Table of Experts

Cybersecurity

SPONSORS
BeachFleischman
collaborate forward
OSBORN MALEDON
University of Advancing Technology
UAT
Learn. Experience. Innovate.

Experts tackle latest issues in cybersecurity, including remote work, insurance, legal issues, disinformation, espionage and more

DAVE BOLMAN: I'm so glad we're able to spend some time talking about cybersecurity as it relates to the community at large, and then how it plays out here in the Valley, especially from a business perspective. What are we seeing as consultants or business owners? What should people be worried about or paying attention to? As always, cyber is an ever-changing kind of landscape, and what we dealt with 20 years ago is not what we're dealing with now, and it probably won't be the same thing we deal with in 10 years. It certainly seems like cyber is a permanent piece of our landscapes.

I am Dave Bolman, provost of University of Advancing Technology. Joining me on the panel are Zach Fuller, founding partner of Silent Sector, and Danielle Janitch, an attorney with Osborn Maledon.

And to kick things off, we're over 18 months since the onset of Covid, I'm curious, for those of you who are working in the field day in and day out, what do you think the pandemic has changed with cybersecurity? What's different now, and what trajectory does it have going forward?

ZACH FULLER: Over the last 18 months, we have certainly seen an increase in opportunities for cyber criminals to attack. With the sudden transition to a remote workforce, a lot of organizations were not set up to issue devices that have hardware certs and appropriate protective measures to truly secure connections between their remote workforce and their environment. A lot of people went home, they started working with business data, but using computers that other family members use. In many cases, the IT team doesn't have any kind of control over them with centralized management. That has caused a lot of headaches, especially for mid-market and emerging size organizations. Larger enterprises, not quite as much, but they have their own struggles. That's what we've seen, and as a result, the attack surfaces have opened up. Cyber criminals know this and have been going after smaller and smaller companies. By doing so, they're make a higher return on their investment of time and resources.

DANIELLE JANITCH: I'm an attorney and I tend to work with mid-market and emerging growth companies. I advise them on issues related to cybersecurity and privacy, as well as helping them after an incident has occurred. One of the biggest things that I'm now working with my clients on — that I did little to none of before Covid — is helping them to think about the security and privacy issues around protection of monitoring of employees.

There are a lot of interesting questions, at least from a legal perspective, relating to employee monitoring. This can sound awful and scary, but it's also a necessary component of the workplace today. It involves thinking about how and what data you monitor, especially when you're in the remote environment, and then, as you transition back into the work environment, thinking about what we're going to do to maintain data around vaccination statuses, negative tests, sensitive information for people that opt-out for personal reasons, and whether those personal reasons are valid. A lot of tricky questions that deal with privacy and security issues in a global sense are very relevant now.

DAVE BOLMAN: Danielle, if you had to make a short list of things that companies need to either be aware of or tend to when dealing with privacy when you've got employees working from home, what would that list look like, or what are you consulting people on these days?

DANIELLE JANITCH: From my perspective, I'd be thinking about what kind of consents or permissions do I have from employee to have access to those home systems? How do I maintain access to those home systems? When an employee is working from a company-owned piece of equipment, whether that's in the facility or outside of the facility, you can put certain types of consents and permissions in place, and you can have software and tools available to you to assist in monitoring activities. A lot of times these smaller companies don't have the resources to buy everybody what a larger company might buy them, and so they try to share equipment.

How do you get the appropriate consents, and how do you deal with that? The other thing that's been happening is that some states have been passing laws on gaining consent on both sides of communications, because the concept of privacy, I think, is gaining traction in the United States.

So, even when you're in an environment where it's a company-owned computer, you may not be able to monitor and track all the emails and all the communications that you used to because you need to have consent from both sides of the communication. You have things in place to monitor those kinds of things, but you may not be able to do that without the consent from the other party, and you may be violating state law now without even knowing it. That's certainly true in a couple of jurisdictions in the United States right now. And how do you work around that, especially if you have employees in those jurisdictions?

DAVE BOLMAN: Is the General Data Protection Regulation language making its way into US laws?

