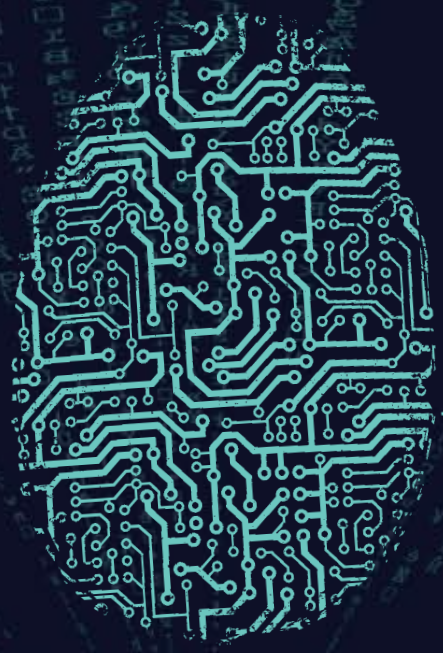
Special Section

CYBERSECURITY



Each time we compile a special section on cybersecurity, we're struck by how many new developments there are. Akin Gump litigator Michelle Reed leads off with an analysis of the New York Department of Financial Service's new regulations. We hear from IBM's first chief cybersecurity counsel, followed by advice on improving oversight in the boardroom. We close out with a briefing on ransomware attacks, a warning on pitfalls when purchasing cyber insurance and an exhortation on how in-house lawyers can play a larger role in this area.

Getting in Line with the New Regulations

Cybersecurity rules from the New York Department of Financial Services are broad and complicated

***Michelle Reed**, a litigator at **Akin Gump Strauss Hauer & Feld LLP** and co-leader of the firm's cybersecurity privacy and data protection group, breaks down what the New York Department of Financial Services' new cybersecurity regulations mean for covered entities and the in-house counsel who advise them. Her remarks have been edited for length and style.*

The New York Department of Financial Services (NYDFS) recently revised its cybersecurity regulations for covered entities, with compliance required as early as February 15, 2018. Who will be impacted and how?

Michelle Reed: The NYDFS cybersecurity regulations are really the first of their kind nationwide. The regulations apply to covered entities: state chartered banks, licensed lenders, private bankers, mortgage companies, insurance companies and other service providers. There are certain exemptions, but they're pretty limited.

The regulations were effective in March of this year, and many of the requirements actually needed to be adhered to as of August 28. That means by August 28 each covered institution had to adopt a robust cybersecurity program. NYDFS provides solid detail of what it expects in that cybersecurity program. For example, you need to identify your cybersecurity threats. Companies need to employ defense infrastructure that would protect against those threats. They need to have a system to detect what's happening and a system to respond. Once companies respond, they have to fulfill different regulatory reporting. People who work in the cybersecurity industry are going to be familiar with this because it parallels the National Institute of Standards and Technology's cybersecurity framework.

There's an expectation that any organization will have this robust cybersecurity program and a comprehensive cybersecurity policy. This policy is specifically going to cover information security, access control (who has access to what and how) and disaster recovery in the event of a total system shutdown or a ransomware attack (so that your company can get back up to speed). It also requires that companies have policies regarding systems – network security and data privacy. And then, most importantly, that they provide regular risk assessments. All of these policies needed to be adopted by August.

NYDFS expects a qualified chief information security officer (CISO) to oversee and implement the cyber program. Many companies may have a chief information officer or network security administrator who's filling that role, but they don't actually have a CISO designated. Third parties can also be hired to fill this role.

Additionally, NYDFS has an expectation that personnel will be trained to manage through these various cybersecurity risks. And companies are expected to notify the NYDFS of all material cybersecurity events. For those that carry a reasonable likelihood of causing material harm, companies also have to limit access privileges. They should make sure that privileged access is not being given to a wide variety of users, but instead access is very limited. In a breach situation, privileged access can often determine how extensive the damage will be. These are the requirements that need to be addressed by August 28.

Michelle Reed *is a litigator at Akin Gump Strauss Hauer & Feld LLP and co-leader of the firm's cybersecurity, privacy and data protection practice. She specializes in advising clients on data breach investigations, notifications and subsequent litigation. She can be reached at mreed@akingump.com.*

What are the exemptions to the revised regulations?

Reed: There are not many, but if you're a small company, there are some. A covered entity with less than $5 million in gross annual revenue in each of the last three fiscal years, fewer than 10 employees or less than $10 million in year-end assets total is exempt. A company that is an employee agent, representative or designee of a covered entity that itself is covered by the cybersecurity program is exempt. So is an entity that does not operate, maintain, utilize or control any information or does not control, access, generate, receive or possess nonpublic information. But they must be rare because virtually every company has some kind of nonpublic information that is going to require protection.

The other piece that I think is important is that the rules allow for some assessment of your own entity, and when you did your cybersecurity risk assessment, they allow for some scaling based on what it showed. That doesn't mean that your company is exempt, but there is some flexibility with certain requirements. For example, Section 500.12(b) on multifactor authentication says that a company can use a different method to control access to data if the CISO makes a specific finding that the alternative method is a reasonably equivalent arrangement.

Who are the enforcement officials for these regulations?

Reed: Ultimately, you're going to be dealing with the NYDFS, Financial Frauds and Consumer Protection Division (FFCPD) and potentially the state attorney general, depending on the issue.

If you say, "I don't fall under one of these covered entities, and I'm not subject to the NYDFS, so I don't need to worry about any of this," my recommendation is to take a step back and ask, "What am I subject to?" You do business across the United States. There are varying state laws and regulations that address some of these requirements. Companies need to know where they are operating and what the applicable standards are. Most states have notice requirements, as opposed to technical cybersecurity requirements like NYDFS, but in that case, your company is subject to any state attorney general in the United States. If you're an international business, you'll soon be dealing with the EU's general date protection regulation (GDPR). There are many technical requirements and notification obligations associated with that – and subject to the data protection authority (DPA) in the various European countries.

Do you think the New York threshold is higher or lower than the GDPR standards?

Reed: I wouldn't characterize it as higher or lower; it's just different. There are probably aspects that are more rigorous, but there are aspects that are not. Some of the privacy

Continued on page 3

Continued from page 2

by design requirements in GDPR are significant, but the New York standard also contains significant responsibilities; for example, encryption. The base level expectation is that you're encrypted in transit, encrypted at rest. That's a significant requirement that requires a real investment from companies and can impact day-to-day operations. The reality is that both of these regulations demonstrate that regulators are going to take a more detailed, compliance-heavy approach with cybersecurity than they have in the past.

The regulations require entities to "establish a written incidence response plan designed to promptly respond to and recover from any cybersecurity event materially affecting the confidentiality, integrity or availability of the covered entity's information systems or the continuing functionality of any aspect of the covered entities business or operations." Would you talk about the materiality threshold?

Reed: This materiality threshold is going to be a bit of a moving target in terms of understanding what is going to require reporting and what is not. Those who don't deal with cybersecurity regularly think, "Well, it's simple. You have an event and therefore you report it." What people don't realize is that a lot of these companies are experiencing thousands of events a day, of varying success levels.

Evaluating what is material is important for an in-house lawyer and sometimes requires seeking outside counsel's advice in determining what materiality means. There are lots of contexts in which we assess materiality, but in general, something material is not trivial. Under securities laws, you look at the total mix of information, then characterize it based on the risk of harm and likelihood of occurrence of that harm.

