AUGUST 3, 2018 | ADVERTISING SUPPLEMENT TO THE CINCINNATI BUSINESS COURIER

CYBER SECURITY

FORUM DISCUSSION //////////

PANELISTS

Lou Carli

Principal Consultant,
Security Practice,
RoundTower
Technologies

Scot Ganow

Co-Chair Privacy &
Data Security Practice,
Taft Stettinius &
Hollister LLP

Mike Rock

Chief Information
Security Officer,
Vernovis

Terry Williams

Chief Technology
Officer,
Belcan

RoundTower
Business impact through technology

Taft/

VERNOVIS

Belcan

CYBER SECURITY FORUM

The *Cincinnati Business Courier* recently hosted a cyber security panel discussion with four, top industry experts. Editor Rob Daumeyer led the discussion as the panelists discussed topics such as planning for a breach, identifying a breach, post-breach, what to do if you're hacked, and disaster recovery.

The panel of experts consisted of Lou Carli, Principal Consultant, Security Practice, RoundTower Technologies; Scot Ganow, Sr. Counsel/Co-chair of Privacy and Data Security Practice, Taft Stettinius & Hollister LLP; Mike Rock, Chief Information Security Officer, Vernovis and Terry Williams, Chief Technology Officer, Belcan.

ROB DAUMEYER: My name is Rob Daumeyer. I'm the editor of the Cincinnati Business Courier. This is the Cyber Security Forum. We have four great people to talk to you today. The Cincinnati Business Courier uses this space at Taft a lot for these kinds of forums and it works out well. So, thank you to the Taft. And, thank you to our panelists from Taft, Vernovis, Belcan and RoundTower, who are also represented here. They've allowed us to get this together. My goal today is for an hour or so, we will talk, followed by 15 minutes of questions. My first goal is to make sure you get out of here on time. My second goal is to make sure that this becomes a conversation. I'm hoping we don't have too many speeches, especially from me. So, I'm just going to let our panelists talk, and if they have questions for each other, fantastic, but if you have questions, save them to the end and I'll open it up. You can write them down, or just remember them, and we will save time at the end for questions. So, here's what we are going to do to start. We will start with Mike and go down to Terry. Introduce yourselves, tell us where you work and what you do.

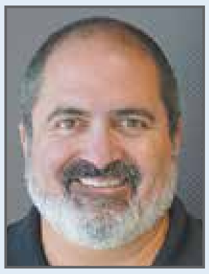
MIKE ROCK: Good morning. My name is Mike Rock. I'm the CISO and the Cyber Security Practice Leader for Vernovis. We are a staffing, consulting and project completion company serving the Cincinnati, Dayton and Columbus areas. I've been serving in the security leadership space for about ten years. Thank you very much.

SCOT GANOW: Good morning. I'm Scot Ganow with Taft Stettinius & Hollister. I'm the co-chair of our Privacy and Data Security Practice, where we do about everything, when it comes to data privacy, from policy development to compliance and all the way through to incident response. I've been doing privacy work, long before I became an attorney, going back to 2003 (before privacy was so cool), as a chief privacy officer in the health care and technology space.

LOU CARLI: My name is Lou Carli with RoundTower. I'm the Director of the IT Security Practice, comprising everything from compliance, incident response, forensic, IT security controls and technologies. RoundTower, as many of you know, is about a 400-person company with 400 million in revenue, located off of Interstate 71. My background is in IT security. For about the past decade, I've worked at various consulting firms. I came to RoundTower via an acquisition. I was the president and founder of a company called Mainstream Security, where we built a 24/7 Security Operations Center and provided capabilities around incident response and forensics.

TERRY WILLIAMS: Good morning. I'm Terry Williams I'm the chief technology officer for Belcan, and if you're not familiar with Belcan, Belcan provides engineering services in aerospace and manufacturing. We also have a very large government services business unit where we provide IT and cyber security services, for some high profile government agencies. Belcan has 9,000 employees, globally. We've completed eight acquisitions in the last 24

MEET THE PANELISTS



Lou Carli

Principal Consultant, Security Practice, RoundTower Technologies

Mr. Carli brings over 20 years of IT security expertise to his current endeavors and clients worldwide. His main area of expertise is building world-class, security- centric engineering and sales teams that support the most complex environments. He has launched several security and forensic firms and has built them to successful exits.

As a leader in the security field he recognizes client needs and supports those with industry leading service offerings. To that end, Carli advises clients on intellectual property protection and security and manages security breach efforts. His background in the security start up space is extensive.

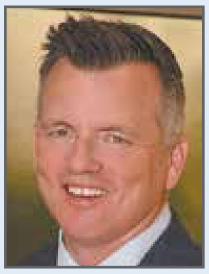
Affiliations

ISSA – President of Cincinnati Chapter (2012-2013)

DFWG – Founding member of the Digital Forensic Working Group

Data Discovery Alliance – Founding member, and co-chairman

SecureScan.com – Co-Founder and board director



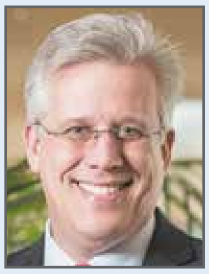
Scot Ganow

Co-Chair, Privacy & Data Security Practice, Taft Stettinius & Hollister LLP

Scot is co-chair of the firm's Privacy and Data Security Practice. As a former chief privacy officer and leveraging more than ten years of management and compliance experience in Fortune 500 companies, Scot brings a diverse business background to his privacy and data security practice. Scot has represented clients in a variety of sectors, including consumer reporting, construction, healthcare, and manufacturing. Scot assists clients in all areas of the data life cycle, including: policy development, implementation, assessment and training; identifying, evaluating and managing privacy and security risks; third-party management, including onward transfer agreements and audits and data breach and incident response management and counseling.

In addition to his data privacy and security practice, Scot also has experience with intellectual property matters as a patent attorney. He also counsels clients on general business law matters.

Scot attended the University of Dayton School of Law, where he currently serves as an adjunct professor of law. He clerked for the University of Dayton general counsel's office and the Cincinnati Reds general counsel. Scot is admitted to practice in the state of Ohio, in the U.S. District Court for the Southern District of Ohio and before the United States Patent and Trademark Office.



Mike Rock

Chief Information Security Officer, Vernovis

Mike Rock, has over 24 years in the Technology industry, and brings extensive Fortune 500 Enterprise and SMB Consulting experience. He has a strong executive presence with proven ability to translate security risks into business language for optimal business partner engagement during risk-based decision-making. Throughout his career he has been integral to the security teams of large companies such as Western & Southern Financial Group and Procter & Gamble. His impact has ranged from leading a group of 30 senior managers to align on a single vision and strategy for consumer mobile platform security for over 80,000 devices globally, to $15 million of IT Infrastructure integrations including over 3,000 applications and 35+ locations, to creating an effective, metrics-based awareness & training program for 110,000 global employees. He is an invaluable addition to Vernovis as our CISO, working to provide cybersecurity solutions like compliance and risk assessments, remediation project management, security program roadmap and oversight and ongoing CISO advisory services, for small to mid-sized companies.