DANIELLE JANITCH: Certainly, in California, there is a statute that passed and was recently amended about a year ago now, to bring it kind of closer. I think what's happening is there is pressure in the marketplace. My companies aren't large companies, but they contract with large companies, and their clients need to be GDPR compliant. So, when they contract with us to process data on behalf of them, they're expecting our smaller U.S.-based, U.S.-focused businesses to have in place the necessary policies and practices and procedures to close that deal. That's causing pressure, even though I doubt that my clients are marketing themselves enough into Europe to be directly subject to GDPR, and likely to have enforcement actions from supervising authorities out of Europe, but they need it to close their deals. They need to be able to present answers to security questionnaires, and to present systems in ways that show that they are doing the compliance that they need to do.

I did one of these roundtables about four or five years ago now and was asked if there would ever be a federal law for data privacy issues, security issues. I said no at the time, but I think now there is more pressure to have a federal law.

DAVE BOLMAN: Zach, as you're advising clients on how to configure systems for work from home and having a remote presence, what's your approach, or what are you telling people to be compliant, with monitoring rules, ensuring privacy and those kinds of things?

ZACH FULLER: Security is always a bit of a challenge for organizations because it seems like the compliance framework of the week is popping up and companies must address it with limited resources. What we're seeing is that businesses of all sizes are expected to comply with security frameworks that were really designed for large enterprises. Take the Department of Defense supply chain regulations, for example. We have small organizations that still have big hurdles to get through to keep their customers and stay in business.

The best approach to cybersecurity and compliance is to work on aligning with an industry-recognized cybersecurity framework first. Don't chase one compliance requirement to the next. Those are always changing, and they tend to have a narrow scope. Your major cybersecurity frameworks like NIST CSF or CIS Controls, for example, are two excellent frameworks for mid-market and emerging organizations. They are much more holistic in nature than most compliance requirements. If you follow an industry standard cybersecurity framework that's holistic, covering down on your compliance requirements will be much easier, and you won't have to build a new program every time you need to face a compliance requirement.

Industry standard cybersecurity frameworks should always be the foundation of a cyber risk management program. Cybersecurity should never be a "make it up as you go" approach. It requires following industry-recognized best practices and being able to prove you're doing so. In simple terms, a cybersecurity framework is a list of all the activities that an organization should be doing and controls that should be in place to be considered proactive in its cyber risk management.

The biggest thing that people face and will need to understand is that it's been very inexpensive to use technology for a very long time. We've been very blessed in that regard. Now we're starting to see what you could almost think of as "the tax of using technology" and it's something we must accept. So, doing things like issuing company devices, where we have centralized management through Active Directory, JumpCloud, or other tools is a requirement. Companies must set up command and control over their devices and data. I'm sorry to say it, but organizations must bite the bullet and start issuing devices, managing from a central location, and running a formal cyber risk management program. This is one of the most common hurdles we see but allowing your users to have administrative privileges can undermine all your other security controls.

DANIELLE JANITCH: I always tell my clients that they need to, in closing deals, be able to show in reps and warranties and their service agreements that they do comply with NIST, that they do have regular independent audits. You don't close the deal with the large companies anymore, if you don't do what Zach is saying. There are companies that will provide good guidance to smaller businesses on a relatively cost-effective basis for them. Also, you can often transfer those costs into the cost of your product because it sets you apart from your competitors. You are steps ahead. You give them that feeling of security. At least with my clients, I've seen that by adding a good value product, and then having extra value security protections around it, they close the deal more often.

I think smaller and mid-stage growth technology companies, SaaS-based companies that I work with, are taking it a lot more seriously now and willing to spend those costs. Also, they think about data management. They take less data in, they put more burdens on their clients to make sure their clients are managing the data flows better. And working together, it becomes more of a two-way street, and I trace that directly back to GDPR. Even though GDPR may not impact that deal in the U.S., the mindset and the fear is there now, causing people to be more privacy and security conscious.

ZACH FULLER: Our discussions have changed quite a bit over the last 18, 24 months alone, and it's exactly that — companies are now seeing cybersecurity as a revenue generator and a business enabler, rather than just a cost, because security is setting them apart. They're going after third-party attestations more, and they're demonstrating the benefits of security throughout their sales and marketing language. Cybersecurity the very next thing a large enterprise will look at, after they've evaluated the vendor's service or product. If service or product meets the business objectives, the very next thing they're looking at is the cyber risk that it presents. Nobody wants to get fired for selecting a risky vendor that results in a breach.