For example, if you had an event that was a low likelihood of occurrence but a high degree of harm, you may find that material. On the flip side, if you have something that is highly likely to occur, but it's not going to impact the company at all, then a lot of times you consider that not to be material. To apply that to the cybersecurity context, you want to look at events that happened and ask questions. What happened? Did they gain access to information? Did they gain access to credentials? Was any information exfiltrated? If it was some sort of Distributed Denial of Service (DDoS) or ransomware attack, how did that harm our website availability for business or our ability to conduct business if our systems were encrypted? Once you consider all of the information from a particular attack, it becomes clearer whether something is trivial or not trivial, material or immaterial.

One of the tricky parts of the NYDFS regulations is the requirement for reporting if there's a cybersecurity event that had a reasonable likelihood of materially harming any material part of normal operations of a covered entity. This is difficult because it is assuming that the attack was not successful. A lot of people would ask, "If an attack was not successful, how can that be material?" This goes back to the likelihood of occurrence and the magnitude of harm. If you have an attack that wasn't successful but could have a significant impact on your business, that may be required to be reported under section 500.1782 of the New York regulations.

A question that's going to evolve over time is an attack that may be material now might not be in a few years, depending on what our resources are and our abilities are to protect against it. It helps to talk to someone who has been through this so that they can evaluate whether or not something is material for the purposes of reporting.

What are the implications in terms of training to execute an incident response plan?

Reed: There is not a great way to implement an incident response plan without testing it. You really need to test it and train the people who are designated to respond so that they know what they're doing. I work with clients to establish incident response plans. We come up with what we think is going to be a good fit for a particular company, and there isn't an incident response plan that you can take from one company and drop into another because companies operate so differently. We'll think the plan is great, and then we'll test it. We'll do a tabletop exercise where we come up with a hypothetical scenario and run through a breach. We gather the team, figure out how they're going to respond, and in connection with that tabletop scenario, discover we hadn't thought about this question, that question and the other question. Maybe an employee doesn't even know how to report the incident, you don't have an incident response hotline or you don't have a clear establishment amongst your employee base on how to report the incident. Maybe you don't know at what threshold to report up to the board. Maybe your information security team doesn't have proper authority to shut down a ransomware attack fast enough. Maybe PR wasn't looped in to begin with and then issued inconsistent statements or otherwise wasn't consulted early enough to frame the response. There are so many different problems that happen with incident response.

Stepping back and evaluating that by going through your hypothetical scenario will ultimately make your response to an actual breach infinitely better. Every company at some point will have a data breach. The way it is going to be judged by the regulators, by its customers, by its employees is going to impact its long-term public relations battle, its regulatory battle and ultimately its legal position in the ongoing litigation. How you respond matters, and investing in testing matters.

What is the in-house lawyer's role in cybersecurity for covered entities?

Reed: The regulation doesn't explicitly state that there are obligations for the in-house attorney. When you evaluate the regulation, however, it becomes very clear that in-house attorneys play a critical role in helping frame and provide follow-up for the cybersecurity protections of various financial institutions. It is important for the in-house lawyer to take the lead in making sure that there is compliance. So the lawyer is going to want to look at things like incident response. Do we have a plan? What is my role as an in-house attorney in responding to incidents? Breech notifications – what are we going to do if we have to notify? Do we know what our contractual obligations are? Do we know what our statutory obligations are? Vendor management is a huge part of an in-house attorney's job, and I think a big headache for a lot of them. In-house lawyers constantly deal with third parties and vendor contracts. What are the requirements for those vendors, what audits have been done in connection with that and what follow-ups are critical for the in-house attorneys to understand and to encourage?

Then, of course, there's compliance. You can have policies all you want, but if you're not complying, it ultimately doesn't get the company where it needs to be from a cybersecurity standpoint. The in-house lawyer plays a critical role in helping ensure that a company is compliant with the policies that have been adopted.

What do the revised regulations state about breach notification, and how can in-house lawyers navigate the various breach notification rules?

Reed: The current regulations set forth a materiality standard for reporting within 72 hours of the determination that the event requires notice to any government body, self-regulatory agency or other supervisory body or has a reasonable likelihood of materially harming any material part of the normal operations of the covered entity. In the data breach world, 72 hours is a really short time line.

That doesn't mean that if you have a breach and you realize there is a problem, it's 72 hours from the time someone told you, "We may have bad guys in our system." That's not the rule. The rule is 72 hours from the time you've made a determination that you may have to provide notice. That gives you some time. Why does that make a difference? Because typically, the notice provisions are going to be triggered by what data was taken or accessed. If the data contained nonpublic personal information, then you're likely going to have a reporting duty.

But it can be difficult to know when the decision that notification would be required was reached. You have to have someone who is familiar with the rules and the decision-making process on when to notify, how you determined it, how you determined what data was accessed, how you determined if it was a successful breach or an unsuccessful breach. These are technical questions but also legal questions. That's why the in-house attorney has a substantial role in making that happen and making that determination.

The revised regulations call for written policies and procedures designed to ensure the security of information accessible to or held by third-party service providers. How can in-house counsel best achieve compliance with this portion of the regulation?

Reed: In my opinion, this is one of the hardest things to implement for a company. Most financial services companies of any size are pretty sophisticated in their cybersecurity governance and their cybersecurity policies. What is really challenging is for companies to come up with a procedure for handling third-party service providers. For this reason, the regulations give two years for compliance with this piece. I think the regulators recognize that this is going to take a long time to get in order, so this is not required until March 1, 2019.

Lawyers should be looking at helping develop third-party management programs. Make sure that you know where your contracts are, that you conduct ongoing diligence, and that you documented it. A big pitfall for a lot of companies is that they do due diligence when they bring on a new vendor, then never do due diligence again. Negotiate contractual provisions that address issues with respect to cybersecurity – access control, encryption, warranties on policies and procedures related to cybersecurity – and of course and importantly, notification of cybersecurity events. Under these new regulations regarding vendor management, you want to make sure that you have explicitly contractually provided for the data breach notification and security obligations so that you can comply with your own procedures and the NYDFS regulations.

What do covered entities need to know about data retention, encryption and multifactor authentication?

Reed: With respect to data retention, covered entities must have policies and procedures for disposal of nonpublic information that's not needed for business operations or other legitimate business purposes. I'm so happy that they put this in there because the best way to protect yourself against a cyber event is to have less data. Some of the worst things that come out of data breaches are not necessarily current data. It could be data from a long time ago that can make quite a public splash once it's made public by hackers.

The regulations require multifactor authentication only for individuals accessing internal networks from an external network. The CISO would have to approve reasonably equivalent or more secure access controls to opt out.

On encryption, you're going to have encryption requirements for data in transit and at rest. And that's going to cause some growing pains for lots of companies.

Meet IBM's First Cybersecurity Counsel

It helps that he also has public-sector experience

***Andrew Tannenbaum** is the first chief cybersecurity counsel hired by International Business Machines Corporation (**IBM**). Before he was hired for this position, he spent a decade as a national security lawyer. He worked in Washington for the U.S. Department of Justice (DOJ), first as a litigator handling national security cases, then as a legal and policy advisor on issues involving privacy, government surveillance, terrorism and detainees at Guantanamo Bay. In his later years at the DOJ, he was one of the first lawyers in the National Security Division to cover cybersecurity. This experience led to a job at the National Security Agency (NSA) that was also focused on cybersecurity, which in turn segued to the position at IBM. We were eager to talk to Tannenbaum about the perspective he's gained from working on cybersecurity in pioneering positions in both the public and private sectors. The interview has been edited for style and length.*

What did you do during your year at the NSA?

