TABLE of EXPERTS

CYBERSECURITY

Businesses across the country are grappling with security concerns about their devices, their data and more. What does it mean to be secure in an age of massive data breaches? The *Albany Business Review* hosted an industry discussion on best practices for keeping information secure and how new regulations could impact businesses.

Let's start the panel off with an easy lay-up question: What is cybersecurity?

Vigorito: I would say cybersecurity is the evolution of policies, procedures, technology and concepts that are designed to protect information in all of its forms. It's really top of mind for many organizations, as it should be, as any security matter, even physical security, should be.

I saw a survey of Fortune 500 CEOs, which indicated that, for the past three years running, their number one concern is data privacy and cybersecurity. Joe, why is cybersecurity important to businesses?

Vigorito: If you adhere to some of the statistics that are out there, the average cost of a data breach, is about $3.79 million. And that's as per the company FireEye and their arm for threat intelligence, which is Mandiant. Let's say that is heavily skewed towards the JP Morgan Chases and the Bank of Americas of the world. So let's say the average cost of a cyber breach is just a little under $2 million. For most organizations, especially those in the SMB space, $2 million would be a substantial hit to that business and would impair them in a probably fairly significant way. Cybersecurity is important because of the fact that it is one of the areas that can bring an organization absolutely to its knees in terms of its ability to perform its operations, its function, its security, and operate as an ongoing entity.

Chris, what do you have to add from the legal practitioner's perspective?

Meyer: Companies have been concerned about security for decades. Companies have been dealing with cybersecurity for 30 and 40 years. It's only recently that we've seen in the newspapers major cyber events that have caused people to stand up and take notice. In the past, cyber incidents were generally viewed as technical issues. They've now become viewed as major business issues where it's not just the IT department and the head of IT who's losing his job if there is a cyber breach.

What is ransomware and how does it impact companies; and should companies pay for it?

Meyer: Not all companies are necessarily concerned top of mind about a data breach. Ransomware is terrifying because you walk in one day, sit down at your computer, turn it on, and you get a message that all of your files have been encrypted and you don't have access to them anymore, which means you can't run your business. A company with good backups generally can recover from a ransomware incident very quickly. What we've seen is that, in general terms, ransomware attacks are very smart. People behind them understand that if they charge an enormous amount of money, people won't pay. So the dollar figures are relatively small. It might be $5,000, $10,000, $15,000, which makes for a very effective business model for a cyber criminal to be able to hit an organization. So a lot of companies make that choice, we're going to pay, because it's a lot cheaper to pay $5- or $10,000 than it is to try to reconstruct our systems.

So it would not be advisable business to contact law enforcement, to ask the state police or FBI to intervene in a cyber ransom attack?

Meyer: I think it's always advisable to contact law enforcement and see what assistance they're able to render. The unfortunate reality, however, is ransomware is so prevalent and law enforcement is so busy, it's not always possible for them to respond to your specific incident in a time that you consider appropriate.

Joe, from the technology solutions point of view, what have you seen and what do you advise for companies to do with respect to cyber ransomware?

Vigorito: I think ransomware is the electronic, economic crime of our time. $209 million lost just in Q1 of last year. I think the total tally for 2016 will end up close to a billion dollars. From a technological standpoint, not only have great backups, but have good tested offline backups. And take those backup copies to multiple mount points. Put one up in the cloud, put one on tape, put one in a virtual library. The other point, is one of awareness and education and training. 76% of ransomware is born out of somebody clicking on a bogus e-mail that has an attachment or has had a web link. The other advice that I would give is time is not your friend. The longer you wait when you get hit with ransomware, the worse off you are, because the extortionist will quickly move onto many others. The last thing is negotiate the dollar amount. But again, only offer to pay if you question the validity of your backup strategy and your recovery strategy.

Once an organization has been hit with a ransomware attack and it has paid to have access to their data, what should be their next steps?

Meyer: If you are an organization that found it necessary to pay, you probably have some things to take care of in terms of your procedures. Organizations, as a general rule, do not like to spend money to prevent issues when they're focused on running their business. When companies are hit in any environment, those are the opportunities where they step back and say maybe we need to invest more resources into getting our systems in line, making sure we're doing the things we need to do to reduce our vulnerabilities in the future.

Do companies have an obligation to provide notice to their customers, their shareholders, their vendors or their parent corporations, affiliates, that they have suffered a cyber attack? And if so, what forms would that notice take?