Terry Williams

Chief Technology Officer, Belcan

As Chief Technology Officer (CTO), Terry Williams is responsible for leading Belcan's strategic and operational information technology initiatives. Mr. William's responsibilities also include global cyber security and the evaluation and deployment of current and future technology platforms used throughout Belcan. Terry oversees both domestic and global technology-related investments required to enable and streamline ongoing business functions. He holds a Bachelor's degree in Business Management, with a minor in International Business.

PROTECTING YOUR BUSINESS FROM CYBER CRIME

months. So it's a growing business. Cyber Security is extremely important to us because of the type of work we perform for our clients in Government and Commercial Markets, classified work that we do and some of the work that we do for the Department of Defense and other government agencies.

COURIER: I'm going to slide up here when I ask the question. I know I don't have the microphone right in front of me, so I'll try to talk loudly, I just don't want these guys to wrench their necks when I ask a question. So, I will ask the first question, and I have a very quick follow up. What kinds of companies should be prepared for a data breach? Again, I have a super-fast follow up question.

ROCK: Let's not overthink this one. If your organization has a computer, and you're connected to the Internet, you should be concerned.

GANOW: Absolutely. I would agree. I don't care what area of business in which you work - you have data issues. I would expand that to say it's more than just the data. It's the access to and integrity of the system. When we talk about security, it's not just protecting the confidentiality of data, it's making sure you can get to it, that you can use it, and you can maintain your business when things go sideways.

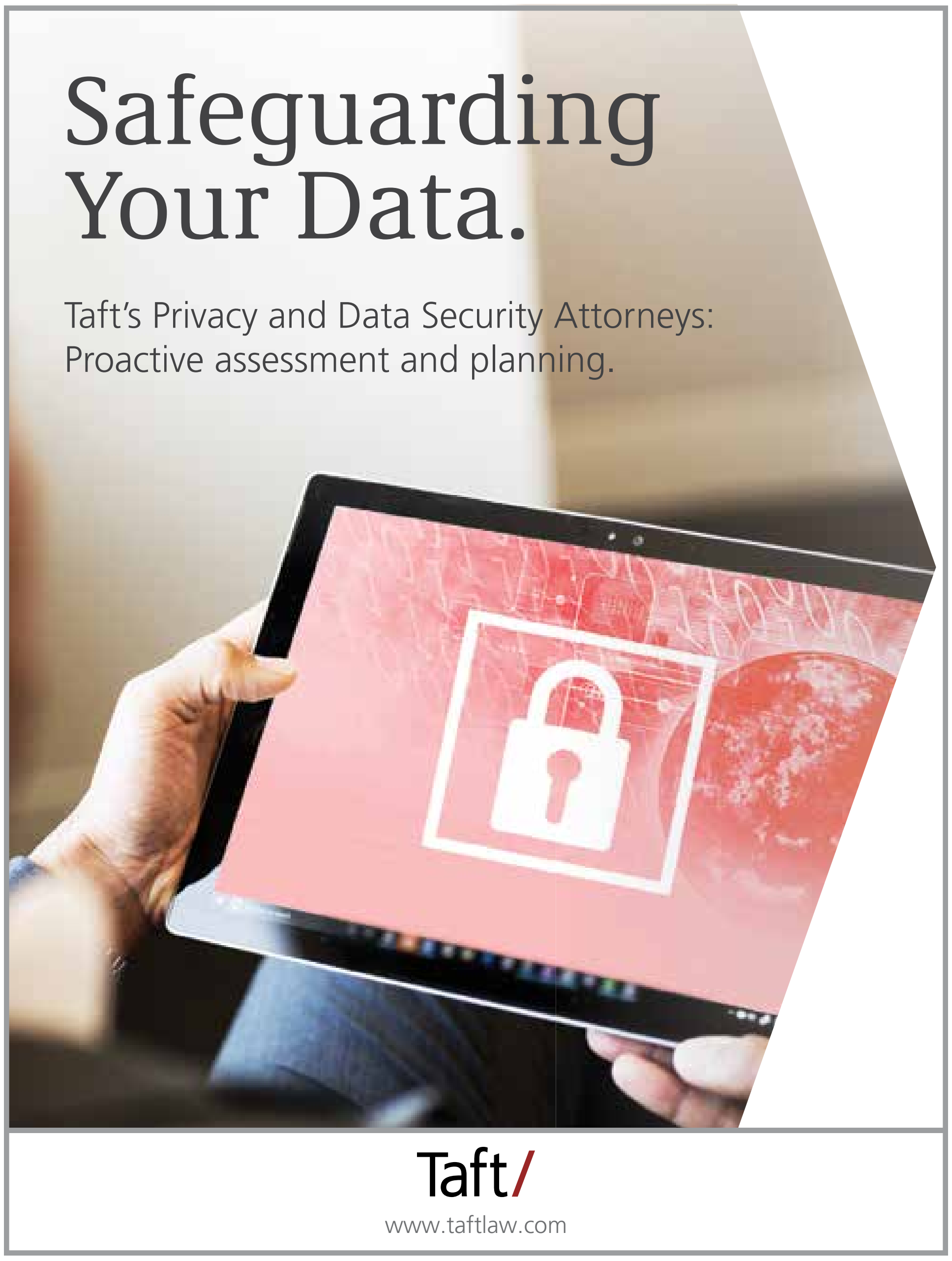
WILLIAMS: Things have evolved from a cyber (standpoint,) over the last 10 years or so. If you look at the different types of threats out there, you have foreign-government-sponsored threats, which are for more elaborate and planned. Cyber has become the new battle field. It's no longer an issue where you have a hacker in the basement just doing something because they can. You have foreign threats, insider threats, and things have really picked up with ransom attacks. The other thing to think about is that if you are part of a supply chain to any large high profile manufacturer, you should be concerned, because that's one of the areas where we're seeing a lot of focused attacks. They're getting to some of the larger manufacturers and companies through their supply chain. You probably are a target, regardless of how big or small you are.

CARLI: I would add compliance to the mix. So, keep in mind here, in any of the verticals, retail, healthcare, etc. If you're in those spaces, you are mandated to do certain things and have certain controls in place, so make sure that you're getting that in line. But, what we see a lot of is that compliance doesn't equate to security. Just because you're compliant, it doesn't mean you're secure. Keep that in mind. That's a misnomer out there. We have a lot of retail clients that are under PCI, and they think if they adhere to PCI they're completely secure, and that is not the case. It is a good starting point, understanding what your intellectual property is, and what your responsibilities are, and that will give you guidance on how to prepare for a data breach.

COURIER: Why are some companies not worried about this? When the answer should be everybody. Everyone should be concerned about cyber security. Why is this not fully understood?

