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

1st Annual Billington Corporate Cybersecurity Summit

May 27, 2015 New York, New York

Tom Billington opened the conference by thanking its sponsors and introducing the first speaker.

Future Cyber Threats Post Sony and Anthem

Former NSA Director Keith Alexander (now President, IronNet Security) began with a Memorial Day remembrance of those who served, and continue to serve, in the Iraq-Afghanistan war. He noted that early in that war, the intelligence developed wasn't the intelligence that troops needed. Signals intelligence (SIGINT), which one would think yielded its product relatively quickly, was too slow to arrive, and the NSA worked hard to drive down the delivery time. "We fixed a broken strategy," he said, "and today cyber strategy is broken."

Consider the bromide that says there are two kinds of companies: those who've been hacked and those who will be hacked. "If everyone's hacked, then cyber strategy is broken." We have a huge number of companies selling cyber products, but we've yet to figure out how to integrate them. This will keep up with neither technological change nor the pace of threat evolution.

He reviewed lessons learned from observing Russian operations (both cyber and kinetic) against Georgia in 2008, and the history of the establishment of Cyber Command. The upshot of those lessons is that we need to let machines do what they do well, and let humans do what they excel at. We need to share at network speed, and reduce the time during which we're vulnerable. Anything less will be inadequate. We need to share cyber attack indicators and warnings. This, he argued, is technically possible today, through behavioral models and big data analytics ("the sentries on your networks") with situational awareness achieved by sharing across sectors.

We can make a huge leap forward if we take an integrated, partnering approach to security, and if we realize the potential of big data analytics and behavioral modeling.

In response to a questioner who asked how to get Congress ("a bunch of Luddites," the questioner called them) to understand cyber realities, Alexander said the challenge is to explain how FISA can provide both security and support for civil liberties. He described his experience, while serving as NSA Director, with dealing with the presidential panel on surveillance, and his surprise at the intelligent and fair hearing that the NSA received. There's common ground to be found here, and he recommended an opinion piece he and one of the President's panelists recently published on where that common ground lies. In any case, Congress needs to fix FISA and pass appropriate cyber legislation.

To questions concerning whether there were sufficient incentives in place to encourage information sharing, Alexander said that companies want to share but want protection as well. They fear liability, reputational damage, and government regulation. So we can and should, he concluded, establish ways in which they can share cyber information anonymously.

An Interview with John Carlin, Assistant Attorney General for National Security, National Security Division, Department of Justice by Deborah Feyerick, CNN.

Feyerick began by asking how we can build an integrated approach to information sharing across the classified and unclassified domains. Carlin began by noting the importance of imposing costs on attackers, and then considered why it seems difficult to share information that would help us do so. The biggest obstacle to sharing among companies, he finds, is typically the general counsel. To ease the minds of counsel, the Department of Justice has clarified the Electronic Communications Privacy Act and the applicable anti-trust law. "Ultimately, however, we need legislation to provide liability protection." We also need to do more to share classified information, and this will entail getting clearances for individuals at companies, declassifying more information, and sanitizing classified information for broader release.

In response to Feyerick's question about how the government itself shares information, Carlin offered that he thought the government was doing better. Joint intelligence bulletins, for example, provide actionable information without breaking anonymity.

He noted the difficulty of defending against dedicated nation-state attacks. "There's more to defense than buying the right system (and firing the CISO if it turns out to be the wrong one)."

Carlin also decried the "blame-the-victim mentality" he sees with respect to cyber attacks. A company hacked by a nation state is a victim. While there's surely room for technological improvement in security measures, he also said the government and the private sector needed to "work with you, CNN, and other media on getting the coverage right." The media should say, for example, that Sony took the right steps when it was hacked, and explain why.

Feyerick pointed out that the government attributed the Sony hack to North Korea — but what about China and Russia? We don't hear as much attribution to them. Carlin thought there had been a change in this regard: "We no longer consider nation-state hacks purely an intelligence matter. We now investigate with the goal of attribution for the purpose of imposing costs."

This prompted Feyerick to ask at what point a nation-state cyber attack becomes an act of war. It's a complex issue, Carlin said, and noted, for example, that most insurance coverage has an act-of-war exception. So there are serious consequences, both obvious and non-obvious, to calling a cyber attack an act of war.

Are we, Feyerick asked, creating another layer of bureaucracy in the form of, for example, the CTIIC, that will only make defense harder? Carlin agreed that this was a question we always need to ask, but that we needed a center of analysis. The new center fills this gap.

Cybercrime and Incident Response — Viewpoints of the FBI, SEC and Private Sector.

Shawn Henry (CrowdStrike's CSO) moderated the cybercrime panel. Panelists included Leo Taddeo (Special Agent in Charge of the Cyber and Special Operations Division, New York Office, Federal Bureau of Investigation), David Remnitz (Global and Americas Leader, Forensic Technology & Discovery Services, Fraud Investigation & Dispute Services, Ernst & Young LLP), and David Glockner (Regional Director, Chicago Regional Office, U.S. Securities and Exchange Commission). They focused on incident response and preparation.