Andrew Tannenbaum: I was brought in as a deputy general counsel. At the time it was a newly created deputy role focused on cybersecurity, which reflected the importance of cyber as an issue in the government and across the national security landscape. The NSA had two sides of the house – the surveillance side, which is focused on accessing the systems of foreign adversaries for intelligence purposes, and the flip side of information assurance, which is the protection of U.S. national security systems against intrusions by foreign adversaries. Those two operational issues previously had fallen under one deputy general counsel, but because cyber had become such an issue, they broke it out into a separate role. And that's the role I stepped into.

Were you primarily focused on protecting the government from attacks?

Tannenbaum: We were focused on protecting both the government and the private sector – namely the critical infrastructure. We were still in the early stages of figuring out how the government was going to interact with the private sector in defending against this threat, so there were all sorts of new and interesting legal issues to consider. When you're talking about inward facing threats to the government, it's a lot easier to share threat intelligence, classified information, with internal government agencies and control the process as needed to protect sensitive systems. But when you look outward to the private sector, what's the government's role in helping protect companies and private infrastructure? This was one of the major issues we were grappling with back then – and to some extent still are.

Andrew Tannenbaum *is chief cybersecurity counsel at IBM, where he guides the company on a wide range of cybersecurity legal, policy and investigative matters. He has legal and operational experience in both the private and public sectors and has overseen hundreds of cyber incident response investigations worldwide. Prior to joining IBM, he held several senior national security positions at the U.S. Department of Justice and the National Security Agency during both the Obama and Bush administrations.*

The laws in this area were somewhat outdated. They had not been written with the cyber threat in mind, and they didn't address the need to share classified information at such scope and speed. Privacy issues were also implicated, issues that we've heard a lot about in recent years with respect to surveillance. But scanning packets of IP traffic and logs for technical signs of malware and other threats is not the same as reading a person's emails to understand what they are up to. The privacy laws needed to be refreshed to account for widely accepted methods of cyber defense, and we began working on that as well.

You did this from 2011 to 2012, and that seems like ages ago, but the same kinds of issues are obviously still with us today. Did you spend a lot of time actually talking to companies about ways you might be able to cooperate and vice versa?

Tannenbaum: We did. There were a number of different government groups trying to coordinate with companies, and some of them were led by the Department of Homeland Security (DHS). As an intelligence agency, the NSA wasn't normally in a position of being out front in the public and speaking with companies. That fell more to DHS and the FBI. But those agencies would loop in the NSA to help them coordinate with the private sector, because there was so much technical expertise and skill at the NSA.

When you took this job and started to sink your teeth into it, did you have a sense early on that this was going to become the focus of your career at least for a substantial stint?

Tannenbaum: Yes. It was such a fascinating issue. And it brought together a lot of different elements I had worked on before in the government, whether it was as a litigator representing the NSA, or advising on surveillance, privacy and technology issues. It was new, the threat wasn't going away, and there was so much work to be done.

In those days, 8, 9, 10 years ago, there was a lot that was known inside the government about the cyber threat that took a little while to gain public awareness. From that vantage point, you could see how important this was going to be for some time. For example, we were very concerned about the cyber threat evolving from the theft of data to the physical destruction or manipulation of systems and infrastructure. Today we are seeing more and more destructive attacks. The recent WannaCry and Petya outbreaks showed how ransomware could be used in a highly destructive manner, shutting down corporate operations, including commerce and the shipment of goods. This is a problem that unfortunately is going to get worse, and we are going to need lots of skilled people to help address it.

What made you decide to move on, and what options were you considering at that point?

Tannenbaum: It was a great job and a hard one to leave, but at that point I had spent a decade in government. I was always oriented toward public service and I loved every minute of it, but I felt it was a good time to transition to the private sector and gain a new set of experiences. And for family reasons we wanted to move back to New York. I was very much interested in finding a role like the

Continued on page 5

Continued from page 4

one I had at the NSA – an in-house legal job in an organization where you could really partner with the technical and security experts and work with them at an operational level to help protect the organization and the country.

That's why IBM was so appealing. Here you have this incredible company with this amazing 100-plus year history in technology with so much technical expertise and research and development, on the cutting edge of so many technologies. It also sees cybersecurity from every vantage point possible as a provider to clients all over the world, many of which are large enterprises in critical infrastructure sectors like banking and health care. Then you throw in new technologies like Watson, cognitive computing and blockchain. Not unlike the government, there is a real sense of mission and belief that you are part of an effort to help protect the world from cyber threats.

This is an issue that government, industry and academia should work on together, including competitors. That's always been our posture.

IBM had never had a chief cybersecurity counsel before. Were they looking for one, or did you convince them that they should be?

Tannenbaum: They hadn't posted or advertised that they were looking for one, but when I came to them and pitched the role, they were immediately receptive. I think they had been thinking along those lines, so the timing worked out very nicely. I give IBM and our general counsel at the time [Robert Weber] a ton of credit in recognizing the importance of this issue early on. They were really on the leading edge of thinking about cybersecurity as its own legal focus, its own in-house practice. That was not common five years ago, and I think IBM was one of the first companies to really build out that kind of practice. Since then we have grown it to include seven lawyers globally who are dedicated to cybersecurity, making it probably one of the largest in-house cybersecurity legal groups in the country.

Do you have any idea how many similar positions are out there, let's say in the Fortune 500? Any guess what percentage of companies have created a position like the one you occupy?

Tannenbaum: I haven't done a formal survey or tally, so I couldn't come up with a number off the top of my head. I do know there is a small but growing community of in-house cyber lawyers, and we tend to either run into each other or talk on occasion. There's definitely a number of them out there. It is more common, though, for corporate in-house lawyers to have cyber as one piece of their portfolio with other aspects too, whether it's privacy, intellectual property or something else.

So what exactly do you do?

Tannenbaum: One of my main roles is advising our chief information security officer (CISO), who is the operational owner of the IBM corporate cybersecurity program. That includes everything from the overall governance model for how to manage cyber risk as a corporation, as well as the company's policies, tools, employee training and incident response process. We also have to keep track of the developing laws and regulations all over the world. Cyber is still a relatively new area of law in its formative stages. There are new developments all the time not only in the U.S. but also Europe and Asia and elsewhere. We look at those evolving requirements, but we also have to think beyond specific statutes and regulations and ask questions like, "How would the Federal Trade Commission (FTC) think of this issue? Under what circumstances do they take enforcement actions against companies for poor security? What do the courts consider to be reasonable security practices? What are international best practices?" And then we have to translate all that into: "What should our company's policies, practices and operations look like?"

If they're going to make a move to enhance their security, do you think that companies that are not as large as yours would likely hire a chief information security officer and not a chief cybersecurity counsel?

Tannenbaum: They are definitely two separate roles. The CISO is responsible for the operational aspects of securing the company. Most companies will want and need a CISO as their first and most important security hire. In fact, recent laws and regulations have actually been requiring companies to have a CISO responsible for a comprehensive security program. We saw this with the new cybersecurity regulation issued by the New York State Department of Financial Services. If you're just starting out and figuring out how to secure your company's assets, the most important thing you should do is to hire a strong CISO and give that CISO the resources, authority and tools to be able to successfully execute that mission.

And your role adds what?

