ADVERTISING SUPPLEMENT TO THE PHOENIX BUSINESS JOURNAL

CYBERSECURITY

Table of Experts

TABLE OF EXPERTS PANELISTS

ERIC CRAINE
Sr. VP and Manager of Treasury Management
UMB Bank

DANIELLE JANITCH
Partner
Osborn Maledon

JAMES P. MELENDRES
Partner
Snell & Wilmer

MARK PRIBISH
VP & ID Theft Practice Leader
Merchants Information Solutions

MODERATOR

DR. DAVID BOLMAN
Provost
University of Advanced Technology

Sponsored by

SmartIDentity FOR BUSINESS™ | OSBORN MALEDON | Snell & Wilmer LAW OFFICES | UMB®

DANIELLE JANITCH

Partner | **Osborn Maledon**

Q: What are the key considerations in a breach response plan??

A: First, figure out the level of detail. Does your organization require a carefully detailed, step-by-step plan or is it more nimble, where a framework that you can follow is more appropriate. To assist with this determination, focus on identifying the key risk points for your organization.

Second, identify when to invoke the plan and who gets called when. Remember engaging your attorney early, to protect the investigation with attorney-client privilege. This is also the time to call your insurance person because you want to determine early on if you have coverage for the situation.

Third, you need to identify the lines of communication. This includes identifying the individual responsible for approving all messages to the public, organization, government, and impacted third parties.

Then finally, there needs to be a remediation, an after-action review. I recommend reviewing the NIST Special Publication 800-61, the Computer Security Incident Handling Guide, which is available free online. It is a great resource for companies on how to organize their response plan.

Danielle Janitch is a partner with the Phoenix law firm of Osborn Maledon, focusing on intellectual property, corporate governance, growth capital financing and mergers and acquisitions. Danielle graduated from MIT with Chemistry and Biology degrees before joining the Army. After her time in the service, she attended law school and then started her legal career at Osborn Maledon.

The average cybersecurity bill for a small business that experiences an attack is nearly $50,000 (Kapersky Lab study, 2015). For medium and large companies that number skyrockets to hundreds of thousands and even millions. How a business handles a cyber breach is critical to mitigating both the organization's risk and their costs.

Area cybersecurity experts from law and insurance shared their insights on planning for a breach during a recent discussion hosted by the Phoenix Business Journal. Dr. David Bolman, Provost for the University of Advanced Technology moderated the panel. As its long standing 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. He is an alumni Valley Leadership and currently serves as its Board President. He is also an alumni of the FBI Citizens Academy and serves on the AZPBS community board.

David Bolman: Earlier we were talking about was how much the cyber topic has evolved and accelerated over the last ten or fifteen years. Let's start off with that. In the last ten years or so, what are the major things you've seen in terms of the trends of cybersecurity and how it's affected businesses?

Mark Pribish: I'm 27 years in insurance and risk, and I've been very involved in the cyber-insurance business. You have to look at the reality of cybersecurity, and IT and hacking are the sizzle that makes the headlines, but let me tell you about the reality.

Trendmicro, a multi-billion dollar information technology company, came out with a report that said only 25% of all of the data breaches that we hear about and read about are related to IT and hacking. Think about it, it's in their best interest to say all these breaches are related to IT. 75% of all these data breaches are people. Current and former employees, contractors and vendors, along with organized crime and social engineering. To level set the discussion on cybersecurity, you have to look at the reality - and the reality of all these data breaches are people.

Danielle Janitch: I think that's a really good point. The Verizon 2016 data breach investigation report had a really interesting statistic as well that ties in with that. Over 60% of data breaches are due simply to failures in password security. Either the password is the default, nobody bothered to change it, the password is easily guessable, 1234, or people have the password posted right next to their computer. Those things are simple, very low cost, effective processes that could be put in place to help bring down over 60% of the incidents that have been detected.

James Melendres: I co-chair the practice at Snell & Wilmer. Before that I worked at the Department of Justice and National Cyber Investigative Joint Task Force where I helped lead DOJ's cyber program. FBI Director Comey has said, and I think that this bears repeating, there are two types of companies in the United States: Those companies that have been hacked, and those companies that don't yet know they've been hacked.

This gets to the preparation costs versus data breach costs, so what I've seen since moving into private practice and counseling companies is that it does pay to make an investment on the front end. To think about what type of cyber-preparedness and regulatory compliance you should undertake in advance of a breach, not just because it will help harden your networks and lessen the chance or severity of a breach, but also because in the event of a breach, your liability will be reduced if you've taken the steps that various regulators are requesting.

David Bolman: Let's dig in a little bit. In terms of breaches, if you were to give guidance to somebody or an organization on how to prepare for a breach, what would you tell them?