DANIELLE JANITCH: For example, SaaS companies, I helped them through sale events and financing. It used to be when I first started that everybody was trying to exploit that something was wrong with the open source code that you were using, and that was used to drive down what the sales price might be once you've signed, and you're moving towards your final close on your transaction. I think security is used that way now too, quite a bit, much more effectively than open source, because the risks are much higher than they are with open source in the real world.

DAVE BOLMAN: That's one of the things we're seeing on the university side, an increased expectation of secure code just from your shared code developers. It's become part of pure science of developing applications that are secure, but also in the last 12 to 24 months, expectations of our graduates having coding skills that are secure as well, has become much higher priority than it would have been five years ago, and I think that's for this reason.

ZACH FULLER: We do a lot of penetration testing on applications. Developers are getting better and better. We see fewer critical and high-risk issues in applications coming out, and they're getting more mature with their Software Development Life Cycle (SDLC). The buzzword today for that increased focus on development security is "DevSecOps". It really just means a mature SDLC process, and we're seeing a lot more emphasis put on that. I think that's an excellent step forward.

DAVE BOLMAN: Over the last 18 months, there's been kind of a new surface contour of attacks. Do a snapshot right now. What are the main reasons or angles that companies and individuals are being attacked?

ZACH FULLER: By far, the main reason companies are getting attacked is due to their failure to commit to building a formal cyber risk management program, then doing the work to get it done.

But as far as attack surfaces go, the human element is always the biggest risk. Oftentimes, it is well-meaning, but unaware employees. We had a company reach out to us when they had about 2,000 machines across multiple offices, encrypted with ransomware. It happened because one of their employees just had to click on an email promising a $100 Amazon gift card and the company had almost no security measures in place. Even when you have strong defenses, your staff can let an attacker right through the back door.

The other thing though, of course, is we see attacks like the Microsoft Exchange hack or SolarWinds hack. This is software that we all know and trust. It's tough to deal with because even with extremely sophisticated security protocols, we still must trust and rely on software from large vendors.

There is a lot happening in corporate espionage. Nation state threat actors are getting people hired in the largest enterprises here in the U.S. and those people are working as developers and in other roles with access to critical systems. I think we're going to see this increase because those attacks are so devastating and give the enemy a significant advantage.

DAVE BOLMAN: Because of the impact of somebody getting access to a large organization's information or network, from databases to transportation infrastructure, you can almost begin to see developers in that area being classified as national security workers in a way you would never have

CONTINUED ON PAGE 26

ZACK FULLER

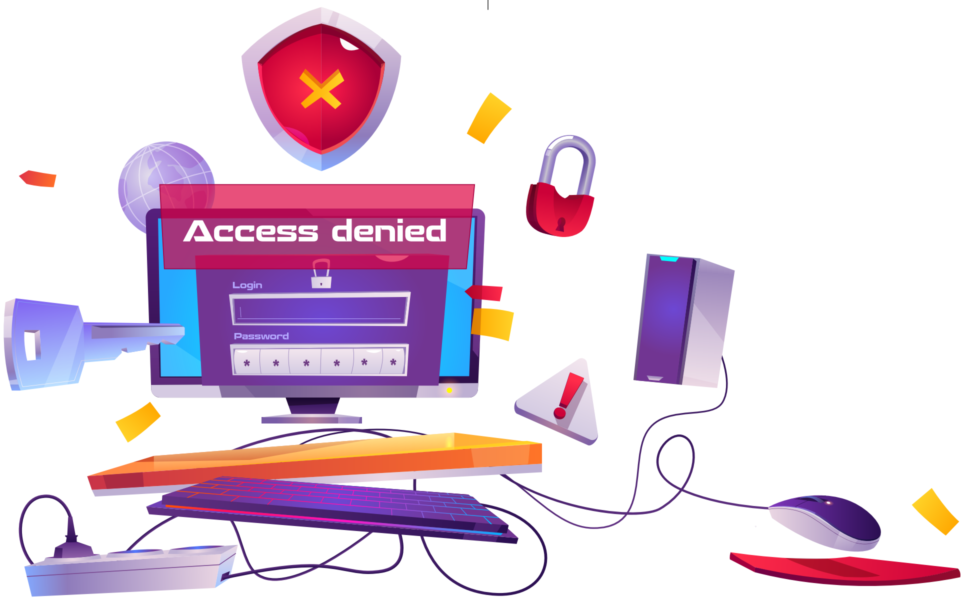
PARTNER, HEAD OF BUSINESS OPERATIONS
Silent Sector