Tannenbaum: It's the other side of the coin, which is managing the legal risk. All of these cyber threats are creating risks to organizations, and the CISO is dealing with that risk from an operational perspective. The general counsel and the legal team look at the same risk and see, obviously, potential lawsuits, potential actions by regulators, costs in terms of what those types of actions will incur – financially but also reputationally, which is a very significant risk for many companies. Lawyers are also good at asking probing questions and thinking several steps down the road, which is a skill set that can help a company prepare for a range of possible outcomes. You're really working as partners, the legal team and the CISO, to manage the same risk, but one brings a set of technical skills and responsibilities and the other brings legal skills and responsibilities. If that partnership works well, it can be a very effective combination for significantly lowering your cyber risk.

How do you use IBM's technology to advance your work?

Tannenbaum: We're very fortunate to have such incredible capabilities in-house at IBM. Most companies, if they have a breach or a suspicious security incident that needs to be investigated, have to get outside help. They have to hire forensic experts. They have to hire outside counsel. We are very fortunate that we have in-house experts that can conduct those types of investigations globally with our forensic analysts, with our incident response managers, with our legal team.

We also have the IBM security business, and we're able to benefit internally from the expertise and tools that they use to help protect IBM clients all over the world. Watson is a great example. That's a technology that is being used in every sector, whether to help find treatments and cures for diseases like cancer or to help make cities safer and more efficient, through crunching tons of data and applying cognitive technology to obtain insights that humans cannot achieve at the same volume and speed.

For instance, about 60,000 cybersecurity blogs are written every month. Plus thousands of other reports and articles and social media posts, all of which, together, could be very useful in helping a security analyst better understand cyber threats. Our security business has trained Watson to read all of those blogs and scour all of that information, which no human could possibly do at that scale. As a result, our security analysts are gaining insights that might not have been apparent before because they were hidden in a sea of data.

Can you imagine a day when you report to Watson?

Tannenbaum: [Laughing] No. One thing we always say is that the idea behind Watson is not to replace people. It's to make people smarter and faster. You

Continued on page 6

Continued from page 5

still need the human expertise, whether it's a doctor, a security expert or a lawyer. They still need to perform those functions. Watson will just make them better at their jobs.

Next time we have a telephone call, maybe we can conference in Watson and see what his side of the story is. How does IBM decide whom to share information about breaches with and when to do it?

Tannenbaum: We've always been a strong proponent of information sharing. Battling this type of threat, with the pace of evolving technology and techniques and the sheer volume of malware that's created every day, you need to have the best data plugged into your systems in real time as fast as possible. We've advocated for laws that will improve the ability, quality and speed of sharing – we were very supportive of the efforts in Congress to pass the Cybersecurity Information Sharing Act (CISA) two years ago. And we've tried to set our own example by both making an enormous amount of threat data that IBM gathers public through our X-Force Exchange (exchange.xforce.ibmcloud.com). We also work with other private sector and government entities to help foster the sharing of information.

What's the X-Force Exchange?

Tannenbaum: It's a portal that our security business runs. We put over 700 terabytes of threat data on it when we first released it a couple of years ago, and we've been updating it on a daily or even hourly basis since then. Other organizations can sign up for the portal, can get access to the data, do research on it, search for different types of malware. It's our way of making that data available to help protect companies.

Talk about issues that make it tricky to decide what to share with the government. You're in an interesting position because you have the government perspective from your days working there, and now you've had a chance to sit on the other side, too.

Tannenbaum: Having both perspectives is helpful because there has been some distrust between the private sector and the government over information sharing and privacy, particularly after the Snowden disclosures. "If I share information, is the government going to come after me? Is it going to demand that we provide more information? Is it in some way a back door for the government to conduct surveillance of our employees or our clients?" But in reality, when you share cyber threat data, you are sharing technical data about a piece of malware, about a technique used by a bad actor, about an IP address that a bad actor is using as part of their command and control.

In those types of cases, the U.S. government is not looking to read your employees' emails or look at your intellectual property. That was part of the discussion around the legislation I just mentioned – especially when efforts to pass that law stalled for a bit after the Snowden disclosures. Before Snowden, CISA was viewed as a necessary update to privacy laws that would allow the sharing of technical threat data. But after Snowden, it became a debate about, "Well, isn't this just the government conducting surveillance another way and getting data to the NSA?" While that was an important issue to address and clarify, CISA was never intended to serve any surveillance function. That just wasn't the case, and we worked to help make sure the law was narrowly written to authorize only the sharing of technical threat data.

There was also the Apple versus the FBI face-off about sharing information that would allow the FBI to unlock an iPhone that was owned by the terrorist who committed those atrocities in California. Where does IBM stand on that issue?

Tannenbaum: That's a difficult issue. Sometimes people say the encryption debate pits security against privacy, but it really pits one security interest against another – the security interest of the government and of law enforcement in preventing crimes or terrorist attacks, on one hand, versus the security interest of strong encryption, which is necessary these days to protect data and protect systems. IBM is sympathetic to both of those interests. We certainly understand the law enforcement perspective, but we are also adamantly against efforts to weaken encryption or to create back doors in technology products or software, which could be used not only by the good guys but also by the bad guys to cause more damage. It's a difficult problem, a 21st century challenge, and we'll need the best minds to figure it out.

> ***IBM hadn't advertised this position, but when they heard the pitch, they were immediately receptive.***

How about deciding when to share and how to share information about breaches with your customers? Is that still as tricky as it seems?

Tannenbaum: For a service provider like IBM, notification is going to be governed either by law or contract. We have agreements with our customers on what they want to be notified about and when. Certainly with any major security issue or breach, you're going to want to notify them right away. But there is a range of other events – thousands of failed attempts by hackers, suspicious activity that may turn out to be nothing serious but requires further investigation and routine activities on our part to clean up systems and malware. And that's a discussion we have with a customer at the outset. But if we're talking an actual confirmed breach or a serious incident, that's something the customer expects to be notified about as quickly as possible.

How about with competitors in your industry? Are there reasons why you would want to share information? Are there also limits or complications that make this a difficult issue to grapple with?

Tannenbaum: My own view is that sharing cyber threat data should never be a competitive issue. You should never be rooting for a competitor to get hacked and taken advantage of by a criminal group. This is an issue that government, industry, and academia should work on together, including competitors. That's always been our posture.

How widely do you think that attitude prevails?

Tannenbaum: Pretty widely. Everybody has their own proprietary technology or data or intellectual property, but I would hope that most companies and organizations feel the same way. Nobody likes being on the end of a major breach, and none of us should ever wish a cyberattack on anyone else.

We've seen plenty of attacks originate from other parts of the world. There are new laws in China. There's a new privacy regime rolling out in Europe. You have a global team, but how does one person with six additional lawyers deal with the multiplicity of threats and issues all over the world?

Tannenbaum: Again, we are lucky at IBM, because we can leverage not only our cyber legal team but also teams of IBM lawyers who provide legal advice to businesses in countries all over the world. With the law in China, for example, we have a Chinese legal team that helps us translate it, understand it, and advise the company on how to deal with it.

There is quite an evolving mixture of laws to follow. Here in the U.S., state laws for some time have focused on breach notification. But that legal focus has been expanding in recent years to require more preventive security risk management. In places like Europe, there's a significant focus on privacy and all of the steps that entities need to take to make sure their consumers and employees have their personal information protected, including when data is sent across borders. You have other places in the world where the focus is on data localization, meaning they want to keep their citizens' data, their corporate data, within their own countries and potentially even give a competitive advantage to technology companies that are domestic. By the way, hackers don't care about lines on maps, so we don't believe that mandating local data storage through public policy actually makes that data any more secure.