James Melendres: I think there are several things that companies should do on the front end. The first one is you should have an incident response plan in place before a breach occurs. Think about an incident response plan as effectively a fire drill type document that outlines what individuals are going to be responsible for what actions in the event of a breach, how notifications are going to occur, and even thinking through in advance the pros and cons of voluntarily notifying law enforcement about the fact that you've suffered an intrusion. I think that those steps on the front end go a long way to helping companies nimbly and quickly respond to data breaches.

Another key piece is engaging with outside counsel, both for advice in terms of preparedness and regulatory compliance, but also when there is a breach, ensuring that outside counsel is overseeing the response in anticipation of any litigation, will ensure that the attorney-client privilege attaches, and that the work-product doctrine protection attaches. Having that team in place along with forensic examiners goes a long way to helping respond when there is a data breach or cyber

incident.

Mark Pribish: To validate what was just said, no CEO or CIO has ever been fired because they've experienced a hacking or data breach event. They've been fired, and I use the Target CEO and CIO as an example, because of their failed management response to that breach event.

Danielle Janitch: Picking up what James was saying, any organization, no matter how small or large, can affordably put into place a good breach response plan. It shouldn't be seen as this extremely expensive thing that you need to hire outside experts for, and that is beyond the capabilities of startup and early growth companies. The federal government provides a lot of resources online. There are many good websites that outline exactly what should be in your breach response plan. There are also a lot of non-profit organizations that provide free resources to help businesses with their own internal disaster planning. Websites with great resources include www.sans.org, www.cert.org, and nist.gov. The nist.gov site includes a very useful special publication, SP 800-61., concerning data breach response plans. Also, www.experian.com/assets/data-breach/brochures/response-guide.pdf.

David Bolman: Let's go on that a little bit, because from a business perspective, if you are inside the field there's a lot of terminology and there's a lot of knowledge, but this is a very new thing. Five years ago we weren't having this conversation, maybe not even two or three years ago. If you had to break down guidance to an organization, where would you go to get a brief response plan built? How would you start?

James Melendres: At Snell & Wilmer as part of our cyber services, we offer data breach response plans. As Danielle mentioned, there are a lot of resources that are available. The fact of the matter is that one size does not fit all. There are nuances. There are different assets that companies will need to protect depending on the industry that they're a part of, depending on their business model, etc.

Eric Craine: It is critical that companies think about it holistically. Depending on the type of intrusion you may need your HR advisor or group of advisors to be a part of that. Definitely legal being a piece of that, IT being a piece of it.

A lot of our conversations with clients center around trying to convince them of the actual risk and to raise awareness beyond a headline, to really put measures in place and best practices in place. Part of it is a technology fix, but I am a huge believer that a lot of it stems from management - the education, management and oversight practices that the business has in place. If they're not a mature business, then that's something that they're probably not exposed to.

David Bolman: For a reader who may not come into this as knowledgeable, could you outline what are the different things that a business is exposed to. I think everyone gets a sense of financial records, but it's more than that.

Mark Pribish: Eric mentioned "holistic." Couldn't be a better word. In the old days, you had the IT guy who was responsible for information security. Information security doesn't work anymore. It's now information security and governance. Information security and governance relates to a holistic view because it's not just an IT event, it's an HR event because there of current and former employee information. It's a marketing and sales event because of current and former customer information. It's physical plant event, but it's not just the home office or the branch office, it's all the people working remotely.

James Melendres: Let me pick up on that and make two points. One, on the oversight and management question, there's a statistic that today 48% of boards have specialized security committees that are responsible for overseeing cyber risk management, and have a responsibility to the company to make sure that the board understands what the particular cyber risks are that need to be addressed and manage these risks on an ongoing basis.

Now, to the broader question that you asked, what are the different types of threats, what is the type of information that is most vulnerable; as you mentioned, financial records. For hospital systems and healthcare providers , medical records. That is particularly rich data. It's highly regulated. They have HIPAA compliance issues.

Mark Pribish: Financial aid to colleges and universities.

Danielle Janitch: Educational data.

James Melendres: More generally speaking, you have what is referred to as personally identifiable information which is basically a name with some other identifying piece of information.

CONTINUED ON PAGE 30

CONTINUED FROM PAGE 29

In addition to those types of records, what we've also seen over the last several years and what has made headlines is the theft of proprietary information, of confidential business information from companies.

It's not just customer information or patient information, or personally identifiable information, but it is truly a company's jewels.

Danielle Janitch: I'd like to pick up on that. One of the things that I've noticed with many of my clients is that there has not been a review of the information shared with vendors and if that information really needs to be shared. Business is largely operating on information sharing as it has been operating over the past ten to fifteen years. There has not been a systematic review of whether changes should be implemented to mitigate risk of data breaches by simply not sharing as much information as historically provided. There is a lot of extraneous information that falls into the categories that James just outlined that is often sent or provided reasonably easy access to vendors when the vendor has no real need to see it. Both vendors and their clients need to focus more on this issue. One very simple way to mitigate the risk of a breach is simply not sharing high risk data when it is not necessary for the business deal.