Meyer: It depends highly on what industry they're involved in and it depends on what their business practices are. There are 47 states at last count that have data breach notification requirements, including New York. Figuring out what industry you're in, what regulation applies, how it applies, and whether the breach that you've experienced is one that requires notification, is extremely time consuming and extremely expensive.

Joe, can you give us some insight into the disciplines and the components that will allow an

organization to have an effective program for cybersecurity?

Vigorito: Sure. We often cite comparing as a baseline against NIST 088-53, National Institute of Standards and Technology. Or if you want to go more towards risk, move towards NIST 800-30, which deals with risk of controls and issues in an information technology environment. I usually tell organizations these things to focus in on. The first is data classification. If you don't know where your data is, and who has access to it, that's a non-negotiable first starting point. The second piece we always talk about is data governance. And then the last piece that we'll talk about is who reports. Christopher did a great job of highlighting the interest of boards and senior executives of organizations. Who's making the final judgment call? Then the other two areas, which I'll just spend a second on, one is asset discovery. Most organizations – I think the number is 64 percent – do not know all the devices and all of the applications and all of the databases that are in their environment. And then the last is device control. Do you actually have control over who uses what for what purpose? If you do things well, those should really be the only policies needed.

Chris, do you advise your clients to adopt a particular framework, such as the NIST cybersecurity framework or ISO 27001, or you mentioned 800-30? What should they grab onto as their starting point for figuring out their program?

Vigorito: When you're doing a risk assessment, you've got to have something which is an accepted standard to benchmark against. We do advise clients to look closely at benchmarking. The reason why we like the NIST standards the best is they map very well to other compliance initiatives. Once you've established that standard, then you need to go through the process of reviewing each part. You're not going to be in full compliance with any of those standards. I think very few organizations ever would be, even those who spend a tremendous amount of money on cybersecurity. Your goal is one of continuous improvement. I'll just make this one final comment about New York state DFS with that respect, which is, they say you don't have to redo your risk assessment every single year. I don't know any organizations that don't change in a year, so I don't see how you can easily get away from doing the risk assessment on an annual basis.

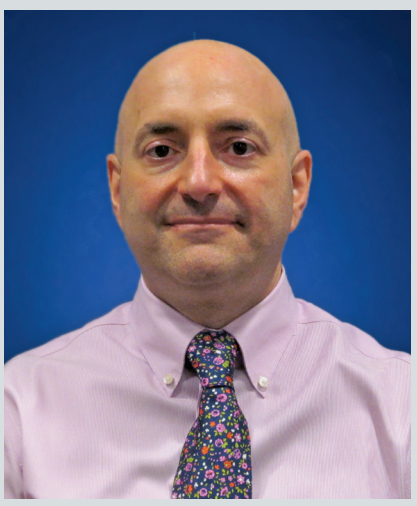
Chris Meyer from Whiteman Osterman & Hanna, left, and Joe Vigorito from Annese & Associates.

KRISTINA WALSER

Chris, how do you advise your clients from the legal point of view regarding creating an effective cybersecurity program?

Meyer: I think Joe would probably agree with this, that there's a tremendous difference between compliance and security. One of the difficulties with all of the regulations across the board, be it HIPPA, new DFS regulations, really anywhere you look, is this issue of are you, as an organization, compliant? Are you, as an organization, secure? When we look at the new DFS regulations, you could go through those and build a program that complies very inexpensive-

MEET THE PANELISTS



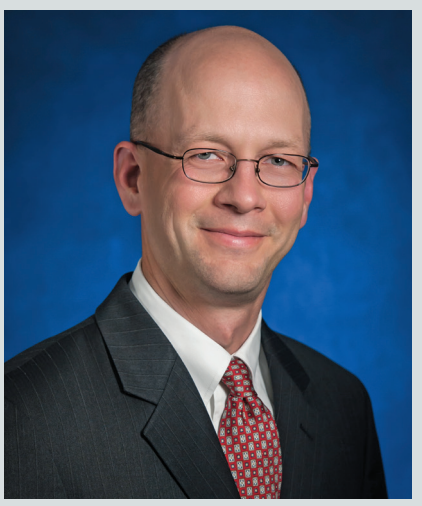
JOE VIGORITO

Director of Mobility & Security
Annese & Associates, Inc.

