the cyberwire

The CyberWire
621 East Pratt Street, suite 300
Baltimore MD 21202–3140
editor@thecyberwire.com
www.thecyberwire.com
@thecyberwire

Georgetown's Cybersecurity Law Institute 2015

May 20-21, 2015 Washington, DC

The Georgetown Cybersecurity Law Institute met on the 20th and 21st of May to offer lawyers continuing education in the rapidly evolving field of cyber security law. Among the themes that the conference addressed were centrality of risk management to protecting the enterprise, the coming importance (and current immaturity) of insurance markets and their legal environment, the ways in which new technology (particularly that surrounding the Internet-of-things and strong artificial intelligence) will disrupt a surprising range of human institutions and modes of organization, the relationship between corporations and law enforcement (where trust and benefit need to be enhanced), the impermissibility (and inadvisability) of "hacking back," and the new but increasingly important expectation that lawyers be technically literate.

Georgetown Cybersecurity Law Institute: Day One

A Primer: Ten Things You Need to Know about Cyber Security Law

Panelists included Stephanie Cason (Cooley LLP), Harriet Pearson (Hogan Lovells US LLP), and Andrew Tannenbaum (Cybersecurity Counsel, IBM Corporation). Their expertise includes healthcare, privacy, data breaches, and national security. They offered the attorneys in attendance a primer on their role in cyber security, organized into ten areas of responsibility:

1. Counseling the company: cyber risk governance and the duty of care.
2. Counseling the company: cyber risk management.
3. Counseling the CISO.
4. Counseling the CIO and Procurement.
5. Workforce issues.
6. Partnering with privacy.
7. Preparing for an incident.
8. Guiding information sharing and government / law enforcement interactions.
9. Cyber insurance considerations.
10. Handling an incident.

They noted that cyber security law is "complex, multi-disciplinary, and dynamic," not a single unified field. This makes risk management all the more important. Lawyers must be concerned with the applicable standards of care. Compliance is a place to start, but of course compliance is insufficient; look to the relevant sources of law, and don't overlook emerging law.

Counsel plays an important role in risk management and incident preparation and response. Counsel should "know what's radioactive," and such proactive risk management is an important aspect of standard of care. While many key issues have yet to be litigated, one would do well to start with close attention to the NIST Framework, and to state laws where you do business (often diverse, and often more developed than federal law).

Corporate counsel should work closely with CISOs (and note that it's impractical to keep communications with CISOs under lawyer-client privilege). They should document their communications, and ensure that they follow up on what's documented.

Work on a daily operational level, but don't neglect strategy. Take note of the relationship between the CIO and the CISO. Be alert to information accessed by vendors and contractors (and of what information your client has when that client is itself a vendor or contractor).

Vendor oversight is notoriously difficult to achieve, but it's a lawyer's role to assess third-party risk. Third parties may themselves need to be audited, and required to cooperate in incident investigations.

Workforce issues often come down to managing human error and controlling social engineering. Push to train your workforce: they should see themselves as guardians of your company's reputation.

Think about how your company handles employees who violate security policy, and note that many (perhaps most) violations are well-intentioned. Well-intentioned actions can result in real risk and real loss to your company, so setting the right tone and dealing with policy violations assumes considerable importance. This, of course, requires counsel to interact closely with human resources (always a field for the exercise of attorney-client privilege).

Privacy issues arise in cyber security in very specific, concrete ways. It can, for example, affect security tactics. Companies commonly increase monitoring to deal with insider threats (for example, ongoing background checks are becoming common). Such monitoring is becoming increasingly technical and increasingly intrusive, thereby raising obvious privacy issues. Consider what kind of notice of monitoring and what kind of consent may be required in the various jurisdictions where you operate. BYOD, for example, has driven increasingly aggressive monitoring policies, but such policies are problematic in many jurisdictions. Here again, the NIST Framework is useful — consult its privacy sections.

Preparing for an incident is increasingly important to counsel. Have the incident playbook ready and rehearsed. Fix incident response roles in advance.