David Bolman: I was thinking earlier when we were talking about what a high percentage of breaches related to people. Can you give us some guidance on what people could do to help change that?

Danielle Janitch: I think solving the problem (of human breaches) starts with training that comes from the top down. It has to be coming from the CEO and the entire C-suite, not just from the information technology department.

There are a lot of fun ways that you can train people today that are a lot more interactive than making them go to an hour meeting and listen to, "Turn your computer off." You can do phishing expeditions to see who gets caught and who doesn't get caught. Get employees involved in competitions to learn and help each other and educate each other. In addition, I think that you should look at your systems. Why don't employees turn their computer off every night when they go home? Is it because it takes 25 minutes to log back in? Because you have to put five different passwords in and the system is too slow to come up?

On the second prong, you have to look at my point about what data is being shared, and how are you sharing it. A lot of these companies are sending data out that vendors that don't need.

They should be thinking more practically on the front end about what am I doing with this vendor? What information am I sharing with them, and how can I manage the flow of information? Maybe we don't send it by email. Maybe we send it by other secure mechanisms that we've vetted and we manage.

James Melendres: In addition to locking down vendor agreements, there are some concrete steps that companies should take, and we advise companies to take, based on the guidance provided by the Federal Trade Commission and what the FTC has done recently in terms of cyber-related enforcement activity. These are some basic best practices that should be instituted, and that go a long way to addressing some of the human factors.

David Bolman: Let's say you are an emerging company. What are the short list of steps you can do, that are within your resource framework that are going to protect you as much as anybody can hope to be protected?

Danielle Janitch: First off, you have to identify who's going to be on their cyber task force. As a small company, you probably won't have a lawyer in house, so you should retain counsel that you can call. It doesn't mean that you're spending money on them until an incident occurs, but you definitely need to have somebody in your pocket.

David Bolman: How many law firms have cyber units?

Danielle Janitch: The last 5 years has seen exponential growth. I think every law firm of significant size has created a cyber security unit.

James Melendres: At Snell & Wilmer, we have a dedicated Cybersecurity, Data Protection and Privacy Practice that I co-chair. We have ten to twelve attorneys focusing on those areas day in and day out. In addition to providing cyber preparedness, data breach incident response, and post attack litigation services. We are responding to a need for growth companies, small companies to have outside counsel that can function as in house counsel to bounce ideas off of, and to think through what

a response plan should look like.

David Bolman: We cut you off half way down your list of things. I want to make sure we get back to the rest of your stuff.

Danielle Janitch: I think that's the way I always train my earlier growth stage companies on how to think about this. It's really nothing new. It's just simple disaster recovery. When I was in the army, there were four points that you have to go through when you have a disaster. You have to mitigate in advance, think about how to decrease risk, what can you do on the front end, then you have to prepare. That's your disaster response plan. Then you've got to respond when it happens.

That's implementing the plan, getting your advisors in the room, sitting down and working together. Then afterwards, you evaluate what you did - What went wrong? What could you do better? What new controls should you put in place? And the cycle just repeats itself.

Mark Pribish: I think that the big lesson in this especially for smaller to mid-size businesses, is recognizing that this is not their space. You encounter an area that is not your space, you bring in an expert. I've seen great programs in some law firms. I've seen great programs in some accounting and advisory firms as well. To help then again think holistically about everything that's there, the financial piece, the human resources piece, the IT piece.

James Melendres: Having counsel who is familiar with how the federal government internally is responding to these threats is also important. As I mentioned earlier, one question companies will face when they suffer a data breach is whether or not they should voluntarily disclose it to law enforcement.

There are pros and cons to doing it. The pro is the FBI can offer insight about whether or not your breach is part of larger systematic campaign.

It can be advantageous to victim companies to cooperate with the FBI because of the insight that they may be able to gain. At the end of the day there may be no better way to deter further attacks by holding perpetrators responsible in a court of law.

Having said that, there are also cons. One is companies, for many reasons, do not want to invite the FBI into their networks. There's concerns about whether it's going to waive privilege, and expose trade secrets.

There's also reputational damage that can occur. It's a nuanced calculation.

Mark Pribish: Contacting legal counsel is huge. There have been actual experiences with businesses and organization who experience a data breach event, where they thought they had a breach event, but they didn't. Based on the state breach notification law; because that lost data was encrypted, they didn't have to report it, but they did. Once you report it, now you have to notify. You have to call your legal counsel, in house, outside counsel. They will help direct and guide you on whether or not you actually had a breach. Going back to what James said, compromising confidentiality is huge.

