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

SINET Innovation Summit 2015

June 25, 2015 The Times Center, New York, NY

Welcome

LifeJourney CEO Rick Geritz, acting as the day's master of ceremonies, opened with brief remarks welcoming participants and characterizing the ways in which cyber security has become both a boardroom and an international issue.

SINET CEO Robert Rodriguez also welcomed the participants. He noted the innovation he saw during a recent trip to Tel Aviv. Clarity about the threat drives innovation, and he looked forward to seeing increased cooperation on cyber security among trusted allies. Industry need not wait for government to undertake research and development, and he challenged entrepreneurs to continue their commitment to innovation. Now's the time for them to come to Washington, not only to share such innovation but also to influence policy as well. He briefly reviewed both the Sony and OPM incidents, and saw them as a clear sign that we need to move beyond legacy systems and approaches.

Regulation, Enforcement, and Information Sharing: a View from the SEC

Commissioner Luis A. Aguilar of the US Securities and Exchange Commission (SEC) delivered the morning keynote, mentioning the OPM breach as a clear object lesson in the importance of cyber security. The balance of his talk described the SEC's focus on cyber crime (a species of crime which he said is evolving and advancing rapidly). He holds up the commission's new rule, "Regulation Systems Compliance and Integrity" ("SCI" in brief form) as a regulatory model that other agencies might well follow. He believes SCI avoids the pitfalls of an "overly prescriptive" approach, and regrets that it doesn't apply in all areas of capital markets. In some respects, the SEC fills an educational function by issuing firms cyber security guidance: advice on protecting client data would be one example of such education.

Enforcement efforts, he said, have difficulty keeping up with new developments in cyber crime—the SEC's current investigation of the FIN4 crime group is an example of that difficulty—but that enforcement nonetheless needs to keep pace as criminals advance their own techniques. Intelligence is vital to enforcement, Aguilar said, and he closed with some sharp criticism of the current state of cyber information sharing, especially as practiced in the ISACs (Information Sharing and Analysis Centers): it's too slow and fatally siloed.

Global Trends in Cybercrime

Anne Neuberger (Chief Risk Officer of the US National Security Agency) chaired a panel composed of Suleyman Anil (Head, Cyber Defense, Emerging Security Challenges Division, NATO), Chris Gibson (Director, CERT-UK), Eduardo Perez (Senior Vice President, North America Risk Services, Visa, Inc.), and Dane VandenBerg (Director, Qintel). The panel generally agreed that the rapid expansion of organizations' attack surfaces, which the Internet-of-things accelerates, has led to generally increased vulnerability. The hugely complex scale of enterprise

IT, driven by market pressures, inevitably opens new vulnerabilities. Gibson noted that small businesses continue to show an unjustified sense of immunity to cyber crime, but small size is no protection at all.

This is particularly so, VandenBerg noted, when simple, commodity attacks remain so effective. Perez, agreeing that well-known and low-tech criminal attacks continue to succeed, argued that the PCI standards have helped considerably here. "Where we find successful attacks, we also find PCI deficiencies."

Asked about incident response, Gibson described UK-CERT's incident-handling mission and advised every organization to have a sound, practiced, and regularly reviewed response plan. He, too, saw the continuing threat of simple attacks and strongly recommended basic cyber hygiene. Anil, in turn, advised business to connect both incident-response planning and basic cyber hygiene to business continuity planning. "Believe me, lack of a telephone number in an emergency can be a problem."

As far as anti-crime measures are concerned, Perez said that his industry was interested in technologies that "devalue" compromised data, particularly EVM, tokenization, and encryption, but also neural network scoring methods to assign individual transactions risk scores in real time.

VandenBerg discussed darknets and the Dark Web. He believes the threat they pose has been much hyped. The threat observed coming from that space, he said, is actually relatively low.

NATO's Anil and NSA's Neuberger had the panel's last words, with Anil observing that "every conflict today is a cyber conflict," and Neuberger remarking on the surprising extent to which we see criminals succeeding with familiar techniques.

Where is the Identity, Credential, and Access Management (ICAM) Roadmap headed?

Moderated by Greg Crabb (Deputy Chief Information Security Officer, US Postal Service), this panel included Michael Antico (Director, Global Head of Identity and Access Management, Barclays), David Hah (Vice President, Corporate Information Security and Risk, Hearst Corporation), and Tom Patterson (Vice President, General Manager, Global Security Solutions, Unisys).