With respect to counsel's role in guiding both information sharing and interactions with government and law enforcement, note that there's potential benefit to these interactions. It's not unusual that government investigators are the ones who discover an incident. But there are obvious potential downsides as well: loss of control, disclosure of sensitive information, public exposure, and so on. If hiring outside forensic help, consider doing so through outside counsel, under privilege.

Counsel is also involved in cyber insurance: what coverage to purchase, its terms and conditions, the risk transferred, etc. But the market for cyber insurance is very immature. Litigation risk with respect to pay card breaches is now well understood, but that's an exception: in most areas the necessary experience simply isn't there. The panel made an obvious but strongly emphasized point: the fine print really matters in insurance coverage. And cyber insurance is no substitute for sound risk mitigation policies and practices.

In incident response, the first step is to "stop the bleeding." Mobilize key responders early. Be sure to train your people in what attorney-client privilege means. Use the same best practices all the time, and stick to facts in your communications.

What's Hot: The Latest Cyber Trends

This panel was moderated by Luke Dembosky (Deputy Assistant Attorney General, U.S. Department of Justice), with panelists Michael A. Aisenberg (Principal, Cyber Policy Counsel, The MITRE Corporation), Judith H. Germano (Senior Fellow, Center on Law & Security, Adjunct

Professor, NYU School of Law, and GermanoLawLLC), and Timothy P. Ryan (Cybersecurity and Investigations Practice, Kroll Associates, Inc.).

The discussion opened with a familiar restatement of the importance of prior planning for cyber incident response. That response will often involve engaging the government, particularly law enforcement agencies. Despite years of talking public-private collaboration, the private sector remains leery, unsure of the benefits such collaboration might in fact bring. Norms are clearly needed, but the continuously evolving threat makes development of norms problematic.

Law enforcement agencies and the Intelligence Community could help the private sector by becoming more sensitive to their obligations. The government needs to establish benefit and trust, and much work remains be done here. Panelists hoped pending information sharing legislation would help. They also noted that the government has an issue with over-classification that should be addressed to foster information sharing.

One emerging trend seen in the Department of Defense (and therefore in the Defense Industrial Base) is an increased interest in controlling sensitive but unclassified data. The modes of protecting such data remain unsettled and controversial, but the trend bears close watching.

The private sector, panelists suggested, would do well to learn from government practices in training and exercises.

In summary, the panel offered this general model: Expect the government to handle the stuff outside your network. Thus, you should take care of your house, and let the government deal with what's going on outside.

One corporate counsel in the audience had the last word, urging the government to spend some time with private industries so it may gain a realistic understanding of what that sector is dealing with.

Interview with the Director: Cybersecurity Challenges in the 21st Century

Benjamin Powell (WilmerHale) interviewed the Hon. James B. Comey (Director, Federal Bureau of Investigation).

Director Comey began by noting that the FBI now organizes its response to cyber crime according to the nature of the threat. That response is talent-based, not geography-based. In general, the Bureau's goal is to "impose costs on the [bad] actors sitting at the keyboards."

Asked about the biggest threats, the director named ISIL, especially with respect to the recruitment and incitement it conducts in social media. He sees the cyber threat in general as layered: state actors, terrorists, organized crime, "and then all the other creeps at keyboards." In the face of that layered threat, digital literacy has become vital to all law enforcement.

With respect to information sharing, Comey said the Bureau always tries to treat information gathered from the private sector as evidence in a potential criminal case. There's incremental risk in sharing information with the government, but the benefits to an enterprise, he thinks, outweigh those risks. And he thinks the Bureau itself has gotten better at sharing information since the 2012 DDoS attack wave. We need, he argued, to get better at this, to operate at machine speed. In passing, he noted one obstacle to smoother information sharing: general counsels, who "are mostly obstructionist weenies" because they're (rightly) always concerned about litigation. He recommended DSAC and InfraGard as good vehicles for cooperation. "The FBI's got offices all over; get to know them." He noted that the Bureau is piloting "Malware Investigator," trying to make this tool available to the private sector through InfraGard. He outlined collaboration among FBI, DHS, USSS, and the NSA, and he stressed the value of face-to-face collaboration among both agencies and the private sector.