GANOW: Well, I was going to piggyback on that. I can't echo enough the point that you made that people need to remember that they may not be the ultimate target. You may just be the door in. I work in the Dayton office and people look at me like, 'Come on, Scot, this isn't going to happen in Dayton. Nothing happens in Dayton. They're going to go after New York, D.C., or some big city.' And, the point is 'no.' They are going to go to the weakest link, and that might be you in Dayton, because you don't think you have sensitive data, or you don't think that you're a connected part of a larger system. The other part of that I hear continually as I advise clients, preferably before they have a problem, is 'It's not going to happen to me. It's going to happen to some other company, someone with more money, or someone that has better data than I do,' or 'I will just pay for it when it happens.' That's always a great response. I love that one, 'I'll just pay

DISCUSSION, CONTINUED ON PAGE 4B



DISCUSSION, FROM PAGE 3B

when it happens.' There's this perception out there that it's always somebody else. I've been in business. I get it. You have 900 million other things to think about besides your incident response plan. I know how it is to work through it, but it's like anything else. It's like a heart attack. You think it's not going to happen to me, and you keep putting it off, until it happens. All of a sudden it becomes pretty urgent and in some cases, and (for many) small businesses, it's game over.

WILLIAMS: I have conversations with companies relative to breaches and they don't believe they are a primary target, or 'We don't think it could happen to us.' I typically say that you probably have already been breached. Not every hacker is going to knock on the door and say, 'Hey, we're here. We've got your data.' It can happen. It probably already happened to a lot of companies that think they are not a target and it won't happen to them. Like I said before, everybody is a target these days. There are people that just want to be malicious and spread viruses. Typically, what I'm seeing is that a lot of hackers that are just doing it because they can are targeting some of the smaller enterprises now, because they know that their defenses are probably not as strong. They know the thought process is 'It can't happen to us.' The targeting methods are different now.

ROCK: What I have observed in the small-to-mid sized businesses is a little more willingness to accept those risks, possibly because in these businesses there is a necessity to wear ten hats at the same time while maximizing every dollar spent into growing the business. It's easier to accept the risk and say 'we'll pay for later if it happens'. What I try to explain to people is that if you have information systems or you have websites that you are part of the computerized, I'll call it a target zone, for malicious automated software that is running 24/7, 365 days-a-year, just looking for something they can break into. Consider this metaphor. If you parked your car at the airport, you chose not to lock your door, because you don't drive a new car and there is no reason why your car should be interesting to anyone. In reality there are people testing those door handles all of the time just to see what's open, and then your car becomes interesting. Equate that to your information systems that are plugging into the Internet. Assume someone tests your digital "door handle" and finds out, 'Oh, I can get in here. Okay, now what is interesting about this company?' So, you don't have to be a high value target to become a victim, because it's a constant threat space where people are just testing your door handles and testing your locks. If you don't have some fundamental controls in place to prevent that, you then become interesting, and once you become interesting, they are going to get you for what they can.

GANOW: I want to add to that this often is considered a compliance or a risk avoidance issue, and companies look at it like it's not going to make money for us. I have yet to go through this effort of preparing an incident response plan and get a compliance program in place and a client hasn't been blown away by the awareness of how their company uses data. They had no idea what data that they had, where it was, how it was being used, and how they could potentially go on the offensive with it. The whole benefit of investing time into this space to protect against attack is you will come to understand your business more intimately than you ever could. Data is like water. It goes everywhere. It is an unbelievable opportunity to learn about your business as well as the business of your customers and your subcontractors. Not just to prevent risk, but I would argue to seize opportunities to make money, to be more competitive, and to offer yourself as a better option as opposed to the other company. Customers will say "I'm going to go with you, because you've got you got your stuff together" versus someone that doesn't. So, it's not just a cost center. It actually can make you money and distinguish you from your competitors.

PROTECTING YOUR BUSINESS FROM CYBER CRIME

CARLI: I'd like to add to that, briefly. Talking to a lot of small businesses and even medium-sized or enterprise businesses, besides the excuse of we're too small or we don't have important information, but what I find interesting is sometimes companies will come back and say we really don't have IP, we don't have patents. We're not beholden to any compliance mandates like healthcare information, et cetera, and I think the job of the security officer on these teams is education. Even if you're a distributor or reseller, you still have client lists, you have important information and your workflow processes. You're obviously a successful business for a reason. I think that gets lost with some employees, even in the IT space, and having that discussion internally is vital, because employees are the weakest link. They have to understand that what we do as an organization is worth protecting, and I think sometimes they come to work and don't really take that as a challenge. So, part of the job outside of the technology and control piece is education. You should be looking within your organization to start an end-user awareness program. They're starting to get a lot more mature. There are a lot of products on the market, and a lot of inexpensive ways you can do that. So, that's another piece of the control puzzle that you want to add.

COURIER: So, if I run a company, or if I'm in leadership, if I'm in the top executive team, and tech is not my game, but I take this seriously and want to take this seriously, what do I do? What does a business owner or president do when they don't have the expertise? Do they get out of the way, or do they figure out a way to lead anyway? How does that work?

PHOTO: PAULA NORTON

"What we see a lot of is compliance doesn't equate to security. Just because you're compliant, it doesn't mean you're secure, so keep that in mind. That's a misnomer out there."

– Lou Carli, RoundTower Technologies

WILLIAMS: That's an interesting question. Let's face it, security people can be annoying at times. No offense. But, I don't think they can be the voice of the program. For example, we send out notifications, and we send out security newsletters. Typically, the response is okay, but it can be perceived as security trying to push something on us again, and over a period of time they become apathetic to it. Generally, you're not going to have your chief information security officer come and be a motivational speaker. That's not what they do. So, where I'm going with this is that the president and CEO has to be the voice of the program. They have to be the ones that are pushing the agenda. It can't be something that the security organization is pushing on us. You don't want it to be perceived as one of those annoying security things, that's going to slow us down, and add more processes. So, this really has to come from the president and CEO. They don't have to be technical people, and I hate when people try to communicate cyber security in technical terms, because you need to keep it simple, and I think that presidents and CEOs have to realize that they have to be the voice, and they have to lead. It has to be a top company priority, and the only way to do that is to have the top executive officer constantly communicating the importance of cyber security to the organization.

ROCK: I want to dovetail on that. The expression I use whenever I talk to somebody is the tone from the top, and if senior leadership is not living it, and if they are not communicating it to the rest of the business, then you're right. It's 'Oh it's just that security guy over there.; They're always paranoid, and they don't care that it slows things down.' We do care, but we have a job to do as well. The other thing I'd like to add though is a savvy president or CEO would include cyber in their overall enterprise risk management portfolio that should be governed and overseen by a chief risk officer, or somebody serving in that capacity where you're talking about cyber risks in the same conversation you're talking about an acquisition risk, or some other type of critical business risk that you have to decide if you're going to try to mitigate or accept that risk. It's all part of the same conversation, because it's not an IT problem. While security has technical solutions, but it's not strictly an IT problem. That's what the president and CEO can do to help level the playing field. And, of course, from a security standpoint, we have to get better at articulating the risks in business language to those within the business. You can't go in there and talk about the number of attacks and the CVE's and things like that. We need to go in there and talk about potential losses without being alarmists.