And there are other countries where governments want to control the flow of data in a way that will maximize their ability to conduct surveillance (without any of the civil liberty protections enshrined in U.S. law). So you're absolutely right. It's a constantly moving legal landscape that is still somewhat immature. If you're going to do business with data around the world, you've got to have legal advice, whether in-house or from outside counsel, in those countries as the laws develop.

At what point should a general counsel say, "Maybe it's time to hire a cybersecurity counselor"?

Tannenbaum: If your company's business depends on the security or privacy of data – your own intellectual property, sensitive regulated data, the personal data of customers – you need legal guidance about your obligations to protect and secure your systems. In this day and age, many companies will fall into this category. Ideally, you have an in-house cyber lawyer who really understands the business and works every day with the CISO. If you do, it puts you on a more proactive and preventive footing, which is where you want to be. If you don't have a cyber lawyer, you definitely want to engage outside counsel. But do it proactively. Don't wait until something goes wrong.

Three Steps to Improve Cybersecurity Oversight in the Boardroom

Directors need to prepare for attacks

By Robert P. Silvers / Paul Hastings / National Association of Corporate Directors (NACD)

Cybersecurity breaches pose a growing threat to any organization. As we've seen in recent years, and indeed in recent weeks, the most sophisticated companies and even governments aren't immune from cyberattacks. Ransomware has become a global menace, and payment data and customers' personal information are routinely swiped and sold on the dark web in bulk. Next-generation internet-of-things devices are wowing consumers, but they are also targets, as internet connectivity becomes standard-issue in more and more product lines.

How do directors prepare for this landscape? Everyone now acknowledges the importance of cybersecurity, but it is daunting to begin to think about implementing a cybersecurity plan because it's technical, fast moving and has no silver-bullet solutions. Most boards now consult regularly with the organization's information security team, but the discussions can be frustrating because it's hard to gauge readiness and where the organization really stands in comparison to its peers. Sometimes directors confide in me, quietly and on the sidelines, that their real cybersecurity strategy is one of hope and prayer.

There are steps directors can take now to prepare for incidents so that when they occur the company's response is well oiled. With the right resources and preparation, boards can safely navigate these difficult and unforeseen situations. Three key strategies can assist directors as they provide oversight for cybersecurity risks:

- Build relationships with law enforcement officials
- Have incident response plans in place (and practice them)
- Stay educated on cybersecurity trends

An incident response plan is only valuable if it is updated.

1. Build Relationships with Law Enforcement Officials

It's no secret that relationships are central to success. Building the right relationships now, before your worst-case scenario happens, will help you manage the situation. The Federal Bureau of Investigation is generally the lead federal investigative agency when it comes to cybercrime, and the United States Secret Service also plays an important role in the financial services and payment systems sectors.

Boards should ensure company management educates law enforcement officials from these agencies about the company's business and potential risks. In turn, the company should ask law enforcement to keep it apprised of emergent threats in real time. There should also be designated points of contact on each side to allow for ongoing communications and to make it clear whom to contact during an incident. This is critical to ensuring that the company has allies *already in place* in the event that a cyberattack occurs.

2. Have – and Practice – Incident Response Plans

Directors should ask to see copies of the company's written cyber breach response plan. This document is essential. A good incident response plan addresses the many parallel efforts that will need to take place during a cyberattack, including:

- Technical investigation and remediation
- Public relations messaging
- Managing customer concern and fallout
- Managing human resources issues, particularly if employee data has been stolen or if the perpetrator of the attack is a rogue employee
- Coordination with law enforcement; and
- Coordination with regulators and preparedness for the civil litigation that increasingly follows cyberattacks

An incident response plan is only valuable if it is updated, if all the relevant divisions within a company are familiar with it, and if these divisions have "buy in" to the process. If the plan is old or a key division doesn't feel bound by it, the plan isn't going to work. Directors should insist the plan be updated regularly and that the company's divisions exercise the plan through simulated cyber incidents, often called tabletop exercises. Indeed, tabletop exercises for the board itself can be an excellent way to familiarize directors with the company's incident response plan and its cyber posture more generally.

3. Stay Educated on Cybersecurity Trends

As your board is building relationships with law enforcement officials and preparing an incident response plan, directors should also be educating themselves on cyber risk. Cybersecurity becomes more approachable as you invest the time to learn – and it's a fascinating subject that directors enjoy thinking about. Do you know what a breach will look like for your company? What protocols do you have in place in case something happens?

According to the 2016–2017 National Association of Corporate Directors (NACD) Public Company Governance Survey, 89 percent of public company directors said cybersecurity is discussed regularly during board meetings. Since a majority of directors in the room agree that cybersecurity is worth discussing, directors should collectively and individually prioritize learning the ins and outs of cyber risks.

One easy way to stay up to date on the latest is to ask the company's information technology security team for periodic reports of the most significant security events that the company has encountered. This will give directors a feel for the rhythm of threats the company faces day in and day out.

Another option is for directors to take a professional course and get certified. The NACD Cyber-Risk Oversight Program is a great example of a course designed to help directors enhance their cybersecurity literacy and strengthen the board's role in providing oversight for cyber preparedness. Consider these options to keep yourself as educated and informed as possible.

The more you can prepare individually, the better off you will be when you have to provide oversight for a cybersecurity breach at your company.

A version of this column was originally published at blog.NACDonline.org. For more information on NACD's cyber course offerings, please visit NACDonline.org.

Robert P. Silvers *is a respected expert on internet-of-things security and effective corporate planning and response to cybersecurity incidents. Silvers is a partner at Paul Hastings and previously served as the Obama administration's assistant secretary for cyber policy at the U.S. Department of Homeland Security. Silvers will speak at the National Association of Corporate Directors 2017 Global Board Leaders' Summit in October. He can be reached at robertsilvers@paulhastings.com.*

Ready for Ransomware

Companies may not be able to prevent malware attacks, but they can prepare for them

Ransomware is much in the headlines of late, with the widespread and high-profile Petya attack just months ago. ***Gretchen Ruck****, a director at* ***AlixPartners LLP*** *in New York, explains why ransomware isn't as straightforward as it sounds and how the best tactic for defense is to pull cybersecurity discussions into the C-suite light of day. The interview has been edited for style and length.*

Please describe a ransomware attack, the motives behind it, and what it looks like to the victims. How is a ransomware attack different from other breaches?

Gretchen Ruck: At its core, ransomware is a form of malware intended to prevent victims from accessing their data. When most people think of ransomware, they envision a chaotic scenario in which a cybercriminal haphazardly unleashes an attack that harnesses software vulnerabilities, allowing the attacker to encrypt the unsuspecting victim's system and then demand money in exchange for code necessary to unlock it. It's true that ransomware attacks frequently follow this pattern, but the methods of these attacks and motives behind them have become more varied.

While other types of cyberattacks focus on stealing and exposing confidential data or committing theft through deception or collusion, ransomware focuses on hindrance through loss of availability or denial of access to systems or files. The attacker usually achieves this by encrypting the victims' data or taking over their accounts and resetting their passwords.

Most often, these attacks are delivered via a phishing email attachment or a malicious website link that surreptitiously downloads malware aimed to exploit an unpatched security flaw or a software vulnerability. Recently, as demonstrated by the Petya ransomware attack at the end of June, instead of initiating the attacks by email, they may be propagated through seemingly routine third-party software updates that deliver a payload of embedded malware.