Director Comey does see, post-Snowden, cultural barriers to information sharing, although he noted some abatement in fear of sharing information with the government. He praised encryption as a good practice, but offered animadversions about how encryption could impede public safety. He sees a general failure to recognize the costs of universal strong encryption. It has benefits, sure, but it also imposes costs. He predicted a big impact on national security and law enforcement if the government loses Section 215 metadata collection tools, set to expire this June. Critical tools, he argued, will sunset with Section 215. Roving wiretap authority will lapse. Access to FISA will lapse. "Lone wolf" provisions will lapse.

The FBI is concerned about proliferation of destructive malware. Director Comey doesn't see it yet, but thinks it's coming.

International partners want more information, equipment, and training. "There are nations not interested in cooperating to stop cyber crime, but they're in the minority," he said. "There's a willingness to make common cause against crime." (They even have productive conversations with China).

He returned to his theme of the importance of imposing costs through shaming, sanctions, and prosecution. He strongly cautioned, however, against private actors seeking to impose costs by "hacking back." It's not illegal, but it's likely to have unpredictable, unintended, and undesirable consequences.

Asked if FBI is still pursuing Snowden, he answered, simply, "Yes." Mr. Snowden, Director Comey said, should be given the opportunity to face charges against him "in the fairest legal system in the world."

He concluded on a hopeful note. He thinks the private sector is getting its act together with respect to cyber security, and he thinks the government is getting better at imposing costs

An Address by Assistant Attorney General Caldwell: a View from the DoJ

The Hon. Leslie R. Caldwell, Assistant Attorney General, Criminal Division, U.S. Department of Justice, presented an overview of cyber crime as seen by the Justice Department's Criminal Division.

She emphasized, as did so many other participants in the institute, the importance of international cooperation, and of government cooperation with the private sector. The criminal division is focused on major cyber crime and the criminal infrastructure that enables it. We see, she noted, overlapping casts of criminal characters when we investigate cyber crime. She described successes indicting and extraditing foreign cyber criminals; she praised the cooperation involved in the GameOverZeus botnet and Cryptolocker ransomware takedowns.

After commending the Department of Justice's guidance to the private sector on reporting and reacting to the cyber attacks, she addressed "hacking back." As had FBI Director Comey, she strongly advised against it. The Department of Justice position is that hacking back is illegal. Even if hacking back were legal, she argued, it would inevitably risk damage to innocent third parties and pose the prospect of uncontrolled escalation. Hacking back also interferes with investigation, and, more seriously as cyberspace becomes a field of international conflict, risks misinterpretation as a state action.

Implications of Disruptive Technologies

Of the two afternoon panels, we attended the futurist one on how we should expect to see "disruptive" technologies affect the way we organize our lives. David J. McCue (President, McCue Inc.) moderated this panel, which included Robert Ames (Senior Vice President, Advanced Analytics, In-Q-Tel), Dr. David A. Bray (Chief Information Officer, Federal Communications Commission), and Michele Weslander-Quaid (Global Cloud Ecosystem Community Lead, Google).

After clarifying that Clayton Christensen's work is their point of departure in understanding what qualifies as a "disruptive technology" (essentially an innovation, usually a lower-cost if in some respects sub-optimal technology, that creates a new market and value network, disrupting and displacing older markets and value networks), panelists noted that the mobile explosion and the Internet-of-things were proving disruptive.

While disruptive tools are usually recognized as such only retrospectively, they can change the ways in which we as human beings organize our lives. The ways we do information technology, and the ways we do cyber security, simply won't scale with the Internet-of-things. More broadly, democracy itself may have difficulty scaling into the world technology is creating. Consider checks and balances. How will they function? And how will political compromise remain possible in a hyperconnected world?

The amount of personal data now consigned to platforms is proving disruptive. Natural language processing is becoming disruptive: machines are probably going to replace human labor in providing financial analysis and (most) legal advice.

A questioner noted that technology, not law, seems to be driving thinking about privacy. Our public choices are being shaped by companies like Google, and not by legislation.