GANOW: Speaking to the leadership side from a legal perspective, in regard to the question whether they should they step aside, absolutely not. It's very clear that directors and boards, in particular, have a duty to be on top of the security part of the business. Taft's Kevin Kinross and I work with boards to educate them on the threat and the diligence they have to have as part of their oversight responsibil-

DISCUSSION, CONTINUED ON PAGE 6B

DISCUSSION, FROM PAGE 5B

ity. You can't just say "we didn't know", or "I don't talk tech." You think hackers and hoodies (because all hackers wear hoodies) and that kind of thing. But security is not all tech. There's two parts of the safeguards that are relatively low tech. They don't cost a lot of money, but are extremely valuable: administrative and physical safeguards. And that is the policies, and procedures. Train your people and make them aware of the risks. That costs you nothing, but it can save you everything. Also, consider physical safeguards, such as locks and ID badges. When I was a privacy officer, I used to walk around the office at 5:05 p.m. on a Friday, and I'd just pull on drawers, and walked into cubes and you'd be amazed how much stuff people left out and left unsecured. Computers were unlocked and drawers were open. I found divorce decrees on file cabinets and medical tests sitting on copier machines. That is low tech security. Not letting strangers or unidentified people into your office space. I do risk assessments with clients and part of is just to see if I can walk in. You know what gets me in? A suit. Because "you look like you should be here", and they let me walk right in and I can do whatever I want. I don't, but I could. How low tech is that? There's nothing tech about that. That's training and that's physical security. So, to any leadership team, and I don't care how big or small you are, I say you don't have to throw millions of dollars at security and loads of technology. Awareness, education, policies and procedures can get you pretty far, because it only takes one employee to mess up. It also only takes one employee to say, 'Yeah, I know you have a suit on, but can you check in with our front desk and get a visitor's badge."

CARLI: I'd like to add to that. We've seen that if the C-Suite is not involved, or if they are not committed, these programs don't go anywhere. The employees don't really have the belief that there's a total commitment from the organization. That's just contributing to what we've said so far but getting that leadership group involved is very critical. Then, this has all changed from a technical conversation to a business-risk conversation, and that's why it's easier to get the C-Suite and board of directors involved. They realize the risk is on them. If they are willing to accept that risk, then that's what it is. I think that it's taken less evangelizing to the C-Suite, lately, because they are aware, which is a good thing for us. There are several things that we can do that are low tech that would support that, but, it all has to come from the top. That first letter, when you're rolling out an end-user awareness program, coming from the president and CEO is important. Healthcare is a perfect example. When you have a board of directors or law firms in some cases, where partners or doctors are on that board they're really looking at it like you're spending their money. They always look at security as a control that is stopping them from doing their job, when in fact, they've got the keys to the kingdom, and we need to do this, so there needs to be that balance. At the same time, if you can sit down, educate the group, and have them be that framework around what you're trying to do as a program, that will be extremely beneficial.

COURIER: Let's say that you have done a good job of selling the president on, 'Okay, we need to get better at this.' Scot's gone through and he's taken people's HIPAA forms out of copy machines, but I would like to know, and you can all weigh in, what does a cyber-security plan look like? Are there 58 steps, or are there three, or does it depend? I don't know what it looks like.

ROCK: A cyber security program is a business plan for how you are going to protect your digital assets, and your hard-copy assets from those with no business accessing it. So, it could be a 50-page, or it could be a ten-page document. It really depends on the complexity of your environment and what you are trying to accomplish.

There are lots of different frameworks and models that you can follow to make sure that you aren't missing anything and they cover most of the elements that are involved in the cyber-security

PROTECTING YOUR BUSINESS FROM CYBER CRIME

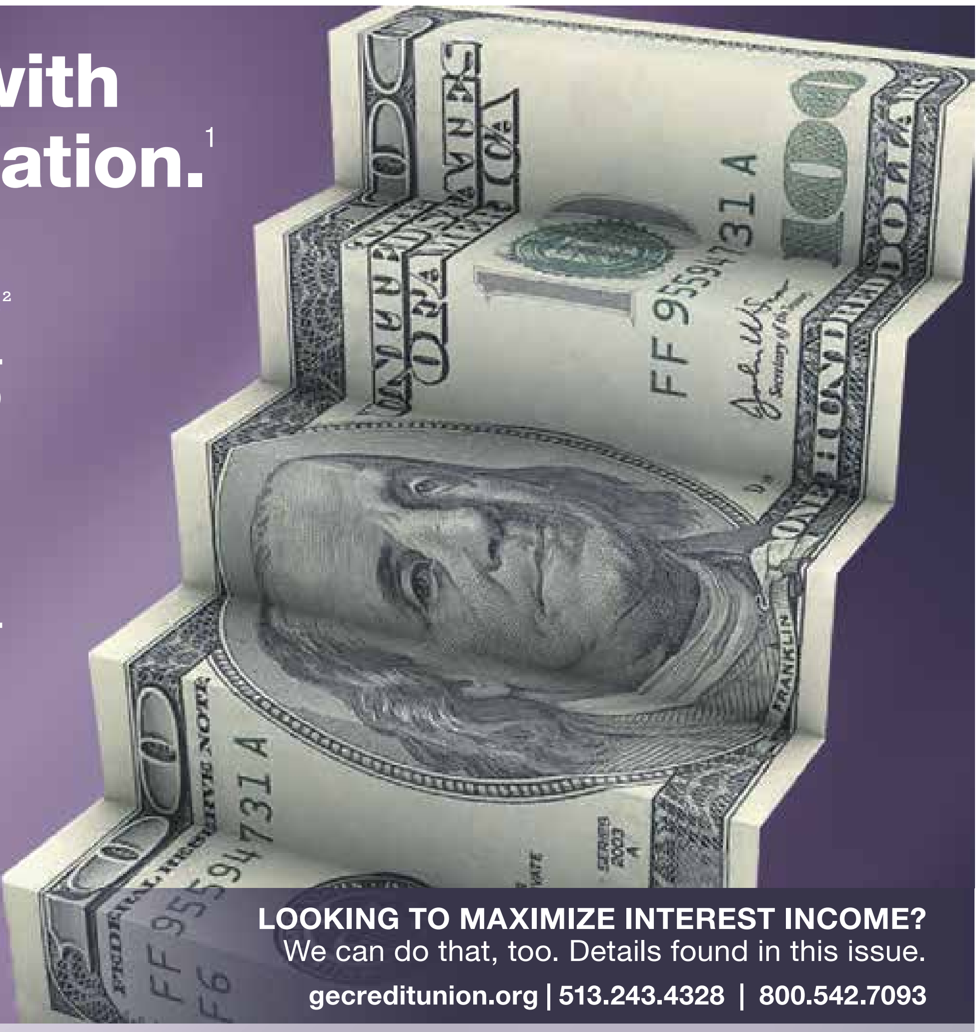
program. (Ultimately,) it is about sitting down with key stakeholders and explaining what all the elements are and having those conversations saying, ‘Okay, this all needs to be included, but we’re not going to the nth level of detail here. We are going to high-level it, have a few policies and controls, and then we are going to have some oversight and governance, which I can’t stress enough, because the cyber-security program is not a fire and forget situation. This is definitely something that is living and breathing and it must be governed. Someone has to be responsible to oversee it and keep it alive.

