TABLE OF EXPERTS

CYBERSECURITY

Sponsored by:

OSBORN MALEDON
ATTORNEYS AT LAW

Ray Schey: We're here with Danielle Janitch and William Furnish, the co-chairs of the Privacy and Data Securities Group from Osborn Maledon. We also have Jason Pistillo, President and CEO of University Advancing Technology. To start off, Danielle, how do we protect ourselves from someone adapting or hacking the algorithms or AI for harmful purposes that can compromise data security and is there anything in the legal or regulatory perspective that addresses those risks?

Danielle Janitch: Thank you, Ray. The first thing that people in the cybersecurity space should think about with respect to AI is it can be a positive, as well as a negative. What AI is bringing to the world today are the concepts of speed and precision, allowing algorithms essentially to mimic and do better things than humans themselves can. That is important because in cybersecurity we are constantly trying to manage changing and evolving threats. It is also important because AI could be a tool that we can use to leverage and deal with the talent gap to enable us to better protect and prevent cybersecurity attacks. On the flip side, AI can be also used by the bad guys to make threats better, more credible and more effective.

Ray Schey: Yes, we'll turn it to Jason, who's in the trenches on this every day at the University Advancing Technology. Jason, what do you have to add?

Jason Pistillo: Let's start with a primer on misnomers with AI, because it's been around for a long time; with teaching of it started in 2004 or 2005. The current popularity of AI is more about a smarter Google. I can now say plain-speak words; it's natural language processing, which has created the tip recently that I can just talk or use plain words into a ChatGPT and create an outcome. The challenge with that, though, is it's creating a need for more precision reports. There are a lot of AI tools out there that can help protect the network. That means it's just self-learning or it's adaptive, but AI is a broad concept that means a lot of things to a lot of different people.

William Furnish: From my practice standpoint, because of where we are and the clients we represent, we tend to see bad actors using AI tools to try to exploit vulnerabilities and attempt to steal data or help humans penetrate systems. But businesses should carefully examine partnering or bringing AI tools as part of protecting their companies.

Danielle Janitch: This reminds me of a cybersecurity incident that occurred at a law firm in Pennsylvania. And the law firm decided just the year before it had its cyber incident not to purchase an AI tool that monitors user behavior, i.e., are you logging in from the usual places you log in? Are you logging in from two different places where you shouldn't be? When you log in, what are you doing within the system? Is your footprint the same as it would always be?

The law firm chose not to purchase it because the partners thought it was too expensive. Within a year they found they had four people in their system accessing data they should not have accessed, and it might have been flagged had this behavior monitoring system in place. It was an internal hack, people within the law firm that were doing things they shouldn't be doing. This exposure implicates a law firm's ethical obligations.

This is an example of AI's potential to go in both directions. We all know from the big splash media events that have happened in the last year or two that AI can create things people do not intend to create, and we are just at the outset of trying to figure out how to appropriately regulate AI. Before 2023, there were only three or four states in the country that were addressing this, and now we're not yet towards the end of 2023 and there's at least 11 that I'm aware of that are actively engaging in having passed laws that are going into place.

Ray Schey: Let's jump into a more general conversation then, about recent cybersecurity trends, too, and we'll start with you again, Danielle. What other recent trends are you seeing with your clients in terms of the types of attacks, the sources of those attacks, and of course the targets, whether it's business or otherwise?

"...the issue is not just knowing what your vulnerabilities are but also the vulnerabilities of the folks that businesses are relying upon to handle their data and process their transactions.."

WILLIAM FURNISH

Danielle Janitch: I'd say one of the things that I've had in my client base, where I represent a lot of small to mid-size companies that are technology providers, is they have

MEET THE EXPERTS:

DANIELLE JANITCH

Attorney and Co-Chair
Osborn Maledon's Privacy and Security Group

Danielle Janitch co-chairs Osborn Maledon's Privacy & Data Security Group, which is recognized as a leader in Arizona on these issues. Danielle assists a wide variety of clients with developing and managing data protection and privacy programs, including helping draft privacy, security, and document retention policies.

WILLIAM FURNISH

Attorney and Co-Chair
Osborn Maledon's Privacy and Security Group

William Furnish co-chairs Osborn Maledon's Privacy & Data Security Group with Danielle Janitch and is a member of the Ethics & Professional Liability Group. He regularly advises businesses, government entities, financial institutions, and attorneys on ethics, trade secret, and data security matters.

JASON PISTILLO

CEO and President
University of Advancing Technology

Jason Pistillo has been a noteworthy leader in the industry for over two decades. In his tenure, University of Advancing Technology (UAT) has been transformed into a one-of-a-kind, elite, private university that features world-class degree programs in a technology-rich campus environment.