The small to medium size business market place, those are the companies, when you look at mitigating risk, that should have legal counsel. They should have an accountant or CPA. They should have business insurance. They all mitigate risk.

Danielle Janitch: The point is that it's going to happen to you if you're a smaller or midsize business. What have you done today to prepare for it so that when it does happen your exposure is protected through insurance, and mitigated through taking the necessary preventative steps?

David Bolman: I think that a lot of people, when they think about fraud, they first think about their wallets. We hear a lot about that. Eric, would you talk to us a little bit about what you're doing in banking to secure financial transactions?

Eric Craine: According to a 2016 survey of the Association of the Financial Professionals, 62 % of companies were subject to fraud during the period of the survey. Again, it's back to our point of it's not if, but when a breach will happen. 75% of the over 600 companies surveyed, experienced a fraud attempt through check fraud.

The incidents of wire fraud, which is typically a very safe mechanism for payments, doubled from 14% - 27%.

The major eye popper (from the survey), is how much it costs when this happens to a business. The average loss reported was approximately $20,000. That's the average. That's the hard dollar cost, but there are soft dollar costs as well.

Mark Pribish: Business Email Compromise (BEC), that's the really big hot trend where someone has infiltrated the business's email and it looks like it's coming from the CEO and it's being sent to the Director of Finance or the CFO. They're saying we need a wire transfer to ABC company. What experience have you seen with your business accounts?

Eric Craine: We definitely see that. That is one of the drivers of that wire fraud doubling. You have exactly that. You've got an email that goes out and laundering that happens. We've seen very creative fraudsters in the sense that they're monitoring an individual's email, the way that individual phrases emails, salutations, those type of things. They watch for that executive

CONTINUED ON PAGE 32

ERIC CRAINE

Sr. VP and Mgr. of Treasury Management | **UMB Bank**

Q: How has the mobile and digital revolution changed your approach to banking?

A: The sheer volume of information and access points for the data stands out as a big game changer. You don't have to look any further than the palm of your hand to get access to your banking information or stock prices and news. The balance that our business seeks to strike is getting that information to clients with speed and putting it on rails that are secure, reliable and consistent. Some of the methods we use are new, related to technology and the digital space, and some methods are making sure we have comprehensive solutions in place and embedded in the business.

Q: How are disruptors in the finance technology space impacting fraud and risk? Fraud is one of the top concerns we hear voiced among business owners.

A: Disruptors in the technology space are using biometrics, anomaly tracking and predictive modeling to counter fraudster activity. Much of the technology is emerging, but it is promising to see how innovative and effective it is fighting fraudulent efforts.

Eric Craine joined UMB Bank in 2005. In his current role as senior vice president and manager of treasury management, he leads the market strategy and business development efforts of UMB's treasury solutions division in Colorado, Arizona and Texas. He provides leadership for a team of treasury and commercial card professionals who serve as advisors for public and private companies, nonprofits and government agencies. Eric is experienced with enterprise-wide initiatives and change leadership related to workforce development, sales strategy and customer experience.

BY THE NUMBERS

81.6 Billion – Projected amount businesses worldwide will spend in 2016 to prevent data breaches from happening (2016 Gartner Research)

60% - percent of attacks carried out by people with access to the organizations' systems. Attacks are usually an inside job. (IBM 2016 Cybersecurity Index Report)

63% - percent of data breaches attributed to weak, default or stolen passwords (Verizon DBIR report, 2015)

77% - percent of organizations that experienced either an attempt or were victims of check fraud (2016 Association for Financial Professionals Payments Fraud Survey)

JAMES P. MELENDRES

Partner | **Snell & Wilmer**

Cyberattacks, data breaches and network intrusions are on the rise and continue to cost companies of all shapes and sizes millions of dollars every year. According to just one study, the estimated cost for data breaches incurred by companies will rise to a staggering $2.1 trillion globally by 2019—almost quadrupling costs suffered by companies from 2015 alone. In response, boards of directors, management, regulators and law enforcement agencies are focused on identifying and mitigating cybersecurity risks, including the deployment of malware, digital espionage, unauthorized insider access, distributed denial of service (DDoS) attacks, cyber extortion and ransomware threats.

Snell & Wilmer is uniquely positioned to advise clients in preparing for and responding to data breach and cyber incidents, leading data breach/cyber incident response efforts, and handling resulting litigation or regulatory enforcement actions. The firm's Cybersecurity, Data Protection, and Privacy practice is comprehensive and is specifically designed to assist clients in five core areas:

1. Cybersecurity preparedness and regulatory compliance
2. Data breach/cyber incident response
3. Post-incident regulatory enforcement & private litigation
4. Law enforcement liaison services
5. Privacy counseling

James Melendres is co-chair of the Cybersecurity, Data Protection, and Privacy practice and co-chair of the White Collar Defense and Investigations practice. He focuses on cybersecurity incident preparation and emergency response, related regulatory compliance and civil litigation as well as white collar criminal defense and government investigations. Drawing on his extensive experience as a former federal prosecutor, James also focuses his private practice on representing companies in high stakes civil litigation and advising clients on crisis and risk management.