Joe Vigorito is the Director of Mobility & Security at Annese & Associates, Inc. With more than 20 years of experience in the industry, Joe is a highly certified and seasoned security professional. He achieved a Masters degree in Information Systems Engineering from New York University-Polytechnic School of Engineering, and holds a Bachelor of Science degree in Communications from St. John's University. Joe is a Fellow & Diplomate at the American Board for Certification in Homeland Security, and is also a member of the American College of Forensic Examiners, ISSA, IEEE, BICSI, and FBI-Infragard.

Annese is a technology solutions integrator with more than four decades of experience in the IT industry. The company, headquartered in Clifton Park, has over 150 employees, and serves both public and private sector clients in education, commercial, government, and healthcare throughout New York State and New England. More information can be obtained on their website at www.annese.com.

ANNESE
INTEGRATED TECHNOLOGY SOLUTIONS



CHRIS MEYER

Of Counsel
Whiteman Osterman & Hanna

Chris Meyer is an attorney with Whiteman Osterman & Hanna in Albany. He helps clients protect and use their information assets in corporate and litigation matters involving privacy, cybersecurity, cyberinsurance, data retention, intellectual property rights, defamation, and other information-related issues. He also has experience in matters involving antitrust, labor and employment, contract, and corporate governance issues.

Chris holds a certification as an Information Privacy Professional (CIPP/US) from the International Association of Privacy Professionals, which is open to both attorneys and non-attorneys with demonstrated knowledge of privacy-related issues. Chris is the Chair-Elect of the Chamber of Southern Saratoga County. Chris graduated from the Washington & Lee University School of Law (JD), SUNY-Albany (MA), and Trinity University (BA).

WHITEMAN OSTERMAN & HANNA LLP
ATTORNEYS AT LAW

ly with those regulations. But it doesn't mean that you're necessarily secure. As companies are trying to figure out what they're going to do, I think more and more are coming to the perspective of, "We're going to approach this responsibly, we're going to protect our assets the best we can, and we're going to document our processes in a way that, if we ever have a problem, we can go back and explain what we did and why we did it. If we are technically non-compliant in a particular area, that's something that we're going to have to deal with and decide is the risk of being technically non-compliant worth it."

There's also the potential cost of litigation. So from a litigation point of view, do not companies minimize their potential legal liability by focusing on compliance and having a checklist and saying we did the standard, as opposed to focusing on security where they may or may not be technically in compliance, but they are more secure?

Meyer: That's an excellent question and it's an extremely difficult area, because in many industries, failure to comply with a regulation is used as evidence of negligence later on. The more regulations that are put down, the more there's an incentive for companies to check off the box and say, "Well, we're compliant." But again, it's a constant conversation between the legal, business and security professionals to figure out where an organization is most comfortable.

that they're less vulnerable?

Vigorito: One of the things that we bring to customers is kind of this campaign-based continuous learning. In my organization, we'll actually take a client and send all of their people phished e-mails on a monthly, quarterly – whatever the program is that they would like to enlist – basis. The other thing that we will absolutely do is put some structure around the awareness element. We should put some automation in place that says, hey, look, from a data loss prevention standpoint, we are going to look for places where there's proprietary, confidential, intellectual property, trade secretes, et cetera, information leaving the walls of an organization. Very often, it's not being done with malicious intent and it's not being done with the focus on trying to harm the financial entity or the business unit of any type.

Joe, if I'm in an organization that's already following the NIST cybersecurity framework or Gramm-Leach-Bliley Act's framework, then am I also compliant with New York State's Department of Financial Services cybersecurity already, or do I need to do more to be compliant?

Vigorito: The answer, Antony, is you may be compliant. If you're one of the major banks in New York City, you're Bank of New York, BNY Mellon, you're Bank of America, you're JP Morgan Chase, everything in New York State DFS is foundational in nature. Odds

> *"Companies have been dealing with cybersecurity for 30 and 40 years. It's only recently that we've seen in the newspapers major cyber events that have caused people to stand up and take notice."*
>
> **CHRIS MEYER,** Of Counsel at Whiteman Osterman & Hanna

I think we set the stage for discussing the Department of Financial Services' new regulations. At Albany Law School, some of our students provided feedback on regulations. And one of the early versions talked about requiring financial institutions to encrypt non-public information. I believe in the final version that's been retracted. I'd like to begin with some perspective from Chris on the current version. Are we in the right place? Do we need to have more modifications? And then also, what can businesses do to make sure that they are compliant?