Cyber Security Risk Management in Vendor and Supply Chains

C.M. Tokë Vandervoort (Vice President and Assistant General Counsel, Technology, Privacy and Security and Chief Privacy Officer, XO Communications, LLC) moderated a panel composed of Peter Adler (Vice President, Deputy General Counsel, and Chief Privacy Officer, SRA International, Inc.), Robert S. Metzger (Rogers Joseph O'Donnell, PC), and Emile Monette (Senior Advisor for Cybersecurity and Resiliency, U.S. General Services Administration).

Moderator Vandervoort began by saying the panel would discuss the issue at a very high level, in terms of policy standards and market expectations, and in terms of risk management considerations.

Robert Metztger offered lessons from the Department of Defense's supply chain management, especially with respect to the measures it takes to protect unclassified technical information. The department works to protect against exfiltration of unclassified information whose loss could affect national security. But across the government, the National Archives and Records Administration (NARA) has been given a leading responsibility for regulating controlled unclassified information (in all of its twenty-three category, eighty-two subcategory complexity). He outlined the (dismayingly) adverse consequences of failure to control controlled unclassified information.

The panel discussed the big unresolved question of whose responsibility it is for seeing that second- and third-tier suppliers comply with their cyber security promises. They concluded by noting that the NIST Framework has given us a common cyber lexicon, and has joined other participants in the Institute by commending it to those in attendance. (But, noted Metzger, the NIST Framework is voluntary. Other coming standards will be compulsory for the Federal supply chain.)

Moving to the Cloud? Ethical and Security Issues to Consider

Maureen T. Kelly (Assistant General Counsel, Corporate Director, Enterprise Shared Services, Northrop Grumman Corporation) moderated the panel. Panelists included the Hon. John M. Facciola (Retired Magistrate Judge, U.S. District Court for the District of Columbia), Dori Anne Kuchinsky (Assistant General Counsel, Litigation and Global Privacy, W.R. Grace & Co.), and Nickolas B. Savage (Supervisory Special Agent, Federal Bureau of Investigation).

The first big point the panel wanted to get across is that US lawyers are now required to know something about the dangers of technology. The American Bar Association now has clear standards, not what Judge Facciola described as the former "mere mushy reasonableness." Yet lawyers don't seem to have made much progress in technical literacy. Panelists noted with satisfied gloom the dismal results of a survey of lawyers on their use and understanding of the cloud: there's much use, but little understanding.

Security boils down to assessing and managing risk, and to do that you need to know the value of what you have. The panel advised grilling cloud providers on their security. Would you, one asked, let someone transport your child in their car without making sure they were safe drivers, had a proper child seat, were sober, and so on? Do likewise before entrusting your data to the cloud. Know what your vendors owe you in the event they're breached.

Facciola summed up by telling lawyers that they've got to understand the underlying technology. Savage told them that they're not, and can't be, in this alone, and Kuchinsky summed up by telling them that they've got to own the issue of data security.

Georgetown CSLI Day 2

Insider Threats and Monitoring: Privacy, Civil Liberties and Wiretap Issues

Mary Ellen Callahan (Jenner & Block LLP) moderated the panel. Panelists included H. Bryan Cunningham (Cunningham Levy LLP), Prof. Laura K. Donohue (Director, Center on National Security and the Law; Director, Center on Privacy and Technology, Georgetown University Law Center), and Steven Kelly (Director of Cybersecurity Policy, National Security Council, The White House).

The discussion opened by observing that, while continuous monitoring is a popular approach to handling the insider threat, it has privacy, civil liberty, and employment law implications. Espionage, as panelist Kelly said, is the second oldest profession, and so the insider threat isn't new. But Wikileaks brought the insider threat to the fore, prompting the current wave of concern. The insider threat isn't a classified world problem, or even a government-only problem. The private sector faces a serious insider threat to intellectual property, for example. Kelly recommended focusing on small teams within organizations tasked with figuring out whether you've got a rogue insider.