Though the name ransomware suggests the motive is money in exchange for returning control of data or resources, attacks have become more nefarious lately and some can be characterized as wiper attacks, which destroy data with no hope of restoring it. The Petya attack was intended to be destructive in nature – the data wasn't released in exchange for the demanded ransom. Instead, the attack provided a way to shut down businesses, perhaps because of radical opinions, to impact market share and competition, or to influence situations for political advantage.

In addition to asking how companies should respond and who should be notified, we should also be asking who will be held accountable.

For the most part, ransomware hasn't typically been a targeted attack focused on high-value data, but that could be evolving. Targeted threats have traditionally been linked to mining for confidential data with the intent to steal it, and to integrity incidents. As the cybercriminals who execute these attacks become savvier, combining the wiper intention with longer-term persistence could signal the beginning of denial and disruption campaigns against U.S. companies.

What can companies do to defend against ransomware attacks, and how have those practices changed over the past few years?

Ruck: Just within the last year or so, ransomware has really taken center stage as a business risk. It's likely going to continue its reign as one of the top cybercrime risks over the next year or so. Cybercrime morphs very quickly. With each new attack, we see modified approaches and new exploits incorporated. The advice I provide concerning ransomware attacks applies more broadly to any malware attack.

To defend against an attack, you need to start with the basics. This includes good security hygiene, such as employing mature security administration, maintenance, operations, monitoring, event management, vulnerability and patch management processes. It also helps to align these processes with recognized industry guidance, such as ISO27000, NIST or SANS20, to ensure a comprehensive set of security controls are in place.

As the next step, companies need to identify and prioritize safeguarding high-value data and business-critical systems. Inventorying and classifying systems based on business criticality and data sensitivity establishes the appropriate levels of security control to incorporate and test against. This should include resiliency, redundancy and recovery requirements for all technology developed in-house and acquired through procurement. Your most valuable data and critical business systems should not only be backed up periodically, but there should also be another site where they are actively mirrored in real-time to allow for failover capability.

Everyone plays a role in defending the company against security threats. Build a user base and customer base that are risk-aware. They should not just be trained on security responsibilities, they should also be engaged in the mission and vigilant in spotting new threats. Think of your security team as playing a role similar to that of a soccer goalie. In this analogy, your security team is not your only line of defense, but rather, they are your last line of defense. If a team expects their goalie to stop every single shot attempt, they're going to have a very worn-out goalie, and they're probably going to have a lot of goals scored against them. There are multiple lines of defense, and everyone has to play an active role. The same reasoning applies to stopping a typical cybercrime attack.

When evaluating security, it's surprising how frequently people treat business as something that's static. Businesses are constantly innovating and, to be effective, security must keep pace. Companies are striving to find ways to better leverage their data: to have more agility in how they engage with customers, to create more digitally augmented products, and to increase the use of automation

Continued on page 12

Gretchen Ruck, *a director at AlixPartners LLP in New York, has 20 years of experience in lead security and risk roles and, as a trusted advisor, in consulting roles at global organizations and government agencies. Ruck helps businesses quickly identify what's really at risk by pinpointing critical, executable improvements focused on protecting high-value data and securing key assets from threats and malicious actors. She can be reached at gruck@alixpartners.com.*

This Is No Time to Stand Pat

As cyber threats morph, companies need to reassess their readiness, including their insurance protection

By Joshua Gold / Anderson Kill

In the present environment, cyber risk management simply cannot stay static. Cyber risks continue to morph and vex organizations worldwide. Recent incidents represent a cross-section of nightmare scenarios for businesses, governments and others. They included a large insurance company's $115 million patient breach settlement; an SEC breach investigation preceding a reported $350 million (downward) price adjustment for a corporate acquisition; an $81 million cybertheft from what was thought to be perhaps the safest banking network on the planet; the sudden shutdown of UK hospital networks; law firms losing control of privileged client files; theft of yet unreleased films and original cable programming; and the destruction of industrial facilities in Europe and Asia.

While no one is immune from cyber threats, investors, customers and regulators expect organizations to take steps to reduce risks and stem the harm if a hacker gets through.

Cyber Risk Management Has Never Been More Important

To have even a fighting chance against the threat of security incidents, every organization must put in place a proactive and comprehensive cyber risk-management plan. Below are several steps organizations can take to improve their cybersecurity resilience. While certainly not an exhaustive list, these four actions can prevent many security breaches and minimize the impact when these types of intrustions hit your organization.

1. Map and safeguard data: It is difficult to draw up a game plan to protect data if you don't know what you have and where it is. Mapping may yield some surprises – revealing, for example, that divisions or individual employees use their own cloud computing, whether company policy permits such hosting or not. Thus, organizations need to map all data for which they are responsible. Additionally, because so many organizations use some form of cloud computing these days, data not on your own servers needs to be accounted for, since you can anticipate that a regulator will deem you responsible for it no matter whose server it resides on. There have now been several high-profile hacks where the criminal attacked the organization through information residing on another entity's computer systems.

2. Update and patch: Malware attacks carried out by WannaCry, GoldenEye and NotPetya are believed to have exploited those computer systems that had not updated their system security to apply software manufacturer patches. Basic hygiene is required when it comes to making sure that programs are updated regularly – especially where those updates are motivated by security concerns. Many hackers target the low-hanging fruit.

3. Keep senior management involved: Gone are the days when senior management could relegate cybersecurity oversight to the head of IT. A sufficient dedication of money, human resources and direct senior manager involvement is required – especially if the organization is a public company. The Securities and Exchange Commission has made it clear that it will investigate the disclosure and handling of cybersecurity incidents, and it has already flexed its regulatory muscle, fining a broker-dealer who was alleged to have failed to adequately protect customer data. Many companies have prudently created the senior officer position of chief information security officer (CISO) and provided that position with access to the highest management levels of the organization.

4. Disclose risks and incidents: Smart risk management requires accurate disclosure of the risks faced and the cybersecurity efforts of the organization. The SEC has provided guidance to public companies on the types of computer system assessments that should be taken into consideration. The FTC has vigorously pursued companies that it says failed to accurately describe their cybersecurity wherewithal. If a breach takes place, prompt disclosure, barring law enforcement instructions to the contrary, is the prudent course. Some regulators and law enforcement officials (both state and federal) expressly say that it is an automatic red flag if policyholders do not disclose a cyberbreach within 30 days of its occurrence.

Insurance as a Key Risk-Management Tool

If a policyholder suffers a cyber-related loss, it may certainly have coverage under a specialty cyber insurance policy. Often, however, the analysis does not stop there. A policyholder may also find insurance coverage for a cyber claim under directors and officers (D&O) insurance, errors and omissions (E&O) insurance, property insurance, crime insurance and commercial general liability (CGL) insurance. If a cyber incident takes place, policyholders should promptly notify all potentially applicable insurance policies.

Don't Be Misled by Titles

The purchase of specialty cyber insurance products is on the rise, and the insurance products geared specifically toward these perils have evolved considerably. Despite this, figuring out what kind of insurance is needed to respond effectively to cyber

Continued on page 11

Joshua Gold *is a shareholder at Anderson Kill in New York and is chair of the firm's cyber insurance recovery group. He regularly represents policyholders in insurance coverage matters and disputes concerning electronic data, arbitration, time element insurance and other property/casualty insurance coverage issues. He can be reached at jgold@andersonkill.com.*

Start Assessing Your Company's Risk

GCs collaborate with IT to develop a cybersecurity risk framework

__Nick Barone__, co-practice leader of __EisnerAmper__'s Consulting Group, has over 20 years of industry experience leading computer investigations and cybersecurity incidence response – breach of data and breach response. He has led teams to respond to data breaches as well as to provide proactive security services to prevent them. He formerly served in law enforcement and has worked in 44 U.S. states and 17 foreign countries over the course of his career. Barone shares his insights about how to prepare and respond to cyber risks. His remarks have been edited for length and style.