Zach Fuller has been passionate about business and technology ever since he first got kicked out of his grade school's computer class for hacking the network. Since then, Zach has built a variety of businesses across multiple industries. He served as a Green Beret in the US Army, with combat deployments in the Global War on Terror where he received a Bronze Star Medal, Meritorious Service Medal, and other commendations for his actions overseas. He later built a methodology and team which raised over $300 million for a real estate private equity firm, bringing the company to the Inc. 500 list of fastest growing private companies.

Zach is a Certified Ethical Hacker and Founding Partner of Silent Sector, an Expertise-Driven Cybersecurity services firm protecting technology focused mid-market and emerging organizations.

SILENTSECTOR
EXPERTISE-DRIVEN CYBERSECURITY

on behalf of BeachFleischman



DR. DAVID BOLMAN

PROVOST AND CHIEF ACADEMIC OFFICER

University of Advancing Technology (UAT)

Provost Bolman has focused his career upon addressing the profound need within Arizona and the nation for a substantial and diverse creative class workforce. As its longstanding provost Dr. Bolman has built the University of Advancing Technology (UAT) into a unique all-STEM institution that marries the best of traditional small private college learning with the genetics of innovation that come with agile technology organizations. As an educator, he has focused on cultivating a base of technology students and future inventors who are as diverse as the people who ultimately use their creations. As a technologist, he has worked to create a university where the culture of innovation and creation is so regular and celebrated that the goal for each student is to graduate having routinely worked on numerous teams and built again and again complete solutions using the technologies that excite their imagination.

As an advocate for Arizona as a remarkable state where innovation is encouraged in all spaces, including education, Dr. Bolman has grown UAT from a single classroom of 13 students into a STEM private college campus that is unique not only to Arizona but also the country. UAT and its community are dedicated to advancing society through students who learn the tools, techniques, concepts, and responsibilities of applying technology in ways that lift up human society. Dr. Bolman has researched, written and spoken on the nature of technology as a foundational human force and how to successfully lead innovation. He is an alumni Valley Leadership and currently serves as its Past Board Chair. He serves on the Board of Directors for the Arizona Technology Council. He is an alumni of the FBI Citizens Academy and serves on the AZPBS community board.

University of Advancing Technology
UAT
Learn. Experience. Innovate.

CONTINUED FROM PAGE 25

thought before.

ZACH FULLER: Absolutely. The vetting, the reviews, and checks and balances must be there. But even the largest enterprises are still limited on their capacity to vet properly, not to mention a lack of counterintelligence measures. I believe there is a convergence happening between the areas of national intelligence and corporate cybersecurity.

What do we do about it as organizations trying to protect ourselves? We need to make sure that we have, for example, principles of least privilege segmentation across our networks. When somebody gets in the door, we can't give them the keys to the kingdom. We can't allow the attacker to access everything. We must limit what every employee can access and be very vigilant about it. Also, recent attacks show the importance of incident response planning, disaster recovery planning, business continuity planning, all those scenarios that everybody needs to plan for, even though most people hate doing it. This type of planning can be tedious and isn't seen as a revenue driver. Regardless, we must be taking the time to think through those "what ifs" meticulously and document plans of action. For example, we trust the software platform that we're relying on today, but what if that goes down tomorrow?

DANIELLE JANITCH: From a contract negotiation point of view, it used to be that my clients and the larger companies, the Fortune 500 that we've being negotiating with, were focusing on confidentiality and the security of the data. I really feel there's been a shift mainly because of the rise in ransomware, where the focus is not just on security, but also on accessibility. That's the way it tends to be negotiated in the contract language. It goes right back to, what are your data recovery plans? What are your backup plans? If we have a ransomware attack, how quickly can we be back online? How quickly do we have access to our data, how stale is our data going to be based off the incident that's occurred? What types of tests do you have around that?