Meyer: The initial version of the regulations were heavily compliance-based. And the necessary reaction from the business community was we can't achieve this because, as Joe suggested, there are other standards out there that take a diametrically different approach, where it's heavily risk-based. I think the DFS did a nice job in responding to over 150 comments in saying, OK, we understand that perspective and we're going to issue revised regulations. There's been discussion that these regulations impact very small organizations. It will be very interesting to see how people confront those challenges. Whether that program necessarily provides enhanced security is an open question.

Joe, I believe two-thirds of all outlaw hacker breaches go back to the employees. What is it that organizations can do to help organizations better prepare their employee awareness so are, those organizations are already in full, and if not in full, in the majority, in compliance. But the reality is you could be compliant with GLBA or GPDR and not necessarily be in compliance with New York State DFS because New York State DFS has a bit of nuance to it. And some of that nuance may bring some new elements to a lot of organizations.

Regardless of the size of your organization, where should primary responsibility for cybersecurity and data privacy rest? Should it be a single person, a single department? And then how does that impact the financial institution's compliance with the DFS regs?

Meyer: It's made very clear in the DFS regulations that the expectation is that senior management and the board of directors will be knowledgeable about cybersecurity and they will be knowledgeable about the steps being taken by their organization. And it really has transitioned into a core business function for all organizations to be concerned about.

How would you advise a chief executive or a chairman of the board in how they can make sure that they are up to speed in their organization's cyber and privacy policies, as well as the industry standards for cyber and privacy?

Meyer: I think we find that, for most business organizations, executives don't get to where they are without having a really good appreciation for how their business runs and what their risk factors are. In terms of what they need to do to become personally aware is that it does require spending time with the chief information security officer, spending time understanding, OK, in the last year, we've been hit 10 times, 50 times, 100,000 times, with attempts to get into our systems. If you don't understand the technical speak, really drive down and get someone to translate between the IT department and the executives to understand in real business terms what are we talking about.

What are some of the sources that you advise your clients to rely upon or that you use personally to stay informed?

Vigorito: From the security perspective, the places I go most often are mep.nist.gov, which I think is a fabulous source of up-to-date vulnerability information which is put out there by NIST ... Of all the exposures and exploits that happened in 2016, 99 percent of them were preventable. Where do you go to find a lot of that information? Well, you go to mitre.org, which is, again, well-known, funded in large part by the federal government ... Another place for full disclosure on security vulnerabilities is SECLISTS, seclists.org/fulldisclosure ... And then certainly, obviously, reading a plethora of postings for people exactly like Christopher about specific compliance regs, and then exposing myself and reading 23 NYCRR 500, for example, cover to cover, always is an aid.

Chris, where do you go for staying up to date on these issues, and where do you advise your clients to go?

Meyer: I think the starting point is always the regulations themselves. There's many helpful comments that were submitted, for example, in response to the DFS regulations. From the legal perspective, there are organizations out there that are tracking this that are spending a lot of time. One organization in particular, the International Association of Privacy Professionals, is a collection of both attorneys and non-attorneys who are interested in privacy and, increasingly, security issues, that does a lot of continuing education on these issues where there is a lot of conversation. There are conferences that one can go to [to] learn about these things, the RSA conference out in San Francisco being probably the leading one.

Vigorito: The attacks are fairly unrelenting. So I think we have to continue to evolve, continue to get better at what we're doing. That means we need to intellectualize and kind of bring cyber to the forefront of every employee's thinking. You asked Antony before about who's responsible ultimately. I would say, in an organization, everyone has to have some responsibility.

Meyer: In terms of designing a security program and working with employees and creating a culture of security, one of the effective tools that needs to be in the tool chest is to find ways to incentivize employees to do something in a positive way.

What predictions do you have for cybersecurity going forward, 2017, 2018; what are some of the trends you see emerging that we should be preparing for?

Meyer: Cybersecurity has become and will be in the future a core business function. So when we look at just looking at the legal practice, cybersecurity and privacy issues now touch every practice area I can think of.