President Pistillo's commitments to life-long learning, personal growth and development culminate in his joy of educating future leaders in the fields of advancing technology.

software platforms that they deliver to their customers, and you worry about introducing vulnerabilities through your software platform into your customers' systems and vice versa through open-source code vulnerability.

One of the problems with open-source code is security and whether you're adequately keeping track of what you put in your software and then whether you're adequately patching it and updating it as vulnerabilities are detected in that software. Synopsis did its 23 open-source security and risk analysis reporting, and it surveyed thousands of companies and they found that out of all the companies that were using open source, which was a large percentage, 84% of the code bases had at least one open-source vulnerability in it.

William Furnish: With those vulnerabilities you identified, Danielle, the key point is no one knows they exist until they have been exploited. From a business standpoint, the issue is not just knowing what your vulnerabilities are but also the vulnerabilities of the folks that businesses are relying upon to handle their data and process their transactions. You can have the greatest security around, but if you're relying on someone who doesn't, then it's a concern.

Jason Pistillo: Businesses also need to consider where they have their information and what that information is. In the education industry and as an educator, I am responsible for the information I have. We are all familiar with the MOVEit data breach. I don't have MOVEit; we wouldn't touch MOVEit on our campus, but we try to assess potential exposure and provide notice within 10 days to report a breach. And the idea of where's your data and who are your data processors is baked into a lot of the current and long-term laws. It's been around for over a decade.

Danielle Janitch: Sitting on top of this you have all the uncertainty of what all the individual states are going to do because most of the action is at the state level. There are a lot of states that are adopting laws that have gone in effect or will be going in effect that require the consumers to have the opportunity to opt-out. So, if you don't build the product thinking ahead, you're going to be in trouble.

Jason Pistillo: To add to that, in terms of privacy and AI, everybody's heard of code interpreter, ChatGPT

"Cyber insurance is also a bellwether for you. If you're getting better rates, it's getting cheaper, maybe you're doing a good job."

JASON PISTILLO

and when it went from beta to public release, the big problem is that's really useful for us uploading a database and having it analyzed in fine prints, but now where is that data stored? The newest version, Buckley, is local. It must go offline for them to do it. But the idea is to be able to join to macro data, if you want to join the zip code or patterns. So, it's a really important concept and really risky.

Ray Schey: I think this next question is probably one that a lot of Phoenix Business Journal readers will be curious to hear your response to, William. What are the best practices or a few of the best practices that businesses can adopt right now?

William Furnish: First and foremost, your response is going to be tailored to the industry you operate in and how heavily regulated that industry is. For instance, if you operate in the educational sphere, you likely already have a decent framework for data security, or at least can look to some federal and local guidance for the policies you should be adopting. Second, you need to consider the expense of responding to the incident, the cost of preventative measures, the cost of social monitoring of employees and how that fits in your overall operational budget. And Danielle already referenced the AI tools that businesses can adopt, but they may be cost-prohibitive for smaller to medium enterprises.

In terms of less expensive tools, businesses should establish policies about who can access what information, what information is going to be collected from employees and customers, and actually follow through with those policies. Businesses should then educate all their employees about what those policies are, establishing preexisting relationships with the support that you're going to need in the event of a data incident, particularly if you will need regulatory compliance help. Ransomware is still extremely prevalent and disruptive, having data backups is extremely important, and making immediate data backups as soon as possible is going to be extremely helpful. If your data backup is from months earlier, then the disruption will be significant because you will have to rebuild that data.

Danielle Janitch: One of the things that William and I get to do sometimes, which is fun, is help assist with training. There are a lot of training tools available, and you can have highly ineffective ones, and then you can have ones that I think do a little better job. For example, training on phishing attacks that come not through email, but through your phone. Those have just gone off the charts. But with AI coming into play, they are going to get more and more effective.

Ray Schey: Jason, what advice would you give to CEOs and executives that need to take some of these steps to protect themselves and their companies?

Jason Pistillo: If people are getting phished on Tinder, they're probably getting phished on just about everything. There are AI bots running in the backside of Tinder, too. I get two to three text phishes a day, multiplied by every platform: WhatsApp, messages, etc. So cultural practices are a big deal. We have all hands all the time to discuss some of the worst and most disruptive examples.

Ray Schey: Let's talk about the legislators and the regulators. Can you share a little bit of what's happening in the regulatory landscape for businesses, and protecting security and data privacy at the state and federal level?