Lawyers can play a bigger role advising on the technology issues as they pertain to compliance risk and liability.

Let's talk about your approach to working with companies to help them prepare for cyber risk and response.

Nick Barone: The general approach to cybersecurity is based two ways: an industry approach and a company IT risk-specific approach. First is a cybersecurity risk framework – there are several out there depending upon the type of industry you're in. Second, and separate from the framework, is the current state of the client's cybersecurity program. When we're sitting down and talking to companies about how to protect their data, we ask them, "What is your current IT security like, and what does your current IT risk program look like? Have you performed a risk analysis?" If yes, we go through the framework they've utilized, or if they haven't already started a cybersecurity program, we propose a framework.

What's the role of the general counsel and legal department in terms of this preparedness and response planning?

Barone: From my experience, the first legal role is as an adviser on compliance and legal risk issues. In other words, in-house counsel provides advice to the company to help it be compliant with various cybersecurity regulations. Second, in the area of cyber legal risk prevention, inside counsel reviews contract language to ensure that all third parties and even fourth parties who have sensitive data are in compliance with the terms and agreements of the contract. Third, Legal's role is to guide the company in two critical areas of maintaining sensitive information: information classification and information retention (or document retention). And finally, I see inside counsel's role as providing guidance in the event of an incident to determine how the company needs to respond – and that may include the engagement of outside counsel and regulatory response.

You spent much of your career helping companies meet regulatory requirements by creating industry-specific solutions to prevent and identify fraud. Or, should I say identify, not prevent?

Barone: Actually, it's prevention – through the various published federal and state compliance regulations like the Health Insurance Portability and Accountability Act (HIPAA) or other types of regulations. But let me take a step back here. There are several regulations that in-house counsel or outside counsel guide companies on. These can either be federal or state regulations. It's the role of counsel to work with IT to make sure that the company protects itself and complies with these various regulations, and also to help the company understand what process or what data is out there that they need to comply with. For example, the storing of sensitive information.

Depending on the industry, there are multiple classes of information out there. For example, medical records fall under HIPAA. Credit card data falls under the Payment Card Industry Data Security Standard, etc. And personal information is just a broad requirement. That could include the names, addresses and Social Security numbers of employees or vendors. Other areas include, for example, education – college IDs, user names and passwords and so on in the education industry.

In your experience, in terms of cybersecurity, what's the most fruitful way for companies to spend their time? Are there certain things they shouldn't focus on? Certain things they should? There's a big shift toward bring your own device (BYOD) right now, for instance.

Barone: Let's start with what the cybersecurity industry calls the Core Four, the main issues that lead to a data breach, a violation or noncompliance. They are (1) testing your network, (2) training your employees, (3) patching your network, and (4) policy and procedures.

Every security issue that comes up, like BYOD, can be traced back to one of these four leading causes of a data breach. Failure by the company to train their employees. Failure by the company to test their network. Failure by the company to patch or put in place security provisions on their network. And then finally, failure by the company to follow policies and procedures.

In terms of BYOD, there are really two forms, and sometimes people don't realize that. One of them is pretty obvious – to be able to be in contact with the company and its operations and clients via email. The second is the storage of company data outside of the network. Those are the two root causes of challenges with BYOD.

Once you introduce a BYOD system and you have a policy in place, companies then face challenges enforcing those polices on BYOD devices. The two biggest ones are control over the storage of company information on these BYOD devices, and that the use of BYOD devices, unfortunately, introduces potential malware into the environment and presents a risk that the companies cannot properly manage. Say, for example, you bring your own laptop to the office, or you work remotely so the company allows you to purchase your own laptop or to remote in with another computer via your laptop, your personal device. What happens is that the company can no longer manage its control and security.

Now, the lawyers, risk officers and our IT departments create a policy. The policies and procedures provide guidance for the proper usage of that device and

Continued on page 11

Nick Barone *is a director and co-leads the Consulting Services Group at Eisner-Amper LLP with more than 20 years of computer and network forensics experience. He served as the Director of Forensic Investigations and Audit for a multinational financial services corporation and is a co-U.S. patent holder in the field of threat risk data analytics and modeling. He can be reached at Nicholas.Barone@eisneramper.com.*

Assessing Risk

Continued from opposite page

what you can and cannot do. However, there's no enforcement of that policy because there's a lack of certain technology to enforce it. So you're left with the voluntary actions of the employee. Now, let's go back to the security of the device itself. Companies sometimes lack the ability to control the device and, therefore, if the device is lost or stolen, the level of security is not as high as it would be for a company-owned device.

You also lead operational fraud risk assessments as well as initiatives to identify new IT threat scenarios across industries like financial services, tech, healthcare and education. Can you talk about some of the new IT threats you're seeing that our readers may not be aware of?

Barone: The first issue is that BYOD is contributing to more reported data breaches. That's an emerging trend, because these devices are not, like I said, adequately secure or controlled.

The second area is phishing. Even if a company does its best to patch security holes and educate and train its employees, people still get tricked into giving up their secure user names and passwords in email scams or malware that they accidentally click on. Companies can only do so much to prevent that email from coming into the environment.

The third area, unfortunately, is personal use of company devices. The increasing use of corporate assets for personal use is resulting in people introducing malware into the system as a result of surfing on their computer during off times. Most companies have a very vague policy toward personal use of a company computer. It's too draconian to tell somebody they can't surf the web on their lunch hour. And Americans do spend a large amount of their personal lives on company computers because that's where they spend the majority of their computer time – at work.

What advice can you offer in-house lawyers?

Barone: I think an area that's coming up more and more for lawyers is understanding liability and risk – internally, it's important that in-house counsel can effectively communicate liability and risk to the company. Often the in-house counsel, or even outside counsel, don't really get an opportunity to weigh in much on the IT network infrastructure. That's the domain of IT. So additions and subtractions that occur in the IT world usually don't involve input from counsel. I believe that in-house counsel should be more involved, or at least participate in meetings where the information technology structure is being discussed. I'm working with a client right now where that is the case – they're starting to consult and include their in-house counsel more to understand their legal and compliance obligations.

That's really the bigger role that counsel should play: advisement on legal risk involving IT-related issues or processes. From my conversations with in-house counsel, probably one of their biggest challenges is sitting at the table with IT, because they really aren't technically savvy – though that is changing. But a lot of them have limited knowledge of their in-house technology – so they're relying on whatever representations the IT department is making. But that's where lawyers can play a bigger role – advising on the technology issues as they pertain to compliance risk and liability.

