the cyberwire

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

Georgetown Cybersecurity Law Institute

May 21-22, 2014 Washington, DC

May 21

Georgetown's Cybersecurity Law Institute opens this morning with discussions of legal and regulatory frameworks. We'll be expanding our summaries with tomorrow's and Friday's issues, but early speakers have stressed the multinational regimes that companies effectively operate under, the importance of data discovery and a sound assessment of the value enterprises have at cyber risk, managing exposure to third-party risk, and corporate organization for effective cyber security.

May 22

Georgetown's Cybersecurity Law Institute opened yesterday with a welcome from Dean William M. Treanor. He was followed by Nuala O'Connor of the Center for Democracy and Technology, who offered an overview of "the promises and perils of cyber security in daily life."

The morning's first panel dealt with enterprise security programs, including a discussion of roles and responsibilities: general counsel, CISO, CIO, etc. This discussion led naturally to a consideration of cyber frameworks and standards, and their legal implications. The NIST cyber security standard (developed with contributions from several thousand stakeholders) was developed as a tiered system. It is not, panelists stressed, a standard. It is, however, an excellent starting point to structure the conversations that an enterprise's key players need to have in preventing, detecting, and mitigating a cyber event. A tiered system as proposed by NIST accommodates the needs of organizations with widely divergent levels of cyber maturity. It is also intended to accommodate rapidly evolving risks.

Frameworks and standards are not legislation, and the panel generally agreed that legislation would be premature. In this area, the voluntary will precede law and regulation. NIST's cyber framework will help companies shape governance and prepare for emerging standards. FTC consent decrees, in contrast, were described as high-level "lagging indicators" that amount to binding cyber standards.

Increasingly, the panel observed, we find that sharing cyber information not only mitigates vulnerability but also limits liability. Information sharing appears to be on its way to becoming a part of standards of care. Such sharing should extend outside a business to vendors and partners: a company needs to take reasonable steps to make sure that vendors and partners have the wherewithal to protect what's invaluable to that company. Reasonable cyber security is a continuing process of assessing and managing risk.

Suzanne E. Spaulding, Undersecretary for the National Protection and Programs Directorate in the Department of Homeland Security, delivered the afternoon keynote. She stressed DHS's commitment to sharing information with the private sector. DHS sees itself, in fact, as an advocate for the private sector in the often difficult-to-access intelligence community, and is working to disseminate cyber intelligence as effectively as possible to stakeholders in the unclassified world. She sees the private sector as having an important role in distributing and circulating cyber intelligence – companies see much that DHS doesn't, and they can contribute

to developing intelligence. An interesting note for researchers: Undersecretary Spaulding said that DHS is currently interested in developing machine-to-machine, automated, near-real-time cyber intelligence sharing.

The two afternoon panels were devoted to the role of the general counsel in cyber security, and to the state and prospects of the cyber insurance market. General counsels have come to play a useful mediating role facilitating intracompany cyber security communications. They remain deeply involved in corporate cyber security discussions and also play a significant role in compliance, acting especially on behalf of the corporate board. Several panelists had considerable experience with the electrical power industry, which has long been a cyber target. They offered an interesting perspective on insider threats: not all insider risks involve nefarious actors. Consider engineers who circumvent an air-gapped system – perhaps they put in a backdoor that enables them to troubleshoot a problem from home (say, at midnight, when they'd rather phone it in than visit the plant).

The panel on cyber insurance noted that data breach insurance is relatively more mature than business interruption insurance. The costs of a data breach are better understood than those of business interruption. Although the market for business interruption insurance is about 100 years old, today's cyber risks are sufficiently novel to present poorly understood problems. The market hasn't yet reacted to the reality of cyber business interruption, and there's a lack of credible cyber risk actuarial data. (That risk is analogous to supply chain risks.) There's a robust third-party market, but the first-party market for transferring risk (of business interruption) is still forming.

We will wrap up our coverage of Georgetown's Cybersecurity Law Institute tomorrow evening. In the meantime, we've included some articles below that address topics relevant to the institute's discussions.

May 23

The second and final day of Georgetown's Cybersecurity Law Institute opened with a long interview of recently retired FBI Director Robert Mueller. (Benjamin Powell, former general counsel at ODNI, conducted the interview.) Mueller traced his own interest in cyber security to his reading, in 1989, of Clifford Stole's book "The Cuckoo's Egg," which described the hunt for someone who hacked into the Lawrence Berkeley National Laboratory. As director, he saw firsthand the difficulty of attribution in the MafiaBoy denial-of-service attack case, an international investigation conducted by the FBI and Canada's RCMP.