Hahn lamented the organizational headwinds CISOs face: "You're bureaucrats," they hear. "You're slowing down our business." But they should draw a lesson from those headwinds — CISOs have got to understand the business to effectively manage identity and access for security.

Antico saw challenges in the general movement to the cloud and the attendant disappearance of the perimeter. Security, he said, is all about data protection. He sees identity and access management challenged by changes in the individual's lifecycle in an organization. Hahn sees shadow IT as one of the issues associated with the cloud, and drew the conclusion that businesses should set up enterprise accounts with the big cloud providers. In the longer term, business needs to work out a cloud-federated identity.

Since stolen or abused credentials are among the most common security problems an enterprise faces, Antico argued that there should be widespread adoption of behavioral analytics around use of credentials. Patterson, tying the identity business to network defense, sees microsegmentation, not firewalls, as the coming wave, and believes that this will involve a new mindset. Hahn agreed with the points about behavioral analytics, and recommended applying the sort of analytics now used to recognize paycard fraud to access management problems.

Patterson advocated focusing on two areas of innovation: risk scoring of behavior, and linking physical security to identity. Antico observed that since a lot of banking customers want easy

transactions and don't care (much, all the time) about security, there's a design challenge here as well: a clean user experience designed for security would help tremendously.

In response to a question about privacy, Hahn commented that "customers also get a little weird when they realize how much data you have on them." This has a strong generational aspect: millennial expectations are unrecognizable to baby boomers.

There was general agreement that we don't need to introduce new form factors, and that business as a whole needs to learn from the paycard industry, which "knows how to do it." Patterson also pointed out the effect liability shifts have on what businesses and individuals are willing to accept with respect to security. Hahn advocated a close look at data and behavior, and more work on plug-and-play identity management. Antico recommended a focus on hygiene, movement toward account-on-use, development of a seamless user security experience, and further work to reduce attack surfaces. Patterson closed by calling the federated model of identity "ultimately the way to go." He also noted that the Internet-of-things will ultimately surround you, and know an enormous amount about you. Why not give the IoT a role in identity management?

Emerging Challenges Facing the Security of the Internet

Conrad Prince, the United Kingdom's Trade and Investment Cyber Ambassador, asserted that it's striking how well understood the threats are. Some 80% of hacks could be prevented by basic hygiene. Cyber security "isn't just about black boxes," but about culture, policy, and—especially—skills. (In an aside, he also noted the interesting work that remains to be done on the monetization of personal data. We'll eventually buy goods and services with our PII.)

From a national security perspective, we must expect that more threat actors will begin making more destructive attacks. Aramco in 2012 was a turning point in this trend. It's interesting to see threat actors attacking their targets' reputation and trust, yet we still lack an understanding of what would constitute a cyber act of war and what constitutes a proportionate response to a cyber attack. Clearly, there's need for work toward international norms of behavior in cyberspace.

The Evolution of the CISO: Security is not just an IT problem anymore. Why the CISO has to be a business leader, not just a security leader.

Chaired by Comcast Ventures Partner David Zilberman, the panel included Mark Connelly (Chief Information Security Officer, Thomson Reuters), Lisa Humbert (Executive Vice President, Chief Information Risk Officer and Head of Information Risk Management, BNY Mellon), Carolann Shields (Chief Information Security Officer, KPMG), and Marc Varner (Corporate Vice President and Global Chief Information Security Officer, McDonald's Corporation).

Panelists were asked to begin with an overview of their organization and their place in it. Connelly said that the CISO's role has evolved and now demands a business-centric approach, with a primary emphasis on risk management. Humbert saw, amid much reorganization, some remaining uncertainty about the CISO's role. He acknowledged that there's a growing understanding that risk is everyone's responsibility, and that information risk isn't confined to technology. The CISO must translate an understanding of risk, explaining it in terms the business can understand and relate to in order to help the business units understand how an incident would affect them. CISOs must use analogies with personal technology. Connelly sees the CISO's role as necessarily multidisciplinary, and that embedding elements of the CISO's organization in business units is helpful. Varner noted that people do have a commonsense notion of risk. If you talk in terms of that understanding, you'll succeed in communicating: make the message about risk real to those who need to hear it.