CONTINUED FROM PAGE 31

to be out of the office on a business trip, some extended time out of the office, whatever it is. When they're least available an associate gets an email from the CEO or someone high ranking, and in an effort to try to please and deliver, they skip some protocols that are in place to verify where that email is coming from. Once they do that, press the button, the wire is out the door. You can't go back.

James Melendres: One issue that we've seen come up with this type of BEC threat is that manner of the cyber policies would not cover that loss because there is a voluntariness to the transfer of the funds. There are insurance products coming online that would cover this BEC compromise. It is an example of the evolving nature of these threats. I believe the projections are in the billions for BEC related loss going forward.

David Bolman: You're talking about business email fraud. Have you seen some organizations that have done a very good job of navigating that both from a policy training and from an IT perspective?

Eric Craine: I used the word holistic earlier. I think that's definitely the best approach. It involves more than the IT guy of a company. It's more than just locking our work stations as we leave. Many clients that think through this in a table top exercise. They're thinking through scenarios of what is going to happen. As a banker, I would like one of the first phone calls to be to me because we can lock down the account. We can help you assess the data as well.

The best practices are those that are well developed. The company that has a very mature business process. They're thinking through as we're doing transactions, whether it's wires, whether it's checks, whatever that is, they have a very developed process for receiving those transactions.

There's also a spirit of empowerment among the associates to question things. To say, "I just don't feel like this is right," and escalate that concern to their supervisor and manager.

David Bolman: If I heard you correctly, what you're suggesting is that rather than doing a PowerPoint deck of here's our protocol, key players get around the table and discuss scenarios.

Danielle Janitch: Absolutely. It's important that the discussion is a little bit of free-form but it's also guided and facilitated. You don't want to necessarily have the group think and process during the table talk exercise. You want to shock the group as they're thinking through things to help them think of different ways to respond.

James Melendres: What you find is when you run through simulations, shock the participants, you will expose the flaws with the plan, and where there are areas of improvement. Continually updating that plan through these types of hypothetical scenarios is a critically important piece of preparedness. Another risk, that we're seeing a lot of right now, is that of cyber extortion and ransomware.

David Bolman: Describe what that is. Not many people know what that is yet.

James Melendres: Ransomware is a form of malware that in the past would encrypt a standalone machine, and more recently has encrypted entire networks and their backups. Effectively what it does is you come into your office in the morning and you have a flash on your screen (like Cryptolocker) that says you have 24 or 48 hours to pay a ransom as a Bitcoin request. If you do not pay the ransom, we will not return the decryption key, so you are effectively locked out of all of your data.

There are particular industries that have been hit really hard with ransomware. Healthcare and hospital systems, because the data that they operate in is patient data, and so there are literally lives on the line if the hospital or healthcare system is unable to access its data, have been looked at as easy marks. The question about whether or not to pay that ransom, whether or not to involve law enforcement, what preventative steps you should take to try and reduce the chances of a ransomware attack, are all issues that companies should be thinking about at the front end

David Bolman: In cases where they are paid, do they get the information back or is it just a further extortion?

Mark Pribish: Just because a business pays the ransom, it doesn't mean the malware will be released. Sometimes they come back within 24 hours and say pay more. Other times they release it, and everything is good. Also, just because they released it, it doesn't mean the malware has been completely removed. The FBI says back up is a solution - multiple back-ups, multiple cloud security providers, multiple server back-ups, even hard copy back-up is the sure fire answer to support an immediate response to patient care, for example. The biggest challenge with ransomware is when you pay that ransom, it doesn't guarantee a thing.

David Bolman: James, you mentioned Bitcoin. If you're outside of this space you may not know what that is. Can you speak to what it is and why it is used?

James Melendres: It's a form of virtual currency that exists entirely online. It floats like national currencies do and it is redeemable for cash. It's believed to be an untraceable cryptocurrency. It actually is not. It's very difficult to trace, but the belief that it is untraceable has really been the engine that's driven ransomware and cyber extortion.