Remnitz noted that there are a few ways a company generally learns it's been compromised. Law enforcement might discover it, the company's security or IT team might recognize the compromise, a third party (especially investigative media like KrebsOnSecurity) might tell them, or they might find telltale data on the dark web.

Understand, Remnitz said, that your criminal adversary is well resourced and persistent, and make sure you've got good digital hygiene in place.

Henry asked the FBI's Taddeo to remove misperceptions about engagement with law enforcement. Taddeo thought that both the FBI and the Secret Service have come a long way in not making an incident worse. They try to minimize a company's impact of working with them. FBI incident response teams include lawyers who speak the corporate counsel's language.

Henry asked the SEC's Glockner about regulatory agencies' roles. The role the SEC plays, Glockner explained, would depend upon whether you're a public company or an SEC registrant in the securities industry. He urged companies to work through cyber incidents to determine materiality for disclosure. Materiality, while not entirely subjective, is nonetheless highly dependent on circumstances.

Remnitz said that organizations have to assume that some form of discovery will be intertwined with their incident response. They should think how they'd handle the incident from a traditional discovery perspective, and prepare a team that's able to handle their legal exposure.

Cooperation between industry and regulators or law enforcement agencies does face continuing obstacles. Classifying too soon or too much can be a big obstacle to information sharing, Taddeo observed. Glockner explained that the SEC has been trying hard to make its relationship with industry less adversarial, especially with respect to this shared cyber problem. "In fact, we approach cyber from a collaborative, not an adversarial, perspective."

In response to a question about whether law enforcement would refuse to investigate a cyber crime if the damage it did fell below a certain level, Taddeo explained how the FBI decides to investigate. "The damage threshold is no help at all. How do you know the damage until you've investigated?"

Henry closed the session by taking the last question about getting security clearances for industry. He said that declassification was the better move, especially when sources and methods wouldn't be revealed, and that cyber intelligence generally was far less likely to compromise sources and methods than was human intelligence.

Lessons Learned from the Latest Corporate Cyber Breaches

Moderated by Dan Guido (Co-Founder and CEO, Trail of Bits) *this panel* included George Rettas (Global Information Security Chief of Staff, Citi), Robert Bigman (President, 2BSecure, and former CISO — with fifteen years' tenure — of the CIA), and Gregory Touhill (Brigadier General (Ret.), Deputy Assistant Secretary for Cybersecurity and Communications, U.S. Department of Homeland Security). The big lesson, as first enunciated by Touhill and seconded by the others, is that "Cyber is a risk management issue. Boards and executives, not the server room, are the ones who need to understand the risks." Beyond that, panelists saw the limitations of user education. Bigman, taking the extreme position, called it "stupid" and "a waste of money." Other panelists pointed out that it might take only one user mistake to compromise an enterprise, and so "Whether you're 20% on fire or 100% on fire, you're still on fire."

The panel advised proper attention to configuration management, which would have rendered some recent breaches less severe. They concluded with a discussion of the insider threat, which they suggested is best understood as a personnel problem, not a cyber issue proper (although the fact that we tend to consider it as a cyber issue illustrates how expansive, or disparate, the definition of a "cyber security issue" is).

The New Cybersecurity Paradigm for Corporations: Replacing Perimeter Defense with the Secure Cloud.

Edward Amoroso (Senior Vice President and CSO, AT&T) began with a question: "If you're sharing cyber intelligence, with whom are you sharing?" Many small and medium enterprises don't have big (or any) security staffs. So how should we proceed?

He described the old, canonical security model: if you're inside the firewall you're safe, but not outside the firewall. He argued that this model is fundamentally silly: you let packets in, do a lot of work screening them, but also induce a lot of vulnerability. He described all the different, exploitable apertures a firewall must have if an enterprise wants connectivity at all. "There are millions of rules at the perimeter, and everything is an exception." When you consider these apertures, add in misconfigurations, unauthorized network connections, and mobility, the perimeter looks pretty porous.

He proposed virtualization and the use of the secure cloud as the solution, claiming it was "inevitable anyway, so you might as well embrace it." Diagramming such a model, he pointed out that it looked a great deal like a virtuous botnet, and botnets are notoriously resilient.

The Department of Homeland Security (DHS) and its cyber priorities

Dr. Phyllis Schneck (Deputy Under Secretary for Cybersecurity and Communications, US Department of Homeland Security) delivered a keynote in which she reviewed current DHS cyber policy and programs, emphasizing the importance of innovation, new efforts at declassification of cyber intelligence, and the pending opening of the Department's new West Coast office. The basic problem we face in cyber security, she said, is that "Computers aren't smart. They're just fast." So we need to take advantage of their strong suit — speed — and let human beings use them in smart ways. This involves developing trust, building teams, developing a capable workforce, and giving them current situational awareness. That situational awareness will depend upon machine-to-machine sharing ("and when we at DHS say machine to machine, we really mean it"). We should think of cyber in biological terms, re-imagining security as immune systems. And, she said, we should be enhancing security without compromising civil liberties. She touted recent initiatives — ISAOs, fusion centers, and others — and invited both feedback and cooperation. (An opportunity to work with the Department of Homeland Security is linked below.)