These really are defining incidents that help you close the deal better. It makes sense to invest upfront in thinking about and building your systems and your software and your products to be able to withstand these issues, so that you can win the sale, because essentially, you get the most security to the client.

DAVE BOLMAN: If you're building a cybersecurity plan, of course, you might get an expert to help, but what are the categories of things they're going to walk you through as you build up your business?

ZACH FULLER: I'll use the NIST Cybersecurity Framework as a popular example. It contains five primary control categories: identify, protect, detect, respond and recover. It takes these five major categories, and then breaks them down into sub-controls, as do other frameworks.

Most of your frameworks out there are going to start with gaining an understanding of what you have, inventory of hardware and software devices, and creating standards on what does and does not go on your company devices, or what your staff is authorized to use and what they're not. You'll get into detection and protection controls which cover a wide range of things, from technical controls to activities like staff awareness training.

Then you're getting into protection. You start to get into different controls like segmentation of your network environments. You don't want to give out the keys to the kingdom just because someone breaches through your perimeter protections.

Later, you'll get into your backup systems, fail overs, all of that. Your incident response plan should be in place in advance, and you should know who needs to be contacted when an abnormal event occurs. You'll have severity levels defined, so you understand how to classify a potential breach and take appropriate action, including contacting everyone who needs to be involved. Also consider your recovery time. Can you fully restore? How long will it take? What are the appropriate back up methods and frequencies?

Of course, what an organization can implement is going to vary drastically based on the size, resources, and technology environment. For smaller organizations, I would recommend looking at the CIS Controls framework to guide you toward proactive security.

DANIELLE JANITCH: I think there are a lot of good publicly available free resources, both in frameworks and how you can operate under them, and then also sample policies. If you need written hardcore policies on how you're going to do data response, you can find some great ones online.

Also make sure this is not something that's isolated to your IT guys. It needs to be throughout the whole organization. The embracing of the framework, the practices, the policies of a company around data security really needs to be at the upper levels of the company. It needs to be an integrated holistic component of the company, from the DNA of the company. That is what I always try to say to my clients.

DAVE BOLMAN: Let's say an organization does reasonable diligence and follows a framework and implements it, they then find themselves subject to attack and some information is compromised. If you do a good job of preparing, how does that affect your liability?

DANIELLE JANITCH: In my experience advising clients on purchasing cyber insurance, because that's where you're going to go first if anything like this happens, is that the policies aren't predictable. You don't want to just buy the cheapest one, and that's where professionals can help. One of the gotchas that some of these cyber policies have is that you have to do all of the things that Zach described.

What happens if you have a cybersecurity incident, and you didn't do everything that Zach just told you should do, and you clicked on that box and said you did? Suddenly that policy is not going to cover you in that incident because you're at fault from the insurance company's perspective.

The other thing is that once you have an incident, you need to engage with counsel immediately, because you want to make sure you have appropriate protections around the investigation. Some of those policies include counsel, so that you'd have a way to work through that. Others, it might be a good idea to have counsel that you worked with while you're pursuing the insurance policy and I do that work quite a bit. Knowing somebody ahead of time and having that be part of your practice in your business model will help you be more prepared for when that event occurs.

It also makes sense to have a relationship

with a firm like Zach's. You can get those through attorneys because we work together, and we know each other.

ZACH FULLER: Perform incident response tabletop exercises at least annually. Quarterly is better. We take kind of a fun approach to the tabletop exercises, role playing with dice, and kind of making a game out of it. When you're role playing, you can throw in realistic scenarios such as a very critical person on your IT team being out on vacation for a week in the mountains with no cell phone reception. What do you do now? Those are the types of questions that you'll need to come up with to create realistic scenarios that test your assumptions for what will work when something out of the ordinary occurs.

I wish there was more education around the use of technology. I'm not saying force it, but I think schools could teach kids network fundamentals, for example.

DANIELLE JANITCH: This information is key to me when I think about cybersecurity and privacy concerns. I feel it is key to provide education about the whole concept of using data to target people, and why the security of your data and the privacy of your data is so important.