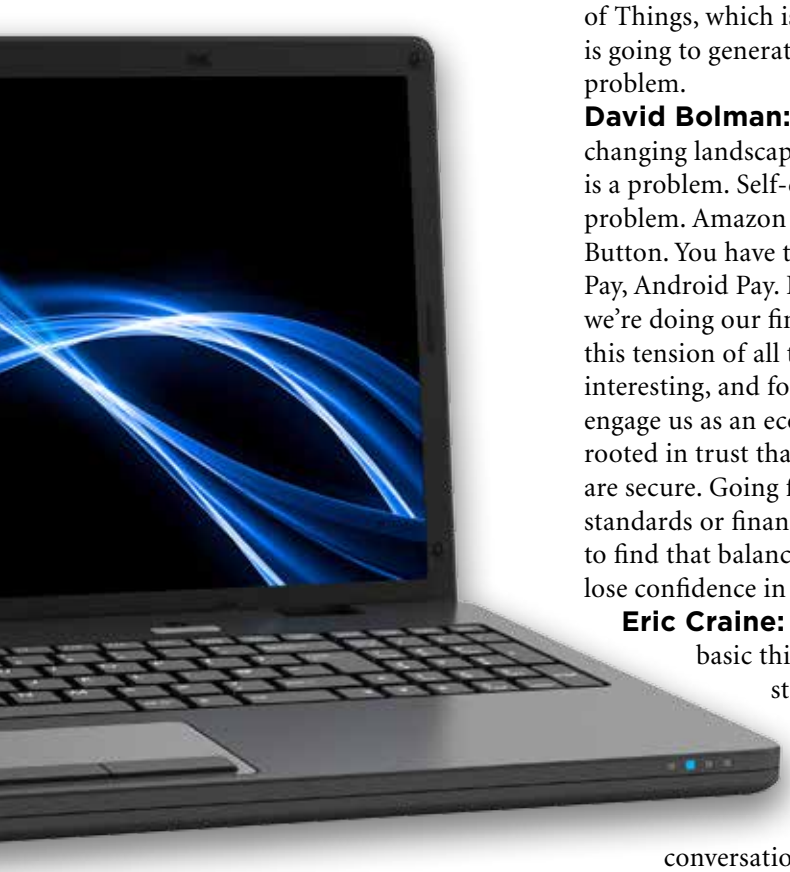
David Bolman: Talk a little about what you see in the next 12 to 24 months that people should be aware of, planning for because it's more complex than it used to be.

Mark Pribish: There's a new phrase

"breach fatigue", describing that consumers and businesses are so sick and tired of the headlines, dealing with ID theft and data breach that they are ignoring the problem. In the next 12 to 24 months, I think there's going to be a push for more leadership, more oversight and more employee education.

David Bolman: In the first 5 to 10 years I was involved with space, everybody who sat at a table like this was an IT professional, but here we are right now... so that suggests that the structure of future response as formation and design needs to look different to be prepared. How would you build it?

Mark Pribish: In a larger organization it's an information security and governance committee. That committee has department representation from IT, HR, marketing and sales, physical security and information security - the holistic approach that Eric referred to. Every company, especially the small to medium size, needs an information security policy. According to the National Cybersecurity Alliance, 83% of businesses do not have an information security policy in place. It should be in writing and reviewed by every employee. Every employee should sign that they've reviewed it, agree with it and will support it.



Danielle Janitch: Over the next 12 months, I think that number (of businesses without an information security policy) is going to decrease dramatically because it's a contractual obligation now with their key vendors.

In the small and mid-sized market, because of their relationships with larger companies, which have adopted more stringent security processes for their vendors, it is finally putting market pressure on small to mid-sized businesses to actually build the type of team that Mark was talking about. As advisors, we could not get them to devote their resources to it until they had the commercial pressure to do so.

James Melendres: Another change I expect we are going to see, and one that we're thinking about at Snell & Wilmer because our clients are coming to us about it, has to do with the intersection of the Internet of Things and product liability. Just thinking through the fact that these medical devices are all networked. A pacemaker is now networked and it can either be an entry point into a hospital network or it can be the target of some intruder who has entered into the hospital's IT space. That is just one example in the healthcare space. If you think about automobiles, driverless cars - all of these network devices and the Internet of Things, which is only going to grow, is going to generate an entirely new problem.

David Bolman: This is a rapidly changing landscape. Internet of Things is a problem. Self-driving cars is a problem. Amazon is selling the Dash Button. You have things like Apple Pay, Android Pay. It's changed the way we're doing our finances. You have this tension of all these things that are interesting, and forward thinking, and engage us as an economy. They're all rooted in trust that the transactions are secure. Going forward, what legal standards or financial tools are needed to find that balance where we just don't lose confidence in this technology?

Eric Craine: There are some very basic things from a financial standpoint that businesses should be using. Although I am still surprised that a lot of our conversations center around convincing the client of the risk.