Professor Donohue took up the right-to-privacy implications of continuous monitoring. Privacy rights, she noted, are rooted in English law's protections against government intrusion into the private sphere. What that law didn't anticipate, legally or philosophically, was the emergence of the corporation and its relation to the private sphere. There are significant costs at stake. Continuous monitoring assumes the individual's guilt, collecting without needing prior suspicion of wrongdoing. There are spheres of life that are private, and intruding into them opens up harms. And, she asked, what of structure? Tremendous power can derive from continuous monitoring. To whom does an enterprise entrust it? Thus, she concluded, the issues are rights, harms, and structure.

Panelist Cunningham summarized the Wiretap Act and other relevant current law, noting that pending legislation may give more leeway to monitoring. Federal law prevents (with a few exceptions) anyone (not, he emphasized, just the government) from monitoring communications without appropriate consent. Similar restrictions apply to stored communications. But there are extra legal issues here, too. The kind of corporate culture you want will appropriately affect the kind of monitoring you do. Your monitoring must also resolve another problem: differences in law and regulation across various jurisdictions. Your employees may be communicating with people in the dozen or so states that have all-party consent laws. Your employees will also be communicating with people in other countries, where it's difficult to obtain consent.

Moderator Callahan asked the panel about third-party doctrine. Professor Donohue's answer was that third-party doctrine is going the way of the Dodo. Collection of metadata is sufficiently capable (and intrusive) to effectively undermine third-party doctrine. The information that can be collected and analyzed makes this not only a new world, but also a new legal world. Panelist Cunningham reminded all that, while the Fourth Amendment applies to the government and not to corporations, some court opinions tend to extend Fourth Amendment protections into the corporate domain.

Panelist Kelly asked his colleagues to clarify what they meant by "continuous monitoring." Suppose a company sees IP leaving. Does the company have a right to investigate? Donohue argued that the company would need prior suspicion to turn on continuous monitoring. Cunningham said that legal and cultural issues would depend upon what you meant by "monitoring" and "continuous." There are Silicon Valley companies that monitor not employees, but traffic (for threat signatures, etc.). You must tailor your electronic monitoring not only to the law, but also to what your culture will tolerate. Calibrate your practices to the corporate culture.

The panel closed with a commendation of "strategic monitoring," giving due attention to the protection of privacy.

Global Cyber Security Perspectives

Prof. Catherine Lotrionte (Director, CyberProject, School of Foreign Service, Georgetown University) moderated a panel composed of Squadron Leader Emma J. Lovett (Royal Australian Air Force), Sanjay Virmani (Director, INTERPOL Digital Crime Center), and Dr. Undine von Diemar (Jones Day).

Much of the panel's discussion addressed international conflict in cyberspace. Virmani offered an overview of Interpol cyber crime investigation, noting that Interpol backed off from investigating state-sponsored acts.

Squadron Leader Lovett debunked the view that cyberspace was somehow the lawless Wild West — an ungovernable and unprecedented domain of unregulated conflict. In fact, cyber conflict offers no serious departure from the well-understood laws of war. She cited the Tallinn Manual in support of this, and suggested that Marconi himself, were he transported to the present day, would readily come to understand cyber conflict.

Lovett also noted that Australia has declared that a cyber attack will trigger mutual defense provisions of the ANZUS pact.

A questioner challenged Lovett about the application of the law of armed conflict to the cyber domain. Isn't this more controversial than she suggested? While nations agree that the UN Charter applies, there's a significant silence on the law of armed conflict. Lovett thought there was less controversy here than sometimes meets the eye. The UN Charter, after all, recognizes the inherent right of self-defense, and that right is important (even to China and Russia). This implies that judgments will be made about what triggers self-defense, and that in turn makes attribution important.

Lovett also observed that the law of war is very much a "do-as-you-would-be-done-by" affair (which is why, she noted in passing, that Abu Ghraib was so damaging). We should abide by jus in bello (right conduct during a war), despite what others may do. And that applies in cyberspace as well.