DAVE BOLMAN: When I think about Covid in the last 18 months, the surprise I had with cybersecurity was disinformation. We saw AI-driven focused disinformation campaigns that if you don't know what you're looking at or how to look at it, you don't know that it's not real. What I find interesting is I've talked to people who are engaged in it. I said, "No, look, I can show you. I can run an AI application that shows you that this was fake, this was not real information." Their response was along the lines of "I don't believe anything," and that's a strange thing. Culturally we've got to work on is finding that middle ground.

ZACH FULLER: Disinformation is a huge problem. Between the U.S. and our adversaries, we've been conducting psychological operations for hundreds of years. So that aspect has been around for a long time, but you're right about the rate at which it has accelerated.

It's about education, but the real problem is, a lot of people are almost caring less or shutting out information completely. They don't understand the sources of the disinformation problem and are getting such a flood of information that it becomes too much for the mind to process.

I don't know how we're going to combat that, but I think that we must come up with something. Somehow, it's got to be done without restricting certain freedoms. We need a generally accepted media platform or environment that has multiple checks and balances, with the best interests of the audience as the primary focus. People don't understand that just because something gets tweeted 5 million times, doesn't mean it's really that popular on Twitter. I mean, a lot of people that use that platform will see that stuff and believe it, but really, it's just bots created by nation-states working hard to undermine our society.

DAVE BOLMAN: I think a couple of things will help. Education, and probably moving some curriculum earlier in the K-12 system on such things as computer literacy and fundamental Java scripting.

The other thing that I think may emerge in terms of disinformation. Some of our students do innovation projects. They have to build a complete solution, and this is one of those innovation projects I've seen repeating. It could be a new category of application that emerges that people purchase and have on their systems. It runs those kinds of checks, and then much like an antivirus, it updates itself to countermeasure things. But it would just give you an indicator, for example, "this is probably not a real story, this is something that somebody put together for psychological warfare." I think that's a possibility.

DANIELLE JANITCH: You've got this wide-open commercial marketplace where innovations can exist. But then there's the technology and the product that creates the disinformation that also exists. How do we as a government, and I think it has to be at the federal level, and maybe at industry levels within private regulation, build systems to discourage and prohibit inappropriate use of data, and encourage, and grow the beneficial uses of data, and where do we draw the line? What is beneficial versus what isn't beneficial? Those are struggles that I don't think our legal framework has ever had to deal with really in the past. And how are we going to build those regulations? Right now, we haven't, and I think that's going to lead to where we are today. But what should they be, and how will they work? It's a tough question.

ZACH FULLER: Do we want the government regulating the information we consume? Whose job is it to regulate that and control the disinformation in our society? There are a lot of deep questions to be answered about AI-driven platforms designed to identify truth and deception. It's outstanding that we have these technologies. But as we know, AI has its own bias, and bias can be built right into the software. We must be conscious of all of that and make some decisions quickly. We're in a bit of a post-truth society at this point.

DAVE BOLMAN: I do think this is an interesting problem that it's going to take time for people to sort out, and it will create new social norms and new laws. The era of a certain number of news channels that are finite and highly protected, because that's how balancing democracy happens, is over. We're in a very different place where we have vast sources of news, and the approaches, the former expectations of professionalism, they just don't apply. Similarly, on the warfare side, I think it's very interesting that we have very few moments of boots on the ground conflict that we deal with. Yet, what we do deal with in terms of national security is cyber. I'm curious to see in the next five, 10, 15 years, if increasingly the federal government's posture is to treat digital incursions as a form of an act of war. And it won't be responded to with a bomb but be responded to very aggressively and normed out. Are we going to take those systems down, just as you would if somebody bombed a power plant?

ZACH FULLER: The problem in the world of cybersecurity and cybercrime is that the only people who win are the people who have nothing to lose. We're going against cyber criminals, cybercrime rings, and nation states that have far less than we do. So, we have everything to lose. By attacking back and taking down their systems, we really have nothing to gain. We can digitally "blow up" a bunch of their virtual machines, then they just spin up new ones and are back at it. There must be a physical response to cybercrime, but attribution is always a problem.

The cybersecurity industry must find ways to become better at delivering cybersecurity

CONTINUED ON PAGE 28

MAKE
GRANDMA
PROUD
Graduate in <3 years
University of Advancing Technology
UAT
Learn. Experience. Innovate.