Positive Pay is a service we ask all of our clients to have. It protects customers by allowing them to see we've issued a check for this amount to this payee. We validate on the back end that it happens. ACH filters is another way of guaranteeing that the payment you're sending out is going to the right party for the right amount, and is clearing on a timely basis. In some ways, these are not new products. Again, it is raising the awareness to make sure that the client has some of these basic protections in place, to safeguard them against those types of risks.

James Melendres: Taking a thirty-thousand foot view on your question, David, maybe look back on the last 20 or 30 years in the development of internet. What we have had is a fundamentally open protocol. The whole concept was shareability, openness, and it's done amazing things for humanity. The amount of information that's available to virtually anyone on the globe is unparalleled. The underside of this amazing development is this vulnerability that has resulted in large scale fraud, in theft of proprietary information. Things like destructive attacks, like what occurred on Sony Pictures USA. The Distributed Denial of Service attack that has been carried out on the financial sector.

Going forward, there's going to be a real challenge to harden the network, to harden the internet. Part of that is technological, like developing the chip and pin system (for credit cards). Part of it is legal, so looking at what regulatory agencies are establishing as best practices. There's also really interesting law being developed on the back end of these data breaches, in class action litigation.

There is developing jurisprudence about whether or not individuals whose information has been accessed in a data breach, has what's called standing to sue. Whether they have suffered an injury just by the mere unauthorized access of their data. The Circuit Courts have been coming out on either end of this. Some have said there is standing, some have said there is not. That's a trend to watch, because it gets back at the end of the day to market pressure. What are companies going to need to do to limit their liability?

Mark Pribish: So far, most companies have not had to pay out on big data breach lawsuits, but boy is it costing those companies a lot of money. Before we were encouraged by our tax preparation service provider, our CPA firms to file online, tax payer ID theft and fraud was a non-event. Today, according to the FTC, in the 2016 report that reflected 2015 statistics, tax payer ID theft and fraud is the number one form of ID theft. Isn't that amazing? Because of filing online. By the way, medical ID theft is number two. Credential ID theft, your license, your passport, your employee ID, your student ID, are all forms of credentials that are being used fraudulently.

David Bolman: In terms of devices going forward, for consumers, are some devices more secure than others? Is a smartphone more or less secure than a laptop?

Mark Pribish: I'm not a technology

CONTINUED ON PAGE 34

MARK PRIBISH

VP & ID Theft Practice Leader | **Merchants Information Solutions**

1. Create an information security and governance policy, formalize it into a written plan, update and test your plan annually.
2. Include penetration testing along with a simulated data-breach event to identify gaps in your information security.
3. Annual employee education should be the No. 1 priority. Individuals, not hackers, are the cause of most data breaches.
4. Define the proprietary/sensitive information for your business, confirm which employees need access to it and then train those employees on it.
5. Your written information security and governance plan should be reviewed and signed on an annual basis by every company employee, regardless of the size of your organization.
6. Complete regular software updates and patches. Most hacking events leverage old flaws that already have been addressed but proper patches have not been applied.
7. Determine if every employee, or only those with access to proprietary/confidential information, need to be background screened. Effective pre-employment screening can identify those who intentionally misrepresent their identities.

Mark Pribish has over 25 years of experience working with financial institutions and Fortune 500 companies throughout the U.S. His background includes working in the Identify Theft, Insurance and Data Breach Risk Management business sectors. He has authored hundreds of articles and white papers on cyber security and data breach risk management and is frequently interviewed by the media as an Cyber Security, ID Theft and Data Breach Risk Management subject matter expert.

DR. DAVID BOLMAN

Provost | **University of Advanced Technology**

Q: How prepared would you say that IT departments of most local companies are at identifying when they have a valid breach?

A: Local companies are becoming more and more trained and equipped to be timely when it comes to identifying breaches. Bigger companies are more likely to dedicate cyber resources as do smaller companies whose business is close to cyber security. What is helping these companies get ready is practicing using cyber ranges, like the ones located at UAT and the Az Cyber Warfare Range in Mesa. This coupled with events like the annual Cactus Con event (cactus con. com) helps the White Hat IT community build up their skills. The companies that currently lag when it comes to identifying breaches are smaller to mid-sized companies who don't think of themselves as targets. Even though they likely have IT staff, their focus tend to be on maintaining services for employees and customers.

Q: What skill sets should companies be hiring for to help develop their cybersecurity team?

A: When hiring for an cyber resource, companies should look for certifications such as the CISSP (Certified Information Systems Security Professional). Other skills to look for include experiences in penetration testing and hardening, scripting for white hat hackers, computer forensics, social engineering, incident response and management, exploits defense, network security monitoring and Federal INFOSEC standards. These should be paired with solid network administration, database, UNIX and programming skills.

CONTINUED FROM PAGE 33

guy, but I know one thing about technology creation, these smart devices are built with minimal security. That's one challenge in today's world that consumers are going to have.