WILLIAMS: I spent several years providing disaster recovery consulting and I don’t see much difference between putting together a cyber-security recovery program and disaster recovery. There’s a proactive factor associated with cyber security and disaster recovery, meaning there is an up front, (pro-active approach to) preventing a disaster. The recovery process is not much different than disaster recovery. If you take that same approach in terms of a disaster recovery plan for example, it has to constantly be updated. You have to make sure that you know where your assets are, what you’re trying to protect and how you’re going to recover them. So, there’s not much difference there. There could be a significant financial loss with disaster recovery. The same thing can happen with a cyber-security breach. The program has to take that into account. So, if you take your disaster recovery plan and you build it around your cyber-security program, I think you’ll capture quite a few required elements.

CARLI: Yes, just to add to that there is a difference between an incidence-response plan and a security program development plan. The incidence response plan is key, because we’re all dealing with this today. It seems like the natural thing to gravitate towards, but that is not a holistic plan to build your entire program. So, you want to incorporate that incident response plan within a larger framework that talks about so many more controls outside of incidence response. Then, similar to the disaster recovery, once you develop that plan, tabletop exercise it and run different scenarios that can flow through the organization. That gets the awareness of the employees and how serious you are about what you’re trying to do. It’s like disaster recovery, if you don’t test it, you don’t know if you are up to snuff when it comes to protecting those critical resources. That’s a significant part of what you want to make sure you’re doing. Also, it’s not just a snapshot in time. This is an ongoing, living, breathing document like Mike has mentioned. You have to constantly revisit it. When we build these things, it’s usually at least once a quarterly basis that we’re re-interviewing and discussing this. Then, I would also say that this does not stay within IT. Human resources, legal and business unit leaders, all of these people should be involved in the process, and don’t keep it as just an IT thing, because it’s really an overall business thing.

GANOW: I would echo everything that’s been said here. At Taft, we developed a 90-page incident response plan that accounts for pretty much everything. Before you say, “yeah, put the lawyers on it and you’ll generate paper.” I’ll be the first to say, and echo it, your plan has to be scalable to your organization. Ninety pages doesn’t make sense for a five person shop. At the same time, people say, ‘Hey, we’re just a five-person shop. I would say, ‘Yeah, but what kind of data are you accessing?’ ‘What about your clients?’ Your risk may be much bigger than that five-person shop. Keep it simple. Number one, you have to classify your data. Do you know what data you have? Do you know what it’s called and what it looks like? Is it protected health information under HIPAA, is financial data, is it credit card data? Have you given it a name? Both externally, in legal terms, but also internally. So your employees know that’s red, and it’s highly sensitive, or that’s green and it’s public. If you don’t give it a name, you can’t govern it. Number two, you have to map it. Where does it live and breathe in your organization? You can’t safeguard it, if

DISCUSSION, CONTINUED ON PAGE 8B



CYBER SECURITY FORUM

DISCUSSION, FROM PAGE 7B

PHOTO: PAULA NORTON

"When we talk about security, It's not just protecting the confidentiality of data, it's making sure you can get to it, and that you can use it, and maintain your business when things go sideways."

– Scot Ganow, Taft Stettinius & Hollister LLP

you don't know where it is. And, you're looking at me like, 'Yeah, Scot, that's common sense.' You'd be amazed how many people don't know about what data they have and where their data is and why? Because digital changes everything. You have to think about all the places your data goes. IT is a great resource to be sure, because they have the network maps and you start there. But as I just told you, you've got file cabinets, you've got offices, you've got the CEOs home office where he likes to keep everything, because it's more convenient. You have to know where the data is and you have a map to it. Third, once you know what your data is, and where it lives, then you can put safeguards around it. And, if you learn anything from me today, learn these three things – administrative, technical, physical safeguards ATP. Use those words. Even if you don't know what they mean, it makes it sound like you do, and the reason why is it's inherent in almost every privacy or security with which I've ever dealt. They all talk about administrative, technical, physical safeguards. Administrative and your contracts, policies and insurance. Technical is encryption, passwords and whatever you want to use to safeguard it. Physical safeguards are locks, ID badges and security, or hard copies. Put that plan in place, and then work it, because it changes every single day. It doesn't stop. Your plan could be five pages, or a 100 pages, or whatever makes sense. The benefit of all of this from a legal perspective is to have it written down, because up here in your head is no good. When I'm dealing with opposing counsel or a regulator, they don't care if it's up here in your head. If I don't see it on paper that you're actually trying to do these things, I can't defend that. If you have it documented, I can show you're being reasonable. You've done everything you can. It's not a sin to get breached. It's a sin not to have a plan for it when it happens. And that's what a written plan does, whether it's five or 100 pages.

COURIER: What is the GDPR? Did you already explain that?

GANOW: No I didn't explain it, but everyone knows now, right? It's the General Data Protection Regulation. It went into effect in Europe on May 25th. And, important to note, even though you're in the United States, if you collect personal data on employees or customers as part of your business, and they happen to be in the European Union, it could impact your business. California just passed a new law. It's not like GDPR, but it has some things that are similar to GDPR and goes into effect January of 2020. Start planning now. It's a consumer protection act that effectively expands what they've already got in place regarding collecting and using personal data for California residents.

ROCK: Privacy compliance is tightly related to security but is not the same thing and has slightly different objectives. I think it's worth mentioning that it's commonly accepted that GDPR-like regulations are going to spill out into the United States, eventually. California's got the jump on it. It's also very accepted that most other states are already working on something along this line as well. So, just because you may not have European residents' data, you better start thinking about how you're going to comply with these types of laws. It's really a privacy situation, and a solution is something that Scot mentioned, which is data governance. People roll their eyes at us technical guys when we ask questions like, 'Do you know where your data is?' Or do you know where it isn't, and can you prove it? And, are you protecting it? It's going to be a fact of life. Those companies that start earlier, just for a little free advice, it's going to be a lot easier for you. If you find yourself up against it, where you can't do businesses in a state anymore because you're not complying with their regulation, it will cost you a lot more and it will be very painful. Data governance is a business problem, it's not an IT issue. What function in business does not use data? That's why it's not an IT issue. IT can help solve it, but the business has to put the clamps down on who's handling it, and who is moving it around. We've been very free and loose in the business environment, moving data around for internal purposes. Everybody likes to have access to that data, and I think it's going to change the data governance conversations and companies that hold this information now have to be protected. Security can help with that, but we can't be the only ones driving it.