In such cases it was important to identify the natural person responsible — the "warm body at the keyboard" — and such identification will remain important. More indictments like this week's charging of PLA hackers will surely come, and will be important in deterring not only individual criminals but state services as well. He recommended that people read the indictment, calling the culpability of the individuals named "indisputable." (The recent arrests of BlackShades crimekit users afford another good example of a salutary deterrent.)

We've seen, Mueller added, many state-conducted attacks. While the PLA indictments dealt with information theft, he believes that attacks will become increasingly destructive. 2012's attack on Saudi Aramco sets the template for the near future. He believes a large-scale destructive cyber attack is "inevitable."

Companies need to identify both insider and external threats, and prompt detection is needed to stop and mitigate breaches. Seven out of ten of the businesses that the FBI warned of breaches last year were unaware that they'd been attacked, so there's clearly much room for improvement both within the private sector and in terms of public-private cooperation. The private sector tends to connect with government episodically, often on the basis of who knows

whom. Cyber security can take lessons from counter-terrorism work, where cooperation among federal, private, state, and local actors is relatively more advanced.

As director, Mueller was surprised at the degree to which companies feared they would lose either intellectual property or a market edge if they shared information. He thinks that the government might usefully provide companies with protection from lawsuits prompted by information sharing.

Business, like the government, continues to grapple with finding the right structures to deal with cyber risks. In the government, despite progress, there remain lanes that inhibit information sharing, and these need to be dealt with. The NSA (which has "more geeks per square foot" than anyone else) is essential in interagency cooperation, particularly in the collaborative use of malware databases. The FBI's own cyber squad dates to 2002, and the Bureau now has more than one thousand specially trained cyber personnel available to respond quickly to incidents. Nonetheless, it remains tricky assembling the right expertise from around the country. We may have, in the future, virtual squads for investigation cyber attacks.

The FBI itself is a target, but Mueller treated this threat as a special case of the long familiar attempts by foreign governments and organized crime to compromise the Bureau. "The FBI's been a target for years. It is hit daily." The Bureau is ahead of the game in identifying internal threats (having for decades been concerned to identify spies). Mueller thinks corporations haven't taken sufficient steps against insider threats, and that they could increase their security by systematically looking for anomalies.

In response to a question about what the Bureau is doing to recruit more cyber personnel (with an explicit reference to hiring people with tattoos, and an implicit reference to the present director's joke about bringing in some hacker-stoners), Mueller made an interesting point: pure technical skill is insufficient. You need cyber ability among your Special Agents, to be sure, but you also need traditional investigative aptitude, and that's the skill set that the Bureau looks for.

An Enforcers' Roundtable followed former Director Mueller's interview. Representatives from CEB, the Connecticut Attorney General's office, the Federal Trade Commission, and the Department of Justice Criminal Division participated.

When asked what triggers an agency's involvement, the panel agreed that reports from agencies, victims, and press splashes all play a role, especially since finding one attack often leads to the discovery of others. The Federal Trade Commission representative pointed out that for a civil law enforcement agency like the FTC, news accounts and breach notifications are a great place to start.

The first thing a business should do is establish a plan before a breach occurs. Once there's a breach, a business should expect a lot of interaction with law enforcement. Be prepared for this, and don't underestimate the difficulty of improvising a breach response. A cursory customer service response won't cut it. The right people must be in place, their plans must be reasonable, and their plans must be carried out. You have to be able to execute the plan in a crisis. (The representative of Connecticut's Attorney General drew upon "I Love Lucy" for an example — Lucy and Ricky had thoroughly planned an impending childbirth, but the plans went out the window at the moment of labor, even with Fred and Ethel helping.)

Companies must reasonably oversee their third-party vendors – they can't assume a vendor's taking care of it.

Standards of reasonableness – as pervasive as they are throughout the law – continue to evolve, and those pertaining to cyber are, of course, still developing. Any granular cyber guidance from the government would soon be overcome by events. One questioner suggested, reasonably, that more disclosure of government security practices might clarify reasonableness.

The institute concluded with a simulation of cyber breach response. Among its lessons was advice to know your networks, know your data (and understand that it's an asset), and know your vendors. Compromise of a privileged ID is the attacker's holy grail, and international forensic investigations particularly benefit from the ability to inspect machine data (as opposed to just user data).

Panelists stressed the importance of disciplined communications during a cyber incident. They also reinforced the advice to have a pre-breach plan in place to avoid the "hair-on-fire" scramble of improvising during a cyber event.

Almost all cyber breaches have some human error at their root. The best prevention is job specific training and awareness. Job-specific reinforcement of sound cyber practices pays off, and it helps immeasurably if there's a good example at the top.

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 8.4.15