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

Cyber Montgomery 2015

July 30, 2015 Universities at Shady Grove Conference Center, Rockville MD

CyberMontgomery 2015 met in Rockville, Maryland yesterday. Sponsored by the Montgomery County Department of Economic Development and the Federal Business Council (FBC), the conference featured participation by industry, elected officials, federal agency leaders, and academics. They discussed the evolution of cyber security, workforce development issues, technology development and transition, cyber risk management, threat intelligence and incident investigation, and the business climate necessary to foster innovation and development. We summarize the proceedings here.

"**A career's worth of lessons learned the hard way**." Tony Sager (Senior VP and Chief Evangelist, the Center for Internet Security) delivered the morning keynote, in which he shared the perspective he's gained on cyber security over a long career. His title, "From Communications Security to Cyber Security," summarized the transition he's seen. This transition can be usefully viewed as a change in control model. The old model prevailing in the era of communications security was that of a monopoly. In the era of cyber security we've moved to a free market model, which Sager illustrated by pointing out the extremely dynamic networks we now take for granted. The online world evolved chaotically and bears all the marks of that evolution.

Where we once approached security in terms of formal models, we now recognize that the presence of an adversary disrupts all such models. We've had, he said, to learn from our mistakes ("and our misery"). Those charged with cyber security face the "defender's dilemma": "What's the right thing to do, and how much do I need to do? How do I do it? How can I demonstrate to others that I've done the right thing?"

The basics of cyber security matter terribly, he argued. Cyber defense equals information management, not information sharing, and no single security tool can stand alone. (Sager observed that security tools tend to have "crappy" security properties.) We now understand security in terms of the OODA loop – the "observe, orient, decide, and act" decision cycle.

The cyber era has also developed a richer, more complex picture of the threat, and that understanding offers some opportunities as the defender tried to operate inside the opposition's OODA loop. As talented as the opposition may be, "the bad guys aren't magicians. They've all got problems, budgets, bosses and so on." That is, they're functionally very much like the good guys. Understand what they do, he recommended, and interrupt it: "Induce uncertainty into the bad guy's cycle."

He concluded by strongly advocating security frameworks like the Twenty Controls and the NIST Cybersecurity Framework. These may represent best practices, which "by definition stand out." Our collective task is to make the standouts commonplace.

"**Workforce needs of the future — building preparedness across whole-of-society.**" Haden Land (Vice President, Research and Technology, Lockheed Martin Information Systems and Global Solutions) addressed the challenge of building a cyber workforce capable of meeting the industry's needs. He noted some familiar important trends: the explosion of mobile

access, the dramatic increase in the number of mobile devices, and the proliferation of the Internet of Things. All of these are placing strong pressure on the labor market, and that pressure will only increase.

There's a need, he argued, to address workforce needs early. An approach that fosters STEAM (science, technology, engineering, arts, and math) education holds the most promise: STEAM offers invaluable insights into problem solving (and imaginative understanding of problems) that a narrower concentration on STEM might miss. He noted the formation of a bipartisan STEAM caucus in Congress, and commended its approach to workforce development. He also commended private initiatives like LifeJourney.

Land didn't confine himself entirely to workforce development; he also addressed the nature of the solutions that future workforce would have to envision, create, and implement. He reviewed the current state of cyber best practices, and noted that they should figure into sound risk management. He particularly recommended the World Economic Forum's cyber risk framework published earlier this year.

"**Aggressively non-regulatory.**" Dr. Romine (Director of the Information Technology Laboratory at the National Institute of Standards and Technology) described "the evolution of applied cybersecurity at NIST." NIST can justifiably claim some real successes in fostering technological advance (he didn't say this in so many words, but we will). The Institute has been successful, in Romine's view, because it's built its credibility on a foundation of intellectual capital, and that capital has accumulated through a balanced portfolio of basic and applied research.

He reviewed a few NIST initiatives he believes are likely to improve cyber security over the next few years: the NSTIC is working on alternatives to the password, and NICE is fostering cyber education (much along the lines recommended by the day's earlier speaker, Haden Land). These involve strong, NIST-brokered public-private cooperation. That cooperation has emerged from decades of trust. Why does the private sector trust NIST? Romine says, with some evident pride, that NIST earned trust because it's been "aggressively non-regulatory."

Communication doesn't mean dumbing down. A panel discussed the crucial issue all CISOs face: communicating with their boards (and the rest of the C-suite). Keith Young (Chief Enterprise Information Security Official, Montgomery County) facilitated a panel composed of Stanley F. Lowe (Deputy Assistant Secretary, Department of Veterans Affairs, Office of Information Security), Karen Lefkowitz (Vice President, Business Transformation, Pepco), David Mashburn (IT Security Manager, U.S. Pharmacopeial Convention), Jason Silva (CIO, ByteGrid), and David Yacono (Senior Director, Information Security, FINRA). The panel addressed the importance of building "a culture of compliance" without equating that culture with a checklist mentality; a healthy organization, for example, welcomes audits as a form of free consulting.

The panel's main bit of advice to aspiring CISOs, however, was to understand that businesses increasingly recognize the centrality of risk management to cyber security. CISOs need to understand how boards understand and evaluate risk, and they should learn to present cyber security in terms of a risk profile. Boards, CISOs will find, have deep expertise in risk assessment. CISOs need to find the right way of communicating with boards. But, as one panelist emphasized, "Presenting cyber risk in terms the board understands doesn't mean dumbing it down. Don't patronize them; you'll lose them."