COURIER: If you've had a breach, how do you prioritize? What data, for instance, is the most important? How do through that? Then, are there any things that you just flat out make sure you don't do?

GANOW: This is why you have it all written down in a plan, and you practice a plan with tabletops, because at 4:30 p.m. on Friday when it happens. The time to figure that out is not when it happens. The time to figure that out is in advance. So, the questions are 'What data is the most important?' Well, that's going to be driven by your contracts, that's going to be driven by state and federal law, and maybe even international law as to which sets of data require notice to individuals or regulatory authorities, or if you have contractual burdens to respond in a certain amount of time. I'm working on a data breach right now, and to say the United States is a patchwork of breached laws is an understatement. So, we have 50 states and 50 different breach laws that you have to satisfy, and look at the individual requirements. And then there is GDPR, which was mentioned before, is 72 hours. That's never been done anywhere in the world, 72 hours. incident response, it takes that long to figure out what your incidence plan response is sometimes. So, it's really going to be driven by contractual requirements, legal requirements and regulatory requirements that may apply your business. So again, the benefit that incident response plan has while we work with our clients on that is it has all of those things already listed out. You already know what data is in play. You have an incident response team that gets around the table and says, 'Okay, do we have a breach? And, by the way, point number two, there are two takeaways – administrative, technical and physical safeguards, right? You're going to take that with you. Don't use the "B" word – breach. It's not a breach until your lawyer says it's a breach. That's very important, because lots of things are more incidents, that's why we call it incident response plan. It's more of an Incident, event, issue or an opportunity. These things happen all day long. Your firewall gets pinged all day long. People will have malware on their computers all day long. That's not a breach, necessarily. So don't use the word "breach." Don't email about it, don't call about it, and definitely don't put the CEO in front of a microphone and say, 'Hey, we've got a breach.' It is a multi-disciplinary approach. It's not just lawyers and IT; it's PR, it's employees, it's operations and it may be outside parties, but if you don't plan for it, you will make those huge mistakes, and I will say one of the biggest mistakes is coming out too fast, getting the CEO in front of a microphone way too soon, and making the problem even worse. It's gasoline on the fire. When you get someone out there that says we've got a breach, but we've got it all covered, and we know exactly what happened, and then a day later, I have to amend that. Now, we talk about a business issue. Now it's not just a legal issue. It's also a stock price issue, it's a public rela-

PROTECTING YOUR BUSINESS FROM CYBER CRIME

tions issue, or a customer trust issue. It can really become a huge problem - all the reasons to have the benefit of that plan written down and accessible, preferably practiced before D-day, but definitely somewhere where people can get it, so everyone takes a breath and exercises it.

PHOTO: PAULA NORTON

"If you have a computer, and you're connected to the World Wide Web, you should be concerned."

– Mike Rock, Vernovis

WILLIAMS: I want to echo what Scot mentioned about preparing for an incident. I don't use the word breach either. Particularly inside the business. It is an incident until it becomes a breach. Things that you have to investigate. Incidents are things you need to investigate. Because of the business that we do, we have government clients, of course, we have commercial clients, but there's a lot of compliance regulations that we have pertaining to data. One of the things I want to mention is that it is really important that you classify your data. I can't over emphasize that, and the other part of that is to understand where your data is located.

Most companies, big or small, don't know where their data is. It could be on someone's PC. You could have something really critical that people keep on their PC. We all know that employees use their e-mail as document management systems. So, you really have to go through a process prior to having an incident of understanding exactly where your critical data is. Now, typically when we find something like that, and when we have a client, we urge them very strongly to make sure that you try to as much as possible to centralize anything that's critical, so you can protect them. The best case scenario is that you can centrally protect your data, you can control it and you can protect it. So, like I said, I can't overemphasize that. Every incident that I've seen has dealt with data, and someone not knowing where their data was, and it's not protected like you would protect centralized data.

ROCK: You're right. It depends on the business as far as what data you try to protect first, but let me take a step back from that. If you believe you have an event or an incident, you do need to activate your plan, but then that plan should spell out which experts are going to get involved., The first thing your experts are going to try to figure out is what's really going on, because likely all they currently have are some descriptions of the symptoms. The next thing they're going to do is contain the situation. They need to put walls up, and figure out where it is, and where it's not so they can stop the spread of whatever is happening. Then, they're going to start fixing things and then recovering systems. So, what's important to incident responders is being able to know what happened so they have a higher degree of confidence that they have corrected the situation, plugged the gaps and have the situation under control. So, don't just turn all the computers off and freak out. You should activate the plan and get the expert involved so they can tell you what steps to take and in what order so the situation does not become more difficult by responding with a knee-jerk reaction.

CARLI: Let's have a discussion around getting the experts involved. What we see a lot of are IT staffs that want to be investigators, want to be the CSI, but you need to look at your staff and you need to understand if you have the capabilities to even execute an investigation from a legal perspective as well as spoliation of data, doing things wrong that could really affect how the defense goes for you. We see more of the enterprise with a larger IT infrastructure probably have certified examiners and incident responders on the team, but that's not necessarily the case. If that's not the case for you, your incident response plan can call for having a third party. There's no shame in not being able to do it yourself, and sometimes it's more beneficial to have a third party, and an independent third party, especially if there's some investigation that's against another employee type of scenario, and Scot can speak more to this. It's really critical that when you're writing this plan, determine what your skill set is in-house. If you don't have that skill set, go find it. These resources are expensive, so maybe it's just more of an IR retainer, or a corporation that can act on your behalf and be part of that team. So, when you open that plan it says engage X Y Z Consulting Firm, that's key. On the B word, what I would also say, which I think is interesting, because we do have a lot of incidence response, a lot of malware, and ransomware, et cetera. One of the things that you definitely do not want to do is engage the hackers, talking directly to them or, taunting them. Believe it or not. I'd say three out of the last five we've actually had IT staff engaging directly with them, negotiating the ransom, trying to actually tell the hackers that it's too expensive. Do not engage that way. Engage along the plan with legal; do not engage with the attackers. I know it's there's a lot of giggling out there, but three out of the last five that's pretty amazing, so don't take that for granted.

GANOW: IT operations are different than IT security. It's a different discipline. I agree with you. Security people are different. The security folks look at the world a little bit differently, and that's a good thing. You want that expertise, but the value of outside expertise is important for a couple of reasons. When you have an incidence response bill, people often think the lawyer is the most expensive one on it. But often it's forensics that is the most expensive piece. It is because that expertise is invaluable, not just because of what they do, but because of what they enable me to do. Remember what I said about the "B" word? ("breach") It is wonderful if you bring in a team that can look at it say, concretely, 'Yeah, that data was there, it didn't move, it didn't leave, it was encrypted in space and it was never ex-filtrated. Depending on the laws involved, I may not have a breach. I have an incident, to be sure. Depending on the data, I just spent a lot of money, but it just possibly saved me millions of having to respond to that, because I don't have a breach as far as the law is concerned and maybe there is no risk to customer to be harmed.

