the cyberwire

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

Cyber 5.0

June 10, 2014 Laurel, MD

Rosemary S. Wenchel (Deputy Assistant Secretary Cybersecurity Coordination NPPD, US Department of Homeland Security) delivered the morning keynote. Opening with a brief description of her department's response to the NIST cyber security framework, she encouraged businesses and others to ask DHS for cyber help.

She then offered reflections on what recent visits to Silicon Valley suggested to her about the future of the cyber industry. Many of the start-ups she's seen there are "excessively well capitalized" ("excessively" in a good sense—there's a great deal of funding available to the sector). Such start-ups focus on scaling, clouds, and end-user mobility. There's less talk now about "big data" than formerly, and more talk about "important data" collected in the cloud and manipulated through algorithms designed to reveal the data's importance. Hugely scaled projects are driving increased crowd sourcing as an approach to problem solving.

Wenchel sees hardware increasingly disaggregated from software. Hardware is now a commodity – everyone will build to a common set of hardware. The intellectual property and value are all in software. For example, Silicon Valley disses BlackBerry, but reveres RiM as a patent-holder: its intellectual property is seen as crucial to the industrial Internet. It's now the era of ARM: the Valley seems to believe ARM is the wave of the future.

She offered two examples of start-ups to watch: Realm, which does big data streaming to mobile devices, and Mesosphere, which brings Google-scale computing to everyone.

Wenchel concluded with an overview of NPDD's current thinking. They care about maintaining the US as a secure, resilient environment, and they care about maintaining US economic competitiveness; the cyber-physical nexus is their central concern.

DHS is seeking economies of scale in cyber security, and she encouraged small business free participation in DHS cyber protection efforts.

In response to questions from the audience, Deputy Assistant Secretary Wenchel said that DHS is interested in research into highly scaled problems, such as DDoS and DNS issues in the financial sector. She addressed cyber education, both in terms of public awareness (as in the Stop, Think, Connect initiative) and in terms of workforce development. She emphasized the importance of beginning workforce development through early cyber education.

A morning panel session addressed trends in critical infrastructure protection. Moderated by Wesley Kaplow of Polar Star, the panel included Jonathan Nguyen-Duy (who leads global public sector cyber security services at Verizon), Eric Ayotte (Vice President of Cyber and Network Security at M&T Bank), and David Fastabend (Vice President of Advanced Information Solutions at Exelis).

Verizon's Nguyen-Duy presented an overview of his company's widely respected 2014 data breach investigation report. It reveals a world dramatically changed since 1994. There's a race now to identify threats, respond to them, and assess their consequences, but the criminal market is efficient, which enables threats to evolve rapidly. Breaches are outpacing our ability to detect and mitigate them. It's telling that most breaches are still discovered and reported by third parties.

Nguyen-Duy called out the three biggest sources of breaches: miscellaneous errors (with a big lead over the others), crimeware, and insider threats. He recommended that enterprises counter the insider threat by focusing on privilege abuse and on understanding the local area network (LAN). Most breaches occur on the LAN, so know your data. With respect to crimeware, he argued that ninety percent of breaches attributable to it arose from simple control failures. So, do continuous monitoring. Know what your normal state looks like (and what it should look like). Follow basic controls; watch for exfiltration of data (look at your logs, and again, know what to look for). He concluded with an exhortation to, in the end, "trust your gut." Cyber remains as much an art as it is a science.

M&T Bank's Ayotte began by observing that small and medium businesses can have difficulty enacting the NIST framework. Yet they are very much in the cyber criminals' crosshairs: criminals know the money in financial fraud is in the commercial, not the consumer, space. Wire transfers are very fast, and hence very dangerous. We often see hundreds of thousands of dollars transferred very rapidly offshore. Unfortunately, many governments turn a blind eye to this. Companies are put out of business by cyber theft of a few hundred thousand dollars, and sometimes it's not recoverable. The Bank of China, for example, now in effect laughs and responds to complaints with 'too bad, tell your customer the money's gone.'

Malware plays an important role in financial fraud. M&T Bank sees a lot of customers with malware on their machines, picked up from phishing emails or waterholing sites. Those who move money should use a dedicated computer for their transactions, with no email and no Web surfing.

Banks are seeing more social engineering in the frauds perpetrated against their customers: man-in-the-email attacks, for example, like assuming control of a C-executive's email to direct malicious actions. They're also seeing an upsurge in ransomware that can encrypt file systems throughout your network. Unfortunately, it may actually be worth paying the ransom—the crime model wouldn't work if they didn't deliver keys.

Ayotte closed by recommending dual authorization in business banking. Make sure humans talk to one another before transfers. Protocols against secret fund transfers are also useful. Let people know you'll never ask them to wire money secretly.

David Fastabend of Exelis drew attention to the metaphors that control our understanding of cyber security. Our current master metaphor is the Cyber Box. We bring an industrial-age conception of everything as a machine to our thinking about security: we have a mechanically locked box, and my data should be in that box, nicely and statically secured.

But what if the problem isn't mechanical, but biological? Consider the difference this might make in terms of transport, assembly, and structure. Mechanical transport is channeled while biological transport is diffusive. Mechanical assembly is positional; biological assembly depends upon surface matching. And mechanical structure is geometric, but biological structure is topological, or connected. Cyber is, of course, interested in connectivity.