In response to questions about relations with boards, Shields said the security understanding at the board level surprised her—it was far higher than she'd expected. Connelly emphasized the importance of not wasting the board's time. Help them learn, and thereby build trust.

In response to a question from TruSTAR in the audience about the risks of information sharing, the panel thought that the real risk lay in not sharing as opposed to sharing. SEC Commissioner Aguilar says information sharing as a problem, but the panel thought that, while sharing with the government might indeed suffer from the issues Commission Aguilar saw, sharing peer-to-peer or business-to-business is really no problem at all.

In closing, Zilberman asked the panelists to advise vendors on how to sell to them. Their advice: Be brief. Don't argue. Get to the point. Don't ever oversell, and be timely.

Managing the Opportunities and Pitfalls of the Global Convergence of Physical and Logical Security Risks

Jerry Archer, Senior Vice President and Chief Security Officer of a major financial services company, chaired this panel, which included F. Edward Goetz (Vice President and Chief Security Officer, Exelon Corporation), Ross Mandel (CEO, VerifyItNow), David Stender (Senior Vice President and Enterprise Security Officer, M&T Bank), and Scott Tousley (Deputy Director, Cyber Security Division, US Department of Homeland Security Science and Technology Directorate).

Archer set the tone by noting the ways in which criminals recruit insiders and drawing the lesson that businesses "need to fix stupid."

Goetz described the effects—wholly positive—of combining cyber and physical security groups. They bring different and complementary skill sets to problems and, working together, they become much more effective at getting to the "why" of an incident. An integrated approach to security will therefore bring together cyber and physical security talent with the third essential element of a sound program: intelligence.

The challenge of identifying counterfeit items—a real risk to health, safety, and prosperity—brings the convergence of the logical and the physical into sharper focus, Mandel argued.

Stender, noting that his bank's customers don't care whether fraud is physical or online, said that as the offensive side converges, the defensive side needs to as well.

After describing the Department of Homeland Security's research and development investments, Tousley offered an anthropological take on why organizations continue to find it difficult to integrate cyber and physical security. The tribes, he said, still don't communicate—cyber and physical security specialists speak different languages, and so do different sectors. Cyber experts need to learn to communicate to the other tribes.

To Archer's question about the importance of ethics in security, Mandel noted the centrality of ethics to anything in business. Tousley also called ethics indispensable, if only because regulations will never catch up with all the business decisions we need to make. Stender thought education was needed: too many people in business tend to overlook the reality that there are, indeed, malicious people out there. In Goetz's view, it's a matter of setting expectations. "You've got to communicate ethical expectations to the employees."

Asked about the key to convergence, Goetz thought that integration was working well. In internal investigations, Exelon sends out both physical and cyber investigators. The cyber investigators have learned that there's a human behind the keyboard (because investigations teach an appreciation of motive) and the physical security investigators have become aware of the technical possibilities human criminals exploit. Exelon has both a physical and a cyber SOC, and they're co-located. Stender said that M&T Bank tries to cross-train, and seeks to build teams with embedded complementary skills. But an organization has to be ready for convergence: the IRS, for example, had a converged program a decade ago – but they weren't

ready for it, and it had to broken up and rebuilt from the ground up. When you bring different cultures together, Goetz thought, a key to success is the first big win.

In closing, the panel thought that technology had gotten pretty good at automating compliance. They saw a need to balance control with permissibility, but with a tilt towards permissibility. They've seen better security wherever controls become—and appear to become—part of a business process. "It all goes back to risk. Find what's important, and prioritize."

Trends in Cyber Security Investment, Mergers and Acquisition

Anand Sanwal (CEO of CB Insights) proudly introduced his presentation with a slide featuring a unicorn extruding a rainbow from its fundament, and gave an overview of trends in cyber security start-up investment. He discussed "unicorns"—privately-held companies valued at $1 billion or more—and also what might be called incipient unicorns—companies CB Insights thinks are on track to become the next stars of the investor community. He named ten incipient unicorns in the security sector: Bluebox, RiskIQ, ThreatStream, Pindrop Security, Wickr, Detex Systems, DarkTrace, Cylance, Elastica, and Dashlane. They've selected these as worthy of attention on the basis of their hiring growth, news chatter, partnerships, customer signings, sentiment, burn rate, and investor quality.