Danielle Janitch: I think it's back to analyzing the risk. How are you using that device? Your question about the laptop versus the cell phone, to me, turns back to how are you using it? Where's the information that you'd be most disturbed if it was inappropriately accessed? That's the device that you want to make sure has got the best security measures in place.

James Melendres: It goes back to the balance that pertains to mobile devices, but also to network architecture. Productivity versus security. The more secure something is, the more difficult typically it is to use. Striking that balance is an important one. For companies, for example, a network that has it's crown jewels, you probably want to limit that access as much as possible. By contrast, an HR network might be available to more individuals within the company.

Mark Pribish: Bring your own device, and that's a big challenge.

Danielle Janitch: I think that's going away. A lot of companies are now wondering why they started those bring your own device programs. They thought they were saving all this money, but in reality, they're creating so much liability risk for themselves.

David Bolman: Despite the fact that there is risk, all economic forces are working towards everything having a chip in it. Talk about Biometrics.

Mark Pribish: Biometrics, I go to my safety deposit box at Wells Fargo, I have a palm print. I have my code, it's all easy. Your eye scan, your fingerprints, your palm print, where is it? It's in an electronic file. That electronic file can be lost or stolen.

Eric Craine: Biometrics is something that we use in banking quite a bit. The basic example is you're in Alaska doing a gas transaction, and you live in Arizona and trying to figure out was that a true transaction or not. There are some developments in that space to help integrate your normal behavior, so when something occurs outside of that, that creates a trigger.

Mark Pribish: Banks and financial institutions are doing a tremendous job on that. All of us have received a phone call or been told when using our credit cards that it's on hold because we need to call. They detected irregular activity.

Danielle Janitch: It's great that we're getting more artificial intelligence that helps pull that type of data together, but the problem is it's all after the fact. The question is how we get there on the front end? I think that's a big struggle.

David Bolman: Are there gaps in laws and regulations that if closed up would help businesses?

Mark Pribish: Let's look at the history. In 2003, California was the first state that created a data breach notification law. Today, there are 47 states, Washington D. C., and 3 other territories that have those laws. When you're a small to medium size business, because of technology, your small business in Arizona might be conducting business in 10 states. The question I would have for that business, is how familiar is that business owner with those 10 state laws? It's a big challenge. To answer your question, and they've been trying this for about 6, 7 years now. DC has been legislating for a national data breach law, and it just hasn't happened. That's probably going to happen, and it's going to make it easier on the regulatory side.

James Melendres: I hope that happens. There is this patchwork of state data breach requirements. What is challenging for companies and our clients, is that the FTC is very hesitant to actually outline best practices in any proactive guidance. Going forward, what would give some degree of predictability to the business community, is some more formal standards of care.

David Bolman: We sit here today, we feel like there's a lack of guidance, and there's too many standards, and they contradict. We're much better than we were 15 years ago, when it was a complete open book, and you had nothing to even look at. It's a process, and I think we're continuing to move towards that more well understood and defined space. We'll continue to get better and stronger at dealing with the bad guys as long as we follow that process. Is there anything I missed that any of you wanted to touch upon as we wrap up?

Mark Pribish: My company has seen an under-served market in the small to medium size business market place, where most business owners are so busy growing revenue, and generating profit, that they are not paying attention to information security and governance. We actually created a template program - a small business data breach solution. It has four components, and the first component is pre-breach assessment and information security assessment. The template is easy for the business owner to understand and can identify gaps in information security right up front. The idea is most small business owners in medium size businesses aren't paying attention, so we think we're serving a need right now.

James Melendres: For companies this is an enterprise risk. The question is not if, but when. Going back to my original point about two types of companies, those who have been hacked and those who don't know it. This problem is not going away. In terms of what we're doing at Snell & Wilmer in the cyber practice, I think it's a helpful way to conceptualize what a company should do legally to prepare for or respond to an attack. We have 3 phases to our practice. The first is cyber preparedness and regulatory compliance. That's preparing and reviewing incident response plans, cyber insurance, cyber risk management, and making sure the companies are conducting themselves in accordance with mandates from regulators like the FTC, SEC and HHS. Building on that, we have incident response services, where we oversee data breach response efforts. We include forensic examiners, we include insurers we typically work with. The third phase is post-attack litigation, class action litigation, regulatory enforcement, private litigation. Those are 3 distinct phases that we spell out in detail on our practice page.

Danielle Janitch: For me, it's that there are resources that are available to help all businesses, small, medium, and large. I think the thing that businesses need to keep in mind is that there's nothing special here that's different from any type of disaster recovery. It's a cyclical process. You need to be prepared for it, you need to be thinking about mitigating risks, and then you have to be ready so that when the time comes you can respond and you can recover quickly.