Another questioner asked about what the cyber equivalent of an armed attack might be. Must there be death? What if the first effects are, say, economic, and not lethal? Do they justify an armed response or not? Lovett responded by reading from the Tallinn Manual, which prohibits attacks on illegitimate, civilian targets. While the Tallinn Manual isn't law, it's nonetheless an important source for understanding how major states will understand the law. There are, of

course, difficulties about neutrality and private actors — attribution is tough — but the cyber domain doesn't really present us with anything radically new in international conflict.

Moderator Lotrionte concluded by pointing out that cyberspace isn't really a "commons," and commended the Tallinn Manual to all in attendance.

The Emerging Law on Corporate Cyber Liability: Privacy, Data Breaches & System Failures — Oh My!

David B. Coher (Principal, Reliability and Cybersecurity, Southern California Edison) moderated the panel. Panelists were Christopher Dore (Edelson, LLC), Hilary Hageman (Vice President and Deputy General Counsel, CACI International Inc.), and Dominique Shelton (Alston & Bird LLP).

Panelist Dore began by citing transparency as a standard. He stressed that liability starts from how much transparency and consent you've obtained from those whose information you hold.

Panelist Hageman, bringing the perspective of a Federal Defense contractor, reviewed the amount of sensitive information a Federal Defense contractor handles. She described her concerns about the liability to which the very nature of the Defense contracting business exposes a firm. Contractors must deal with a "panoply" of requirements. Compliance is extremely daunting, as is the attendant liability. There are also reputational risks that can effectively debar you (unofficially) from further contracting.

Panelist Shelton opened by saying that any company using the Web is vulnerable on grounds of both cyber security and privacy.

Panelists noted the increasingly expansive and aggressive role the Federal Trade Commission (FTC) is playing in cyber enforcement. Shelton ran through varieties of putative class actions brought on the basis of various laws and regulations — these are expensive and burdensome. We're beginning to see FTC enforcement actions, and the Federal Communications Commission (FCC) shows signs of becoming increasingly active, as are state attorney generals.

Moderator Coher asked if big data were becoming too big. Are companies retaining too much data? Shelton thought companies don't know what they don't know, and that they retain data against unknown future needs. Retaining data brings liability, even if the data don't obviously fall under relevant law. She recommended one way of reining in unnecessary collection: have mobile app developers use a checklist to decide whether they really need the data that the apps they develop would collect.

In the Defense sector, Hageman said, much data storage is defined in contracts with the government. Thus, contractors need to pay close attention to particular kinds of data, and to the contractual requirements that govern their collection.

Dore thought the private sector had become a bunch of data hoarders, with deep misconceptions concerning what value various kinds of data have. "People don't understand what data are valuable, and why. Why medical data is worth more than credit card data." Data are not only over-collected, but also poorly protected.

Moderator Coher asked what counts, really, as informed consent to data collection, and offers as an example supermarket loyalty cards. Dore responded that most people who consent don't fully realize that they're "giving carte blanche to share their data with anyone forever." Shelton described "California on the Go" as a measure to explain what data are collected. The plaintiff's bar, she said, "is interested in low-hanging fruit, where there's little transparency," and noted that there are compliance measures companies can take to reduce the risk of litigation.

Coher asked how the panelists approach the standard of "reasonable protection of data." Shelton thought that a definition might emerge from pending litigation, but that it's not here yet. But

there are still things companies can do, particularly by developing checklists for privacy and data protection. Hageman said the NIST Framework provides some great common denominators. But you've got to be careful with respect to each set of regulations. Satisfy the standards of reasonable protection laid out in your contracts, and exercise good digital hygiene.

Dore was asked to discuss the Superfish affair, in which Lenovo pre-installed Superfish software in its machines, exposing unwitting customers to a man-in-the-middle vulnerability. Superfish was installed without consent or notification. Lenovo has apologized and remediated, but there's considerable exposure. Doro believes that Superfish "dwarfs" the Target and Anthem data breaches in terms of exposure, statutory damages, and so on.