William Furnish: There has been some national movement, but not meaningfully, toward a unified data security law. You have numerous agencies that are regulating how businesses might need to maintain data security, what type of information businesses need to share with, for instance, their students in the education space. The main regulators are the FTC, the Department of Education, Health and Human Services, and the FCC.

And then underneath that layer, we continue to have a patchwork of state laws governing what you would need to do in case there is a data breach. This is something that businesses need to really drill deep on is because of the patchwork and reach of data. A business may think that it is in Arizona so it only needs to comply with Arizona law, but it may handle data from people governed by California law or General Data Protection Regulation. They may not think they are subject to the Gramm-Leach-Bliley Act, but that is broader than people anticipate.

Jason Pistillo: It's interesting. GLBA covers non-banking financial institutions and catches more companies than they realize, and I feel badly for the companies that don't realize that they're missing a big rule, which will, by and large, have huge ramifications in terms of the fines for them unless they have any sort of touchpoint with the government contract.

Ray Schey: It begs the question. So, let's turn to a topic that probably is on the minds of many of our readers and subscribers too: the insurance market. What are some of the pitfalls related to cyber insurance policies that the insured should be aware of and address that have emerged recently?

William Furnish: The most important thing about cyber insurance are the ways you can mess up insurance coverage, including not getting enough coverage, not having high enough policy limits, and not having the right kind of coverage to put you back where you were prior to the incident. If you have a ransomware attack and you need to then go out and get a vendor to conduct a thorough investigation, you may need to do notifications. You will probably need to engage legal counsel. You'll need to engage with PR. Those costs go quite high pretty quickly.

Jason Pistillo: Cyber insurance is also a bellwether for you. If you're

getting better rates, it's getting cheaper, maybe you're doing a good job. If no one will cover you, maybe you need to get some things put together. It's not just loss or lapse of coverage. You can have holes in your coverage, right?

Danielle Janitch: I'd speak from a practical perspective on what I have seen from my clients from when I started working in this space to now when they're negotiating their policies. And I think I've seen insurance companies get a lot smarter. The policies now are priced better for what the actual risks are because they figured that out better. And the other interesting thing that I've seen lately is the questionnaires. Insurance companies check in. It's not just that they fill out the questionnaire, the insurance company wants to see it. They want to know that the potential insured have a policy in place, and they want to see proof for all of the responses in the questionnaires.

Ray Schey: So, should all companies and organizations have cyber insurance?

William Furnish: Yes.

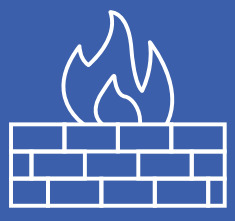
Danielle Janitch: I would think so. Is anybody running themselves completely offline? You're going to have HR data and probably client data. I don't know a company that wouldn't. Also, the more sensitive the data is, the more regulated the data is, the more valuable the data will be, the more important it is.

William Furnish: If you have expensive equipment that would be hard to replace you need replacement coverage.

Jason Pistillo: If you put in access in your data for a day, what would it cost the business? Some places it's not a big deal. But I know what it'd cost us a day. What would happen if you can't open any of your emails for a month?

Ray Schey: So, any final comments from each of you as we close this up?

William Furnish: I'm concerned that the prevalence means that there's a little bit of apathy in the business community regarding data security: "Oh, it's going to happen to us, and we'll deal with it when it happens." Instead, businesses need to prepare for an incident before it happens by having a plan, having relationships with key support established, and pressure testing yourself to see how you will respond to an incident. It is far better, and ultimately cheaper, to pay a little bit upfront to be prepared than it is to try to handle an incident on the fly.



"Data security issues are only going to get bigger and harder and evolutions in technology are going to make the bad guys better at being bad."

DANIELLE JANITCH

Danielle Janitch: Data security issues are only going to get bigger and harder and evolutions in technology are going to make the bad guys better at being bad. Our challenge is going to be how we as businesses and producers in society use those same tools so that we prevail in that fight. We must do that together as a society, thinking about it from a global regulatory basis as well as from a business perspective. And more attention needs to be given to society about managing these risks so that when these new technologies are deployed, they're deployed in a healthy way that preserves society and preserves our privacy.

Jason Pistillo: Another major issue going forward is awareness of where your data is, and what it is, and who's looking at it. For instance, many people do not realize that Google staff can check your Nest footage if it's stored in a bot. How many different examples of that can you give people of where things are and what's available that they're naive about?

You got hacked last month.
You'll find out next month.

Are you prepared? These days it's not a matter of "if" you get hacked, it's "when". 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.

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

(602) 640-9000 • OMLAW.COM • 2929 N CENTRAL AVE, SUITE 2000, PHOENIX, AZ 85012