DANIELLE JANITCH

ATTORNEY

Osborn Maledon

Danielle Janitch focuses her practice on representing a wide variety of clients in cybersecurity, data protection, privacy, intellectual property and technology-related matters such as developing and managing data protection plans, licensing, distribution, procurement and trademark prosecution. In addition, Danielle has experience with construction contracts and outside general counsel services.

Danielle has been recognized by the Phoenix Business Journal as one of the top Forty under 40, as well as named a Rising Star by Southwest Super Lawyers in the area of Intellectual Property. She regularly moderates and speaks at programs concerning cybersecurity and intellectual property.

Before joining Osborn Maledon, Danielle was a judicial clerk for Judge Roslyn O. Silver of the U.S. District Court, District of Arizona, attended Stanford Law School, earned a Bachelor of Science in Chemistry and a Bachelor of Science in Biology from the Massachusetts Institute of Technology and served as an officer in the United States Army.

OSBORN MALEDON

CONTINUED FROM PAGE 27

services. We need less emphasis on tools and technology, and more on professionals implementing the fundamental practices that many thousands of companies are still missing. It's really the basics that companies are missing, not a shortage of tech.

As an industry, we should be taking our lessons from the U.S. military's approach to counterterrorism and asymmetrical warfare. We're in a war of attrition that will be a tremendous waste of resources over the long term. Right now, companies around the world are spending about $1.8 million per minute responding to cyber-attacks.

DANIELLE JANITCH: These things are happening globally, and I would like to see us globally have more summits and communications, and coordinated plans across the free world on what are our practices? What are our policies? How are we going to regulate? How does data transfer?

And then what are the securities and the access rights of government? Who knows how that's going to work? And how do we react with bad actors as well? I think we need to have a global initiative that is focusing more on this. In my practice I deal with data transfer issues, which kind of touches on this. It's a similar concept, and we need to make it easier for business to get their data in and out of Europe, and vice versa. That's something that must start happening. We must come up with policies and procedures to allow that to happen more without as much uncertainty as right now.

DAVE BOLMAN: Are you seeing new technologies, like blockchain, being used more and more often to secure information motion between businesses and countries?

ZACH FULLER: Blockchain has a lot of great uses, but I don't see it as a game changer for cybersecurity. We've already had various levels of encryption for a long time. It's more about how that data is handled and understanding that a lot of organizations don't have visibility through things like architecture diagrams and data flow diagrams. Companies often don't understand where their data exists, when it goes there, who's responsible for it, the security controls around every point along its path. And so, I think most of organizational cybersecurity comes down to implementing the basics. That's where we see the greatest need.

Most of the cyber attacks occurring today are simply due to the lack of fundamentals. Over 80% of cyber attacks are financially driven. The rest is cyber warfare, hacktivism, things like that. But when attacks are financially driven, it is really about the economics. If the economics no longer makes sense for the attacker, then they'll move on to something else.

DAVE BOLMAN: If you had a roll forward like five years from now, what do you think the landscape looks like in terms of the way businesses are interacting with cyber and intrusions attacks?

DANIELLE JANITCH: There's going to be a lot less data collection by business. I see that now. It used to be my clients collected every bit of data they could collect and store because they didn't know what to do with it. You never thought about the risks associated with that data.

And then GDPR came into play. And then, the rise of ransomware concerns came into play, and really, my clients now do strategically think about, what data do I need? I only want to take as much data as I need. I don't want to take more. And if I am going to take more, what are the cyber costs with it? I think we're going to continue to see a much more intelligent framework around data collection from U.S.-based businesses than has been in our past.

ZACH FULLER: Cybersecurity will become more of a core function and seen in terms of business enablement. We're starting to shift that way with SaaS companies and system integrators, who are using cybersecurity as a competitive advantage. But I think cybersecurity will start to have a better seat at the table. Right now, chief information security officers have an executive team seat, but oftentimes they're kind of shunned. I think that'll start to shift. I think business leaders will be more aware that cyber risk management is a requirement to do business. It's not optional anymore.

We could use some sort of agreement on a framework that is recognized and accepted by companies of all types. We currently have companies with limited resources that are forced to chase one compliance requirement to the next. They're more worried about maintaining compliance requirements than cybersecurity. Just because you're compliant, doesn't mean you're secure. You could be 100% compliant and full of security holes.

