted the legal process and what have courts and law firms been doing to respond, and specifically can you address the different security risks that are created by remote litigation proceedings now?

William Furnish: I would say, high-level, the courts have done a good job in responding to the Covid emergency in moving things to remote hearings quickly. But it's sort of an ongoing process, and the physical courtrooms were closed for a little while, and they're slowly coming back.

Where it's safe to do social distancing, they are moving back to in-person juries. But they're also, at least the courts here in Maricopa County, experimenting with remote juries and other types of alternative dispute resolution, where they will encourage the parties to go to an arbitration process with a certified arbitrator, rather than going through the court or requiring some sort of jury trial. As a result, that's had a bit of a pile-up effect on civil trials, which is business-to-business litigation. Maybe slightly less so here in Maricopa County than in federal court.

What I have found is, at least in my hearings, all the hearings that used to be in court have gone remote. That's less of an issue for hearings that only involve a judge. There's no witnesses or anything like that because you're a lawyer, you're an advocate. A lot of times in the past those hearings would happen telephonically. So, in some ways, it's been a benefit. Your advocacy can be more effective because you're seeing people and seeing how they react.

For pretrial matters, like evidentiary hearings that involve witnesses, that's where it gets a little trickier.

There's a speedy trial right guaranteed by the Constitution. In state court, there's less of a backlog, but still things are slowing down. If you're thinking about trial and you're thinking about a typical jury trial, that may get pushed significantly, or the court may strongly encourage you to not do a jury trial or to do some form of alternative dispute resolution.

Even if it's remote, you still need to be in the frame of mind that, this is a hearing, this is a formal legal proceeding and there's potentially sensitive information that's being exchanged. It's still a hearing, you're still in front of a court, dress professionally. If you're in a deposition, if it's a deposition in your house, that's still a deposition that it may get recorded. If it's video-recorded, dress professionally, be professional, take it seriously.

Ray Schey: Aaron, what's the Arizona Counter Terrorism Information Center and how can it help business owners in the event of a security event?

Aaron Jones: Arizona has a fantastic cyber and counterterrorism focus here. The ACTIC is a mission designed around protecting the residents and critical infrastructure of Arizona. If you have a business IT team or anything like that, you can connect to them through what is a called ACIP, which is going to be the Arizona Cyber Information Program. By connecting with them, they will provide you up-to-the-minute information about threats.

Through the ACIP program, you can receive that information and provide that to your IT team. In real time, they can sit at their whatever edge connection they may be using. They also provide regular meetings, and it's also a great networking tool.

Ray Schey: Maybe a good follow-up question to that would be how should business owners come up with an incident plan and what can they do to start preparing now?

Aaron Jones: Your incident plan should first go to your counsel. Find your lawyer, have a sit-down conversation with them and let them know your concerns. And then begin that process of mapping out. What am I concerned about? What are the things that could potentially affect me, who could be affected? And who's going to respond in the event of an incident?

One thing I will typically tell people is let your people know who you call first. This is who you call second and this is who you call third. There needs to be a three-step plan, three individuals who should be contacted.

That's going to come back to what do you decide as a business is most important for you, but don't operate on an idea that it's never going to happen to you. Operate on the idea that when it happens, this is how we're going to respond.

William Furnish: You shouldn't be thinking about this for the first time when something bad happens. So obviously you ought to talk to your legal counsel because they can tell you what your obligations are before there's even a breach.

You also want to look at insurance, although it's with a big caveat, which is there are cyber insurance policies out there that will protect you or that have some coverage in the event of data breaches and incidents. Your general business liability insurance may also cover that. But this is sort of an emerging field and its insurance based so much on years and years of what certain terms mean in insurance policies and litigation about what that means.

You also need to not only be aware of what your own practices are, but also be careful when you're sharing information with other people. Make sure that at the very least you are getting information from third parties about what their practices are. And make sure that if your third parties are breached, you know about that immediately.

And finally, because there's ransomware attacks and other threats, have an account with Bitcoin or some sort of cryptocurrency set up so that if you want to pay the ransomware, you're not scrambling at the last minute to figure out how to acquire it and how to set up the account and how to set up the transfer. Aaron, what do you think about that one?

Aaron Jones: The official stance from my understanding the FBI as well as the ACTIC, as well as essentially all law enforcement that I know, is don't pay the ransom. And what is also interesting is William brought up the insurance. Let's just say that you have insurance that has claimed that they're promising to pay the ransom in the event that your stuff gets cryptolocked. Well Oct. 1, actually FinCEN which is the financial crimes group part of the Treasury here within the United States has essentially stood up and said actually if you pay off these ransoms, because what we're finding is it may be a country like North Korea or somebody who has sanctions against them, you're now doing what is essentially money changing. And you're sending this money off to these countries that we don't do business with legally.

And we're starting to think here in the courts that maybe we need to start holding you folks responsible for this. So therefore you may be taking that responsibility, that one of these companies that was previously saying, "Hey you know what, we'll do it. We'll go pay this ransom for you. We'll handle all of it, don't worry about it." And then if you buy that Bitcoin and you do it yourself, then you end up in a situation where now you're doing business with North Korea and somebody steps in and they take a look at that.

Your backups need to be offsite, perhaps getting with a third party like Amazon and making sure that on a daily basis, a nightly basis, whatever that you're making backups of your valuable information and moving that to another location with something in between that prevent somebody from pivoting from your network to that network. So therefore, not if, but when your systems are breached or you are otherwise affected by something like malware or cryptolocking or so on and so forth, you will be able to recover.

This incurs costs, it incurs an IT team that is capable of doing these things. And maybe even having to sit down and figuring out hey how do we actually go through this process and spending some money, but it's going to be a lot less expensive than having the treasury department come knocking on your door to have a conversation with you.