An alternative guiding metaphor for cyber, then, is biological. (The mechanical metaphor isn't wholly out of place, and can still inform our understanding: cyber systems evolve, for example, but they do so at machine speed, and under intelligent direction.) But our default understanding remains mechanical. We should consider what shifting to a biological default might mean for an alternative cyber security framework. Biological defenses have internal systems, not just perimeters or defenses-in-depth. They're also automatic. They respond to infections they sense. A network might do the same—detecting exfiltration, for example, tells you you're not right.

Infrastructure problems tend to be misconceived as mechanical problems, but this is misleading. Cyber tools must interact in the way biological systems do. The NIST cyber framework is good, Fastabend concluded, but it's analogous to basic biological hygiene: valuable but insufficient.

An afternoon session featured a panel on risk assessment and the threat spectrum. Steve Zotti (COO of Ciena Government Solutions) moderated a panel composed of Derrick Nixon (Director of Security Solutions at Honeywell Technology Solutions), Larry Letow (CEO and President of Convergence Technology Consulting), and Yul Williams (Technical Director for the National Security Agency/Central Security Service Threat Operations Center).

Dr. Williams opened the discussion by noting that what began as plain annoyances are now more serious threats that tinker with system destruction. Cyber attacks now place missions at risk, and this trend will continue.

Convergence's Letow asked the audience to consider the Target breach. A successful organization's leaders all lost their jobs over a cyber attack. Cyber affects everything we do, and companies need to understand this. It's not about protecting all the data; it's about finding and protecting the most important data.

Honeywell's Nixon predicted that future warfare will target critical infrastructure first, because it lies at the base of citizens' trust in their society and its institutions. Yet we as an industry have a checklist mentality. It's difficult to escape that, but our adversaries aren't bound by—nor are they following—checklists. We need to develop ways of training that mimic the complex and chaotic reality of cyberspace. Analytical thinking by cyber professionals trained within the right environment will provide our ultimate safeguard.

NSA's Williams seconded the point about chaos and complexity. We're trending toward hundreds of millions of malware samples, but not all malware operates in every domain. If we were more mature in how we categorized the threat, we'd find network defense more manageable. We should be moving toward prediction. And, ultimately, we should get to the point of adaptation under attack, where we'd be resilient, reconfiguring your systems in real time even while you're under attack. So, the ultimate goal should be a resilient ability to accomplish the mission even while under attack.

Convergence's Letow noted the importance, with external threats, of preserving and collecting intelligence. Insider threats, on the other hand, lend themselves to behavioral observation, prediction, and prevention.

Ciena's Zotti noted that we're trying to push our threat intelligence out into the distance, building proactive capacity. If we're not proactive we're just taking punches, and the opposition only needs to land one punch. What, then, he asked, are the key tenets of a good security program?

Letow argued that the organization from top down has to understand the problem and put dollars toward it. You have to start with training, and with recognizing that it's not just IT's problem anymore.

Here, Nixon, observed, is where chaotic training pays off. Staff trained chaotically builds muscle memory. We've got to train to segment the threat and continue operations. Threat groups are well funded and unconstrained by acquisition rules. We need comparably agile rules, and the entire supply chain needs to be protected. Threat information sharing is vital – one of the worst things we can do when we're attacked is keep it to ourselves.

To an audience question about opportunities and challenges, Letow described mobile as a huge challenge: mobile device detection and management are important. Application security is the next challenge, but that, of course, doesn't secure devices. Understanding and monitoring user behavior is also important. There's no single fix for cyber security; organizations have to craft their response to how they do business.

To a question concerning the technologies that are essential to protecting the US government, NSA's Williams said that you want tools that will help achieve situational awareness. There

are now some 70,000 potentially malicious tools freely available over the Internet. DARPA's cyber genome project is interesting – we wanted to understand malware's phylogeny, and a set of tools that lets us see this helps craft countermeasures. We need tools that will help the whole community share situational awareness. We need good visualization. We've found that most exploits are rooted in earlier exploits. Things that hit the government hit industry, too, so sharing is essential to defeating the threat.

The panel concluded with pleas to increase information sharing and to organize for continuity, not reconstitution ("When you reconstitute, you've lost," as Williams put it). Make every employee a stakeholder in cyber security. Develop a training environment, perhaps a gaming environment, and use it. Train the organization so that reactions to attacks are normal and appropriate, not panicked. Exercise continuity regularly.

Finally, the panelists agreed on the importance of cyber education. They called for effective outreach to middle and high school students. "The greatest cyber tool has yet to be invented," Nixon quoted. "It's in the mind of a middle schooler." We've got to make cyber security the cool sport to be in. Letow recommended an approach like the ideation that LifeJourney provides. We'll have an effective cyber workforce only if we get to young people early.

Ron Gula, CEO of Tenable Network Security, delivered the closing keynote address. He began with questions intended to debunk some common misconceptions about cyber security. (Prominent among such misconceptions, he argued, is the prevailing view that insider threats always differ significantly from external threats. He pointed out that any pentester, once they're inside a network, behaves like an insider.) He noted the effect of the Target breach: the CEO and others lost their jobs. But it's very difficult to draw prescriptive best practices from that episode. What about Sears? What about JC Penney? They have different business models and thus need different security programs. As we design such programs, Gula suggested, we should look for ways to make better security decisions and gather timely feedback on our policies. Are they being followed? Are they working? Do they meet our business needs? He sees continuous monitoring as extremely important, and he's excited about the possibility of increased security automation: you want to take the human out of the loop wherever possible. Automation can do great things in network monitoring, and it should extend to databases, mobile devices, and other aspects of the enterprise.

Articles linked in the conference section in the daily issue touch on some of the themes presenters addressed.

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