COURIER: This is a related question. We've written about RoundTower's success in this area, but how do you find tech talent right now in this climate when unemployment in general is below four percent, and in IT, it's got to be in the negative numbers. How do you fight it, because if you have somebody who wants to cowboy it, maybe that person's not the right person? How do you upgrade?

WILLIAMS: The reality is that you have to be flexible in the recruiting now. With this particular area, obviously, there's a lot of competition for talent with some of my partners here, and others, and probably some of you also. We've learned that you have to be flexible in terms of where you're looking for talent. So, we've expanded our search throughout the years, and we've had some success in doing that. The other thing is making sure that you can retain the talent once you get it, because there's a lot of opportunities out there. So, we do things a little bit differently in terms of how we train and how we have career plan for them. We don't stick them in the back room, where you don't have to see them. I know some companies do that and treat them like the rest of the IT staff, and that just simply doesn't work. So, you have to make sure that you have a really great retention program. We have a technical services recruiting business. It is a global business, where we place thousands of technical staff around the

DISCUSSION, CONTINUED ON PAGE 10B

CYBER SECURITY FORUM

DISCUSSION, FROM PAGE 9B

globe each year, but one of the things that we've found is that we can continue to battle back and forth for the few resources out there, but the best approach right now is to create your own talent pool. So, we've started a program with Cincinnati Public Schools. It's a three-year program, where we actually have a cyber-security curriculum, starting in the sophomore year. This is the same type of curriculum that a professional outside of high school would take. So, we're helping to build the pipeline of cyber-security specialists. That's the only way we're going to solve this problem. We have to get more people interested. We have to invest. This is an investment for us. The program started last year. It's going to kick off with a major part of the curriculum in August, we're going to expand the program nationwide with our footprint. So, our approach is three-fold, expanding our recruiting reach. And at the same time we've put together great retention programs, and building our own talent pool.

ROCK: There are a couple ideas here, we've been kicking around. There are some adult re-education programs such as Per Scholas that will help adults learn technical skills via a very rigorous program. These adults actually become very good candidates because they have demonstrated motivation and maturity as well as the ability to learn the skills. They wouldn't have gone through that program and would never have succeeded in that program if they hadn't shown dedication and ability to stick with it. You can also look at schools and you also get some by poaching from your IT friends, because some of the best security people we've got are the ones who've been doing programming for the last 20 years. What I would challenge every company is look at what you need, and look at what your job requirements say. I have run into a lot of job descriptions that say you must have a four-year-degree and other qualifications that don't actually contribute to the job. Well, if you're looking for an entry level person to do something that doesn't require a four-year-degree out of college, then why are you requiring it? You are eliminating those who have gone through a public education at a high school program or through tech school and they would be just as good. So, don't limit yourself to someone who has completed the four or six years in higher education. I love higher education, I've been there and done that, but that's not necessarily a requirement to qualify some of this young talent that is coming out.

PHOTO: PAULA NORTON

"It's no longer an issue when you have a hacker in the basement just doing something, because he can. So, you have foreign threats and insider threats. Things have really picked up on the government-sponsored cyber-hacking side."

– Terry Williams, Belcan

CARLI: Yes, I would like to add to that. I think the last count I saw was 26,000 CISSP's, and for those of you that don't know, that's the de facto standard for a security certification. It covers all the demands. There are 45,000 job opportunities, so we simply don't have the people, and it's on a tremendous scale. For a company like RoundTower, it's very difficult to recruit and since we are in the business of providing expert resources and advisory services, we do need higher level resources, which is even thinner air as far as resources, but I'm on the same page with them. We're actually leveraging the local university, so for anyone in this room there's the College of Informatics at Northern Kentucky University (NKU.) They have a tremendous program, great security resources come out of there, usually certified on some technologies like Cisco or some firewalls. They also have a very strong and I believe it's with the NSA, they have a certified lab there. We've brought on incident responders and forensics resources that have come from there. At the University of Cincinnati, their engineering department has a tremendous IT/security capability, and as you all know, they have a great co-op program. We call it the minor leagues, where they can come in for six months, work for us, get trained by our resources, and then we can make a solid choice if that's someone we want to keep on. It's almost a better vetting period for it. But to tie in here, the ongoing education, they need to have a mentor. You can't just throw a worker out there and expect them to survive, especially if you're going home grow them. So, keep that in mind. It's not just identifying workers, but it's the education and retaining.

COURIER: I've heard that before. I've heard from many people recently that throwing away old, worn out job descriptions and job requirements is job number one. I know a lot of companies that have had success when they finally let go of a document that was thrown out by somebody that a left long time ago. Anyway, we are right at time and I definitely wanted to open it up for questions. Who has a question for the panel?

AUDIENCE QUESTION: I have three questions. The first one is the philosophy of ransomware and do you encourage businesses to buy into the whole idea of cyber thieves? The second one is – is the general public really buying into the old,' Oh my gosh, my data was breached.' I know I'm not supposed to use the "B" word, or are they just going, well, because of Equifax, my data's out there anyway? The third one is the ethics of using social media in the office, is that a concern for businesses?

WILLIAMS: I do want to talk about social media, it's a concern. One of the things that we encourage, especially with executives, is to be very careful about their social media footprint. I think all employees should do that, because that is one of the places sophisticated hackers are trolling right now. They're getting personal information about you, they're using it in phishing e-mails. So, especially if you're an executive of a company, you have to be extremely careful about your social media footprint. We council out employees as part of our on boarding process about social media do's and don'ts. You are always at risk of inadvertently putting things out there that you typically don't want to put out there, in terms of your work, jobs, other people, and projects that they've worked on. You would be surprised, or maybe you won't be surprised about what people put out on social media. Some companies that have social media guidelines in terms of what you can post, or which forums you can actually participate in. For us, because of the cyber-security work that we do in the government space, that is extremely critical. So, you have to control our social media footprint.

CARLI: I would add to that to test your controls. So, have a third party come in and do a penetration test, or do vulnerability analysis. There are several thousands of companies that do this, independent third parties with zero information. Let them come in and try to run the scenarios as a hacker. Most of the main compliance requirements with PCI or HIPAA, they're mandated to do this, annually. The trend is that they're doing it quarterly, and they're doing it on-demand, because things change so much. Consider bringing in a third party to test those controls if you think you have it in place, and that also provides a remediation roadmap. They will tell you what's unpatched. They will tell you where the low hanging fruit is and you can start using that as part of your security plan, going forward, and then coupled with that you can have them do physical security assessments, and then they also can run targeted spear phishing campaigns. You want to test that end-user population, run a campaign, or run a scenario, and that that allows you to educate executives, by saying, 'Hey, look you know we had a 20 percent pass rate. We got 80 percent of our population click on this.' Those are all important tools to help you justify your program.