Top CISOs and CEOs Roundtable: Best Practices for the New Cybersecurity Paradigm.

(This panel was conducted under Chatham House Rules, so none of the remarks are attributed to individuals or their organizations.)

What about securing the perimeter?

The problem of the perimeter is fundamentally insoluble (and there was much agreement with Amoroso). Our goal should be to build resilience—our networks should be as resilient as a botnet, or — to take a positive example — as resilient as Netflix.

Enterprises should be able to "stop time" and "preserve a temporal bubble of data" to enable recovery after an incident.

Destructive malware, while an interesting concept, is more often talked about than seen. Offline backups and proactive attack detection seem the way to go in defending against such malware. And in designing defenses, it's important to understand the threat actor's motivation. What their objectives are will properly shape your countermoves.

What's going to keep you awake five years from now?

We'll see a steady drumbeat of attacks. We're in a structural arms race: the offensive will always be structurally dominant. Offense is cheaper, attribution is tough (which renders deterrence effectively impossible), and above all the attacker only has to get it right once. In general, we should expect in five years to see more of the same. What might count as a "cyber Pearl Harbor" is unclear, but the panelists expect to see the situation of the defense deteriorate before it improves.

Who's helping? Is academia in particular helping?

There was hope expressed that we might see the development of cyber norms, particularly norms of behavior for nation-states. They're significant players in cyberspace, and they should establish some norms analogous to those they've evolved elsewhere (including in other domains of conflict).

Other panelists would like to see more business schools discuss and teach cyber issues, particularly cyber risk assessment and management.

CISOs are, panelists felt, feeling deflated. The message they get from people who "want to sell you junk" is "you're being hacked, you're being hacked, you're being hacked." We should try to empower CISOs not by letting them "hack back," which was dismissed as "a big waste of time," but by putting security first. Effectively doing so involves getting human beings out of the business of managing IT at scale. Instead, let the machines do that — they should be able to do it well. Strong attention to secure languages would be an important way forward, and university researchers could help here.

What's your biggest challenge in getting the resources you need?

One panelist said, without provoking much if any disagreement, that he didn't have trouble finding cyber security talent, because he could afford to hire people and enable them to work from where they live. (Others agreed that requiring relocation was often an obstacle to recruiting.) This diverted the conversation into a discussion of the kinds of skills needed in cyber security. "The most damning line in the 9/11 Commission's report was the finding that we suffered from a lack of imagination." It's difficult to both conceptualize a new approach and then articulate it in a way that cuts through the noise. We certainly have a problem with basic IT hygiene, but we face even greater difficulties with integration: "We've got a hard time putting great point solutions together into an enterprise solution."

Questions from the audience:

1. Are any of you partnering with IT audit teams to get independent security assessments? The short answer was "yes," and some panelists said it was useful to rotate audit and security personnel. Doing so effectively is, in some respects, a sales job, and panelists suggested looking at creating an internal team of white hats who report not to IT but to risk management, and whose job it is to break things. "Everyone would rather be a pirate than join the Navy," as one panelist put it, with poetic if not historical accuracy, and that might be a useful approach to putting into effect this kind of partnership.
2. Don't you think we're going to see a shift from concentration on IT security to transportation security, power grid security, and the like? The panel agreed. One pointed out that 18-wheelers, which collectively comprise a hugely important piece of the American infrastructure, were today already connected in ways that far, far outstrip the connectivity people worry about in private automobiles. When hackers turn their attention to the 18-wheelers, the consequences could be disastrous.

3. What about the healthcare sector? Panelists said that we've seen a lot of attacks on healthcare, and we're going to see a lot more. Payers — by which they mean insurers — have a lot of information about individuals, and since individuals have multiple roles (employee, consumer, customer, etc.), their information can serve as a point of access into the enterprises those roles touch. Nation-states, in particular, want individual information. We need, panelists thought, to put different classes of protection in place to protect data of varying importance.

Cyber Insurance: A Practical Guide to a Growing Necessity

(This panel was conducted under Chatham House Rules, so none of the remarks are attributed to individuals or their organizations.)

Cyber insurance policies currently take a pretty broad approach to what's covered. You describe the risk factors and risk controls, and then you work through the process of pricing.

Insurers want to know if you've got a plan — and, if you do, they want to know if you've got the bench to execute that plan. Whether you know whom you're going to call in the event of an incident. The panelists advised having a relationship with your insurance carrier, and to take the common sense approach of treating cyber risk as if it will be a matter for litigation.

Panelists noted that data owners held responsible by their customers for those data's security.

They thought that it was time for insurance to put some financial incentives in place — that is, adhering to certain best practices and standards of care to earn favorable rates (Bbut they reminded the audience that compliance isn't the same thing as security: it's a starting point, not an ending one). The insurance market is creating a de facto standard of care.

They closed by echoing points made earlier in the day: "We've got to recognize that you're not a bad company because you got hacked. Look: banks still get robbed. Why can't we see that in cyber?"

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