No Time to Stand Pat

Continued from page 9

claims is challenging. Just because an insurance policy contains the word "cyber" in the policy description does not mean that the insurance company will be willing to pay a related claim. For example, a recent decision from a federal court in Utah ruled that a CyberFirst liability insurance policy did not cover a claim involving alleged wrongful acts in the handling of data. (*Travelers Property & Cas. Co. v. Fed. Recovery Serv., Inc.*)

Recent history teaches us that court decisions can be all over the place on similar issues. This year, two policyholders seeking "computer fraud" coverage under their crime policies fared quite differently. In *American Tooling Center Inc. v. Travelers Casualty and Surety Co. of America*, a federal trial court in Michigan held that there was no coverage for wire transfers made when the policyholder was duped by fake emails into wiring money to a bogus bank account. The trial court held that there "was no infiltration or 'hacking' of [the] computer system," and that the "emails themselves did not directly cause the transfer of funds; rather, [the policyholder] authorized the transfer based upon the information received in the emails." Conversely, a federal trial court in New York found computer fraud coverage, among other things, for wire transfers that the policyholder was induced to make through fraudulent emails and follow-up phone calls. (*Medidata Solutions v. Federal Ins. Co.*)

Court rulings have also differed on the extent of insurance protection for cyber class-action privacy claims under general liability insurance. In coverage litigation, a New York trial court held the policyholder had no CGL insurance coverage for privacy litigation stemming from a hack of customer information located on the servers of a multi-tenant cloud platform. (*Zurich American Ins. Co., et al v. Sony Corp. of America*) The case was settled before a New York appellate court ruled on the policyholder's appeal.

Last year, however, the United States Court of Appeals for the Fourth Circuit held that a CGL policy covered privacy litigation defense costs for patient medical information that was left on a
publicly accessible searchable server. (*Travelers Indemnity Co. of America v. Portal Healthcare Solutions LLC*)

Here are a few additional issues you may wish to work out with your underwriters at the time you purchase a policy rather than after you file a claim.

Exclusions for terrorism, hostilities and warfare: New revelations have emerged that many attacks come from state-sponsored hacking gangs. Some U.S. lawmakers have described such activities as cyberwarfare. In light of this, policyholders should work with their brokers to get clarification regarding the scope of terrorism and war risk exclusions. For example, many cyber insurance policies contain exclusions for terrorism, "hostilities (whether war is declared or not)" and claims arising from "acts of foreign enemies." Experienced brokers can work to get the most favorable language for policyholders in this area.

Be careful with your board's D&O insurance: It is important to make sure that D&O insurance coverage (including primary, excess, Side A, etc.) remains free of cyber-related exclusions or sublimits. Management will be highly concerned with any argued "gap" in coverage, should a cyber event ensue – especially with the advent of cyber derivative shareholder litigation. Home Depot recently settled derivative litigation aimed at its senior management, and the SEC has repeatedly made clear that it will enforce cybersecurity compliance matters against the entities under its purview.

Cover time-element losses: Business income coverage and reputational damage coverage take on added importance in the wake of recent hacking events designed to harm, destroy and kill. Cybercriminals now have the means to reach industrial controls, attack transportation and other infrastructure, and cause explosions by remote control. As such, business interruption takes on greater importance for policyholders that are industrial or critical infrastructure targets.

Avoid reasonableness representations and clauses: Policyholders should work with their brokers to avoid exclusions, warranties, representations or "conditions" in insurance policies concerning the soundness or reasonableness of the policyholder's data security efforts/protocol. These clauses are a recipe for disputes on potentially every security incident.

Cyber coverage litigation has already emerged involving a cyber insurance company's allegations that the policyholder failed to employ computer security measures it had represented would be in place. (*Columbia Casualty Co. v. Cottage Health System*) Given the pace of technological innovation, almost every computer security step can be second-guessed. Many insurance companies will now forgo these clauses – if requested.

Cover cloud and third-party vendors: Make sure that your specific cyber coverage protects against losses where others manage, transmit or host data for your company. Insurance coverage is available for cloud computing and instances where data is handled, managed or outsourced to a third party**.** Most cyber policies can be modified to extend needed protection to data residing on servers not owned by the policyholder – if requested.

The Bottom Line

There is no single step that will guard against cyber risks. The protection against these risks and the risk transfer to address potential losses are properly viewed as a process. While no one is immune from cyber threats (and no one expects anyone to be impregnable to such risks), investors, customers, regulators and other stakeholders will expect that organizations take the risks seriously and dedicate sufficient resources to reducing the threat of an intrusion, and that they have a plan in place to stem the harm if a hacker gets through.

Continued from page 8

and insight-driven decision-making within their companies. As they do this, they change their attack surface and impact their risk portfolio.

How should companies respond to a ransomware attack? Who needs to be notified in terms of law enforcement, employees, investors or the public in general?

Ruck: In response to an attack, timely reporting to stakeholders and to the user community is vital to avoid any lasting damage. Whether responding to a ransomware attack or any other security incident, successful responses follow scenario-driven playbooks that should be planned for and tested in advance. These plans should elicit involvement and partnerships between security, IT, general counsel, the business and, when necessary, law enforcement.

The plans should put processes into place to enable consistent decision-making regarding when to notify external stakeholders such as investors, customers and the public. As part of these plans, a pivotal and obvious question that organizations must be prepared to answer is how to handle incidents involving ransomware extortion demands. This should be discussed with leadership in advance of such an event occurring.

In addition to asking how companies should respond and who should be notified, we should also be asking who will be held accountable. Years ago, it may have been someone in IT; but, as cybercrime visibility and damages have increased, accountability has shifted upward. Around 10 years ago, we started seeing security regulations incorporate risk management into governance responsibilities in recognition of the need to align security to business operations.

Now, we're beginning to experience another shift. Top executives and boards must demonstrate their understanding of the organization's cybercrime risks when asserting business goals and in fulfilling their leadership and oversight responsibilities. If your organization hasn't shifted crucial security decision-making from the backroom to the boardroom, this should become an immediate priority. Due to the potential impact that a poorly handled security event could have on a business, boards need to be aware of the key security risks faced by the organizations they advise.

How can companies deal with reputation management if they find themselves the victims of a ransomware attack?

Ruck: Whether it's a ransomware attack or a breach of confidential data, follow your defined procedures and respond in a timely and transparent fashion. The organization needs to communicate a clear and consistent message. Within the incident response plan, include a communications strategy that engages your general counsel and PR team in incident remediation.

Be prepared to show that your organization has taken reasonable precautions and has a comprehensive set of security controls in place. These controls, which should map to identified risks, are expected to be verified periodically, to confirm that they consistently function as designed. Where you've identified security weaknesses, vulnerabilities and noncompliance areas, prioritize them based on urgency and begin making progress toward an improvement plan.

There is talk about companies sharing information about attacks to crowdsource their knowledge on how to prevent future incidents. For example, law firms by and large use the same systems. They buy software from the same companies. At the same time, there is concern about competition. Should they be collaborating about their experiences if they've been breached, are concerned about breaches or have identified attempts at breaches, to prevent future incidents?

Ruck: A very affirmative yes. There are a number of industry roundtables where chief information security officers get together and talk about common threats that they're facing and what they're seeing in terms of attacks. People who participate are responsible for keeping the discussions confidential and understanding what they can and can't share. Asking for general feedback on whether organizations are adopting new security techniques, such as if they are doing more around application isolation or webcasting – there's a lot of success in that, and in no way does it make a company more vulnerable. When used correctly, these forums can be very useful tools, especially in industries that traditionally have not invested as much in security, such as professional service firms, including law firms.

METROPOLITAN
CORPORATE
COUNSEL®

Kristin Calve, *Publisher*
David Hechler, *Editor-in-Chief*
Meg Smith, *Director of IT & Operations*
Tina Salvioli, *Assistant to the Publisher*
Amy Lemel, *Director of Business Development*
Lainie Geary, *Client Relationship Director*
Christina Swaak, *Client Relationship Director*
Mickey Kozak, *Sales Associate*
ProCirc B2B, *Circulation Management*
Lester Goodman, *Creative Direction & Design*