Hageman, answering a question about board visibility of cyber liability issues in advance of an incident, said that she thinks a publicly traded company should take shareholder issues very seriously. She would hypothetically advise a board to appoint one or two tech-savvy members, and hold meetings to discuss IT issues specifically. Dore offered another suggestion: "A fox knows how to get into a hen house. If you're protecting a hen house, hire a fox. So, if you'd hire a white hat hacker, consider hiring a plaintiff's attorney to look for problems."

Cyber Risk: Governance & Board Responsibilities

Peter Gleason (President, National Association of Corporate Directors) moderated a discussion by Justin G. Castillo (Head of Legal, BT Americas, Inc.) and Ivan Fong (Senior Vice President, Legal Affairs and General Counsel, 3M).

Moderator Gleason opened the discussion, mentioning the CareFirst breach disclosed just the day before. It's essential to understand this kind of breach as an enterprise risk issue and not an IT issue, he said. "With greater connectivity comes greater risk," and cyber risk must be a board meeting agenda item.

Panelist Castillo wondered whether connectivity had rendered the organizations ungovernable, at least in traditional terms. He believes the mental model for security is shifting from imagining it as a fortress to conceiving it as a kind of immune system. Lawyers think of risk as something to be eliminated, but a more nuanced understanding is necessary. He concluded his opening remarks with a scare story about the growth of data: the Internet-of-things will routinely collect and store petabytes of data. Where? Just imagine the nightmarish implications for discovery.

Panelist Fong offered three (immediately amended to four) Rs with respect to dealing with a board: Risk (both external and internal), Resources (oversight), Readiness, and Response.

Gleason noted that only 5% of public company boards have tech committees. 12% have risk committees. Should boards, he asked, include technical experts? Castillo thought that while membership depended upon circumstance and need, more board involvement in granular scrutiny would be valuable. Fong agreed that membership depended on a company's circumstances, but said he has seen technical people serve on boards. He also recommended educating the board. Equip them to ask the right questions, to understand the answers, and not to be intimidated by those answers.

If our systems can get hacked, a questioner asked, what about portal providers, NASDAQ and the like? How secure are they? Castillo answered, with some indelicate exaggeration, that "as long as we have humans in the loop, we're totally screwed." Secure solutions can indeed be a pain, and it's worth trying to make them easy enough to use that they won't tend to drive users into insecure workarounds. Fong suggested looking at the level of security that the information in question requires. For example, the most sensitive merger-and-acquisition information might be reserved for face-to-face discussion. On the other hand, email is probably just fine for lunch invitations. You might also consider, Fong said, that you keep your money in a bank and not under your pillow. Perhaps you might want to entrust your information to someone whose business it is to secure it.

When a CISO in the audience asked the level of detail he should go into with his board to discuss the cyber security program, Gleason advised him to recognize that his lexicon is different. Speak in plain language. Consult, maybe, with the CFO and the General Counsel on presentation. Castillo counseled simple explanations, citing Einstein's dictum that, if you can't explain something simply, you probably don't understand it yourself. Consider the questions you think they'd have, and try to answer those. Fong advised getting feedback from the board. How was the presentation? Did you understand it? Any questions? Castillo offered a tip from BT: they use John Boyd's OODA construct when describing their security processes, and they've had good success with this approach.

To a question about D&O insurance, Gleason advised that boards should have someone (not an insurer) review their D&O policy annually. There are always gaps, and the business judgment rule is the safety net. Castillo and Fong agreed that there seemed to be no cyber-specific gaps or pitfalls: essentially, a reasonable man standard prevails.

A questioner said that enterprise risk management was the cornerstone of the NIST framework. Given that, how do you integrate the various stakeholders? Gleason said that "enterprise" means "everything" or "everyone." You've got to drive risk management down throughout the organization.

Fong took the last word: with great connectivity comes great risk, but also great opportunity. Too much restriction brings perpetual enforcement, and that's not where any enterprise wants to be.

the cyberwire

editor@thecyberwire.com
www.thecyberwire.com

@thecyberwire
+TheCyberWire

About The CyberWire

The CyberWire is supported by CyberPoint International and its community partners. We invite the support of other organizations with a shared commitment to keeping this informative service free and available to organizations and individuals across the globe.

Revised 8.6.15