Managing Security Data Overload

John Jolly (Chief Revenue Officer of RedJack) chaired this panel, whose members were Jay Leek (Chief Information Security Officer, Blackstone), Tas Giakouminakis (Chief Technology Officer, Rapid7), and George Rettas (Managing Director and Chief of Staff, Global Information Security Department, Citigroup).

Jolly opened by asking about the implications of collecting the large amounts of security data organizations compile. The general perspective of the panel was surprising—they really didn't see security data overload as a problem. "We want visibility," Leek said. "Since visibility depends on information, we want as much information as we can have, and we want a record of it." He qualified this somewhat by clarifying that the data he wants are data important to achieving situational awareness, but on the whole he wants more rather than less. And he wants to store it for analysis, even while granting that "legal paranoia tends to drive us to keep data longer than we probably should."

Rettas, channeling Sun Tzu, saw data collection as a means to self-knowledge and knowledge of one's adversary. He advocated predictive risk management based on knowledge of that adversary.

Giakouminakis saw the battlefield as having shifted from servers to users. Adversaries are increasingly getting into noisy environments where it's hard to detect them. You can, with the right big data tools, keep all the data you need for compliance purposes. Data overload doesn't become a problem unless you mingle large amounts of unanalyzed data with data needed for incident response.

Leek sees considerable utility in analyzing business operational data with security data proper. Rettas agreed that buckets of data could be usefully correlated to see anomalies. He also noted the value of human intelligence in this process, a contention he supported with claims that human intelligence played an important part in detecting and understanding the breaches at both Target and JPMorgan. Giakouminakis thought that security people can easily become jaded or biased, convinced by habit that they know what they're looking for. Adding a naïve data scientist to the team can help compensate for that bias, and is especially useful in detecting unexpected threats.

Talent, Leek thought, is more important than tools. "I can't afford a team member who can't code in Python." Rettas called process "everything." It comes before technology.

With respect to technology, Leek said that traditional signature-based security technology "no longer does me any good." The insider threat (including the threat posed by a compromised account) is his current area of focus and concern. There's no single pane of glass any vendor offers that helps him. "If you don't have a rich API, you won't get into my environment." Rettas always asks how tools integrate. He argued that you've got to think of integration upfront.

The panel concluded by asserting that information security is a risk management business, not a compliance business. Compliance may be necessary, but it's not sufficient.

Closing Keynote: Developing a Standard of Care

The day's final keynote was delivered by the US Deputy Secretary of Homeland Security Alejandro Mayorkas, who spoke briefly but clearly about some challenges in cyber security. After a brief introductory description of his department's new office in Silicon Valley (its goals are to recruit talent and capture innovation), and praise for Doug Maughan and the department's Science and Technology Directorate for their role in fostering innovation, he posed some questions for the conference.

Explaining the department's vision for cyber threat information sharing, he asked whether we could reach a point where knowledge of cyber threat information isn't treated as a commodity to be traded, but rather shared freely. He predicted that we're not far from an SEC determination (and he stressed that this is a prediction, not based upon any inside knowledge of SEC workings) to require full sharing of material cyber information. He would welcome this; 8-K disclosure would shape behavior for the better.

He's often asked, Secretary Mayorkas noted, if the NIST framework is a de facto standard of care. In his view, it's not. It is what it says it is: a framework. So, no—it's not a standard of care. In fact there's a void with respect to standards of care, and that void is being filled by litigation, regulation, state attorneys general, and the plaintiff's bar. But litigation is a poor way to set standards of care. Does the market want a standard of care? If so, how do we reach that outside the path of litigation? Mayorkas predicted that state attorneys general will seize on "the recent breach at a government agency" (he didn't name OPM, but that was clearly the agency in question) to drive their own legal agenda. He closed with a plea for help, and for public-private partnership, in evolving sound, beneficial standards of care.

Final thoughts

SINET's Robert Rodriguez closed the conference with some takeaways: Board involvement in cyber is vital. Resilience is crucial. Development of sound standards of care is essential. He encouraged everyone to meet with the entrepreneurs in attendance, and he closed by thanking Doug Maughan and the Department of Homeland Security's Science and Technology Directorate.

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 8.11.15