Hopefully, as a country, we start to understand that we need to adopt more holistic practices and put less focus on the one-off types of data that we're worried about protecting. When we properly protect the organization with a focus on cybersecurity, by nature, the compliance regulated data is going to be highly secure.

DANIELLE JANITCH: I hope in the next five to 10 years we have a much more standardized system of control and regulation. It really needs to be beyond the United States. It needs to be a global strategy. And maybe it can't be the whole world, but at least the portions of the world that we connect with most frequently need to have a consolidated strategy, because data flow is so important to business today. With these disconnects, I have clients that really have trouble. You must build one set of infrastructures to store data for Europe, a different one for the United States. It's costly, it's expensive. Why can't we figure this out and have a consolidated system? I think economic pressures will be honest, and hopefully, politics will be able to carry that through.

DAVE BOLMAN: In five to 10 years, I do think that organizationally, your cyber department will be mature the way your HR departments are, and your financial departments are. When you're going to do the pie chart of your business, you're going to have a certain cost that you're going to benchmark against standards associated with doing this work, and it'll be just part of the practices, they'll be rules and norms. In five years, I think that's going to be locked in where we just have our heads wrapped around it.

I don't know where it ends, but I think a resolution is going to have to come in areas like disinformation and attacks and infrastructure. One of the interesting things that's happened out of Covid is for the first time in Europe and U.S., and I'm sure elsewhere, we're beginning to experience disruptions in this norm of how goods and information and products flow in an internet era. Over the last 10, 20 years, we've had a new set of expectations in terms of how things are delivered to us, and it's been amazing, and it's driven a lot of economic growth.

Now in the last year or so, we're beginning to see for example, a meatpacking supply chain went down, or we've had a disruption in flight systems, or other instances of service interruption; the result of that going to probably be hardening and laws that are created in response to that. I think that rises to the level of the things that people used to talk about at DEFCON security conferences as a hypothetical in 2005, are now trickling to a point we're like, "Yeah, every year, I'm seeing a half dozen of these, and it can't grow to that." I expect we'll probably see some event that will trigger it over to a "no, we can't do this anymore." And it will be a major push by governments to say how we're going to address it.

DANIELLE JANITCH: We are emerging into what will become more of the golden era of what I do. Managing and preparing your business for cybersecurity and privacy issues is absolutely something you must do well. If you don't do it properly, it's going to have an impact on the valuation of the business, it's going to have an impact on your ability to grow, get funding, and then eventually sell.

Give cybersecurity the respect it deserves, give it the resources it deserves, engage with the industry professionals that you need to engage with, use the free industry resources that are available. And it needs to be the part of your business from the ground up, from the moment of founding through the final sale.

ZACH FULLER: The main thing business leaders need to do is decide to implement a cyber risk management program and get started. Cybersecurity is not about perfection because nothing is 100% secure. It's much more about making yourself a harder target than others around you. No matter what size organization you are, there are things you can put in place today that will reduce risk. When you start doing those activities that you're not already doing and putting some basic controls in place, you're already making yourself a harder target for criminals.

There are tools and technologies that help in some area, but it really comes down to the thought process and strategy first, then the technical implementation. The good news is that you probably don't have to go out and buy a lot of new tools and software. We find that most organizations can be highly secure with the technologies they're already using. When they work with professionals and take the time to think through their processes, get their policies in place, and build a security program with one of these major frameworks, they find that they sleep better at night while adding tremendous value to the company. Implementing a formal cyber risk management program is really what must be done for all organizations at this point because the attacks are very real. They're not slowing down.

DAVE BOLMAN: From a workforce development perspective, if you've got anyone looking at future careers, look at cyber, and maybe look at it a bit differently. There are more opportunities such as in AI, cloud technologies and IoT. Other aspects that aren't necessarily pure on tech are equally as important in cyber, and it's worth studying and learning. Cyber right now feels more like not specifically the tech area, but its own business that requires all the same kind of thinking. It opens it up to far more people than in the past. And frankly, that's what's needed in the next five or 10 years to make a difference and address some of the challenges we can talk about.