Vigorito: I think you'll see the emergence of the CISO becoming more and more of a chief risk officer. We're

already seeing a lot of organizations name a CRO, or they'll have a directorship level person who will own that responsibility. I think you'll see them become less and less technical over time, more and more business savvy and business oriented. I think you'll see a major attack this year. We saw two last year that were interrelated, one in October, one in November. Last but not least, I think we will see ransomware not only continue, but continue to evolve. I think the attacks will become more disruptive in nature. We're already seeing signs of threats, not of encryption, but of system destruction.

One of the big issues for many organizations is cybersecurity insurance. Should organizations pursue it, and if so, what questions should they ask to make sure they have the appropriate policy?

Meyer: Cyber insurance is really an emerging product for may insurers. I think that in large measure, both the issuers and those buying the policies are finding their way. It's an area where there's really very little experience, both in terms of the policies that should be issued and the claims experience after the fact. So from an insurance perspective, I think a lot of companies look at it and say, having insurance is a good idea. Figuring out the appropriate policy to find, whether the organization can afford to pay it, and at the end of the day, whether it's going to provide them adequate protection, is still a very emerging area, and it's probably going to take several years until there's a real solid foundation underneath it. Every insurance policy comes with coverages that are applicable, but often also comes with requirements that you need to fulfill. In the cybersecurity area, it's extraordinarily tricky really because the policies are new and because the threat profiles are constantly changing.

Vigorito: I would say ask your carrier if they do this regularly, is this something they have a lot of expertise in, how long have they been doing it, what types of organizations, is it in your particular space, in your vertical, in your marketplace, before you go ahead and go down that road. If not, "shop around" is really the theme. Shop for organizations who write very specific cyber policies.

What is the Internet of Things and what cybersecurity challenge does it raise for businesses?

Meyer: The Internet of things really embraces everything that's connected to the Internet, other than a computer or a tablet. Think of it in terms of your home thermostat, your video cameras, security monitoring system, pacemakers that are Internet connected. The great vulnerability for businesses is the Internet of things is largely outside of their control. Many, many, many businesses are moving their operations

The panel discussion, from left: Moderator Antony Haynes of Albany Law School, Chris Meyer of Whiteman Osterman and Hanna and Joe Vigorito of Annese & Associates.

KRISTINA WALSER

to the cloud. They're moving their file systems to the cloud, they're moving their accounting systems to the cloud, which is all good, except on that day that the Internet goes down because of the IOT. If the Internet goes down for three days and you're a hospital, and all of your systems have moved to the cloud and you can't access them for whatever reason, that's a business risk. That's where you start to think about, well, "do we have to have redundancies?" So from that perspective, it's frightening, because it's entirely outside of your control.

If there was a compromise created by Zombie or Botnet, if thousands, if not millions, of machines attack Yahoo and other sites to bring it down, who should be liable? Is anyone liable? Is the manufacturer of the digital videorecorder liable? Is it the home user? Is no one liable? Is this a gray area where there's an accident but no one's responsible for the accident?

Meyer: It's a great question and I don't think there's any resolution. That's a very significant public policy, social policy issue that has yet to be resolved. And it touches not only on cybersecurity issues, but one of the areas that has increasingly become important, and we're going to see much more -- we'll probably have the same conversation a year or two from now – is in the area of artificial intelligence and machine learning.

Vigorito: The big problem to date with IOT, and maybe there's some hope on the horizon, is that the device itself cannot withstand a lot of the security software that we might apply in a traditional environment. So you're saying, why don't we just put antivirus software on the IOT device? The device isn't manufactured to do that. It's lightweight both in terms – very often in terms of form factor, but it's also lightweight in terms of its capacity, its ability to absorb tools like that. So that's something that I think a lot of the security software manufacturers are looking closely at, trying to come up with some sort of tool or solution or secure operating system that can be applied to devices like that to help protect them.

Meyer: In closing, although this discussion is part of the *Business Review*'s "Table of Experts" series, I think that today's conversation made clear that the term "expert" does not fit very well when talking about cybersecurity and especially when talking about legal issues in cybersecurity. The rapid pace of change – with near daily appearance of new cyber threats, technologies and regulations – requires ongoing study to remain current on the latest developments. Before taking any action, organizations should always consult with their legal counsel and security professionals about their specific situation.

TRANSCRIPT LIGHTLY EDITED FOR SPACE AND CLARITY.

Thank you to our participants

ANNESE
INTEGRATED TECHNOLOGY SOLUTIONS

WHITEMAN
OSTERMAN
& HANNA LLP
ATTORNEYS AT LAW