PROTECTING YOUR BUSINESS FROM CYBER CRIME

GANOW: To add onto that, people will tell me, 'Well, I don't want to know what's wrong, because if I don't know what's wrong, then I can't be held liable, right?' You've been watching too much television. That's not the way it works. There's a lot of these assessments that you can try to do proactively. If you want to, you can try to do it with attorneys involved and sometimes assert attorney-client privilege. But ignorance is not defense. You are expected to be kicking the tires, trying to poke holes, reasonably, in your budget, trying to know what risks there are. If you're going to traffic in Social Security numbers you better know the security that is around it, or expect the consequences you're going to get from either private litigation or regulatory enforcement.

AUDIENCE QUESTION: I have two questions. One is sort of a piggyback not so much on fatigue, but when consumers as a whole get outraged and how you talk to senior management about the brand and reputational value? Then, we've talked a lot about internal controls, but how are you advising clients on exerting controls on third parties, whether through contract language, ISO's and requirements like that, so that if there's a lot of data sharing, how are we looking externally as well?

ROCK: I will try to take the second one first, relating to the third party. This is a fascinating conversation I have had with most of our clients. In fact, in my prior role in financial services, we seemed to exchange questionnaires with each other every week. It would be laughable if it wasn't chewing up so many internal resources to respond to everyone else's questions. Sometimes, people want to throw a SOC-2 report at us. While that doesn't really give us all the answers, it gives us part of the picture. Then, what do we do? We come back and ask even more questions. It can be very painful. There is a lot of hope in the industry that sooner or later there will be some standards and some services that can stand in the middle and broker that information between all of the third parties so that it provides a level of consistency and a cost savings for member companies in terms of reduced workload. Let's address the fundamental issues here: Number one, put your expectations in the contract. The next thing is to make sure you train them what your expectations are. Then, audit them, because the trust without verify is not a strategy. If you put it into a contract and you stated your requirements, and you've never come behind to check to make sure they are doing it, you're not doing your due diligence. Speaking of due diligence, just because you push your sensitive data to somebody else to hold or process for you, it doesn't make protecting it automatically their responsibility unless put in the contract that we are responsible to secure all of this for you. You still own responsibility for the security of that information. Be very cognizant of where you're pushing that data. This goes back to data governance. If you're going to put it someplace else, it's now your responsibility over there as well.

AUDIENCE QUESTION (same person as previous): I was just more interested in how you were advising, because I've experienced doing it from a contract, but when it's going into a company, whether it's data sharing, or whether you are giving all that data to someone else to hold, it may be a different conversation.

ROCK: It goes back to the question "what's the data?" You have your administrative controls and their technical controls and you're going to assess them. Assessing a partner holding your data is similar to assessing your own company. You need to ask them those technical questions, and then they need to be able to give you relatively clear answers. If you don't know the questions to ask, you need to engage a third party that knows how to ask those questions, and they can come back to you with a recommendation. Again, it's contracts, training, verification. Those are the conversations that need to be had, and if you put all that in writing, and your own company is not willing to actually send someone out there on an annual basis to check, the only value is the words on paper.

WILLIAMS: I think the key thing is, and I'll say three things, audit, audit, audit. The reason why I say that is, because suppliers, especially third-party suppliers, they're very good at preparing for an audit when they know its coming. And, you have to continuously audit a third party supply chain. We are part of a third party supply chain and we audit third party suppliers. So, one of the things we do are spot audits. They are unannounced. It's no longer an issue of these third parties in terms of price and delivery. The first thing on the list right now is compliance, and how they are protecting IP, how they are protecting your data and how they are managing your data. All of those things should be part of an audit process. Like I said, companies have become very sophisticated and prepared for audits. It's a science for them. So you really have to have to make sure that you're catching them in their normal state of operations.

AUDIENCE RESPONSE (same person as above): I think it's so important for a third party. You mentioned at the beginning of the conversation about how a lot of the incidents occur not because of faults on your system, but through third parties.

WILLIAMS: That's where the new attack mechanism is. There's no doubt about that.

GANOW: Manage that privacy concern and customer outrage like you would any other customer satisfaction concern and you will eliminate 50 percent of your problems. People are reasonable, and this is the thing about "breach fatigue." People get it, unfortunately. They just want to feel heard. They want to know you are on top of it, and you're taking their concerns seriously. That's business 101.

ROCK: The advice that I've heard from a lot of public relations firms is come out, be forthcoming, be truthful. Tell them what you know, tell them what you don't know and when you are going to get back to them, and then it's almost a non-event these days. Companies that cover up, or just say, 'no comment,' those are the ones that attract the media attention. That's probably where you don't want to be. From a PR standpoint, it's easier to be straight-up and honest, and make it a non-event, and not only that, you are displaying a level of integrity that your customers can appreciate.

AUDIENCE QUESTION: Mike, you mentioned earlier about AWS Cloud Services. It could be AWS, it could be Google, Microsoft, or another company. Our firm helps business owners with the cyber liability insurance. We tell business owners whether you have 50 employees or 500 employees, two locations or 20 locations, to get with your law firm, draft your plans properly, get with your IT professionals and draft the plans accordingly, and the insurance is a safety net, if and when you get hacked, because 50 percent of small businesses go bankrupt, they don't have a quarter of a million or $300,000 or $400,000 saved aside to fund the forensics, the credit monitoring, or the breach notification across 40 or 50 states, or whatever. I'm amazed at how often a business owner will say we outsource everything to The Cloud, so that's Amazon, or Microsoft is Google's problem, and to your point, Scot, they sign up on the internet with a 45-page contract, and who knows how well they've read it, and somewhere around page 18, clause D4, there's a hold harmless clause from Amazon, Microsoft or Google, (with) a limitation of liability that basically says, if we're breached, we are only going to give you back what you paid us. If you paid us $20,000 in legal fees, we will give that back to you, we're not on the hook for everything else because you originated the data, it's your customer list, whatever. Is that what you're seeing in some of these contracts with some of these Cloud service providers?

ROCK: What you say is true with the limitations and liability. If you dig deep enough, it's probably around page 30, they start to talk about or tell you the data you're not allowed to put out there. So, there are some Cloud services that say 'don't put personal identifying information out here, because we don't protect it'. Sometimes, you may purchase a base-level storage service, not reading what they tell you not to put out there, because they're not backing it up. That's additional cost. They don't have all the security controls in place you may need, that's another additional cost. My recommendation to companies is if you're going to move to 'The Cloud' you might as well mentally kick in 10 to 15 percent higher costs to secure it. A lot of those features you're expecting to be there may not because you didn't read page 30. As Scot said, ignorance is not an excuse.

WILLIAMS: Yes, I agree with that. I think that for smaller companies, even in some mid-sized companies, it is an improvement on some of the practices and security. Now, what I would say is that there is a distinct difference between the typical AWS services or some of the Gov Cloud services that they offer. So, if you read the contracts between the two a lot of the Gov Cloud services have a lot more protection than the typical AWS services.

COURIER: We are out of time. Thank you to everyone one for coming and thanks to our experts for sharing with us about some of the latest cyber security issues.