Public-private partnership to address the big challenges. Nate Lesser (Deputy Director, National Cybersecurity Center of Excellence (NCCoE), National Institute of Standards and Technology) chaired a panel on how partnerships among industry and government can advance

work on the most challenging problems. The panelists included Brian Barrios (Program Manager, National Cybersecurity Federally Funded Research and Development Center), Gavin O'Brien (Project Manager, Health IT, National Cybersecurity Center of Excellence), William (Bill) Fisher (Cybersecurity Engineer, National Cybersecurity Center of Excellence, National Institute of Standards and Technology), Ben Smith (Field Chief Technology Officer - East, RSA), and Jeff Ward (Vice President, Federal for MaaS360 by IBM). Lesser opened with a frank acknowledgment that public-private partnerships have too often been less productive than one might have hoped (and expected). After a review of best practices, the panel pointed out two features that seem to characterize the most successful partnerships: they work on a common response to a common threat, and they recognize that the testing cycle is a particularly fertile field for public-private cooperation.

Translating public market experience into the commercial market. Moderated by Mobile System 7's Founder and CEO Mark McGovern, the panel consisted of Greg Virgin (President and CEO, RedJack), Jim Jaeger (Chief Cyber Systems Strategist, Fidelis Cybersecurity), Patrick Kehoe (Chief of Marketing, Arxan Technologies), and Donna Ruginski (CEO and President, SAINT Corporation). Maryland business is very familiar with the government (particularly the federal) market, and cyber companies in the region often begin doing work for the big agencies headquartered here. But given that the commercial cyber market is expanding faster than the government market, and is likely to continue to do so for the foreseeable future, these companies face the challenge of translating their success with the government into products, services, and solutions that are attractive to the private sector. The panelists, all of whom have succeeded in doing exactly that, offered their insights to the conference.

Educating the cyber security workforce. Chaired by Joe Roundy (Cybersecurity Program Manager, Montgomery College), the panel consisted of Steve Boden (MCPS Foundations Office), Silvia Vargas (CyberSecurity Professor, Montgomery College), Frank Skinner (Director, TAACCCT), Behnam (Ben) Shariati (Cybersecurity Graduate Program Assistant Director, UMBC, The Universities at Shady Grove), Michael Burt (National CyberWatch Center), Devina Pruitt-Mentle (Director and Co-Principal Investigator, National CyberWatch Center, K-12), Daniel Stein (Cybersecurity Education & Awareness, Department of Homeland Security), Marcie Nagel (Vice President of Cyber Programs, Variq), and Alton Henley Jr. (Senior Program Director, Information Technology Institute, Montgomery College). Their discussion covered the challenge of developing cyber security professionals, and how that development can begin in early childhood and continue through school, university, and adult continuing education. While some of the discussion was specific to local programs and conditions, as a whole it offered lessons applicable across the sector. It's worth noting that the panel's composition alone offers evidence of something many conference participants, from Haden Land to Michael Gill noted: the growing importance of community colleges in cyber education and training.

Cyber risk and liability: advice for small businesses. Chaired by Ira E. Hoffman (Cyber Montgomery Co-Chair, Principal, Offit Kurman, P.A.; Co-Chair, TCM Cyber Committee), the panel consisted of Matt Bergman (Chairman/ Co-Chair, Shulman Rogers' Commercial Finance Practice/Cybersecurity Practice), Karen Britton (Senior VP and COO, e-Management), Curtis Levinson (Private Consultant and United States Cyber Defense Advisor to NATO), and Dr. David McWhorter (Founder & CEO, The Homeland Security Consulting Group, LLC). If large businesses like Target, Anthem and Sony can be hacked, what can small businesses, with their relatively limited resources, do to most effectively mitigate cyber risk? The panel began with a discussion of the SAFETY Act, a US federal legislation that controls liability for users and providers of anti-terrorism technologies. The SAFETY Act has some applicability to cyber security: users of

SAFETY Act-covered technology receive a degree of protection from liability incurred from terror attacks. The key, panelist McWhorter noted, is that protections kick in when an act is deemed terrorism. The SAFETY Act can compensate, to some extent, for gaps in insurance coverage.

Cyber insurance is now in the relatively immature state of security product insurance in the aftermath of the 9/11 attacks. We're not yet at a stage, for example, where it's easy to achieve reduced premiums for demonstrated adherence to good practices. Given that immaturity, small business managers—CEOs, CIOs, CFOs—must understand their cyber risk exposure. The NIST Cyber Security Framework offers a useful way of approaching such understanding: businesses need to inventory their assets and prioritize them in order of criticality.

Easily overlooked in analyzing a business's cyber risk is its exposure to third-party risk. Small businesses should evaluate their contracts and agreements that place information at risk and consult a lawyer to help them.

Cyber security recruiters and job seekers: finding grounds for mutual understanding. Moderated by Kathleen Smith (Chief Marketing Officer, ClearedJobs.Net), panelists Kirsten Renner (Talent Management, Parsons) and Leslie Taylor (Talent Acquisition, ICF International) offered their insights into current stat of the cyber labor market. Developing the labor force for the future is important, but companies need to hire the right candidates today if they're to meet their contractual obligations and survive in commercial markets. Some successful companies are finding benefit in bringing recruiting from the back office into other parts of operations and management, but competition for talent remains tight.

One would think that, in a seller's labor market, job seekers would have few complaints. But one would be wrong: even (especially?) highly recruited technical candidates complain of shabby treatment by the companies trying to recruit them. This needn't be so, and the panel described lessons learned at successful companies, and how those success stories can inform mutual expectations.

Lessons from the Sony breach: big hacks are more like looting than stick-ups (says Norse). Fortune called the Sony breach the "Hack of the Century." This may be hyperbolic given OPM's recent issues, and given that the century is only halfway through its second decade, but Fortune at least is willing to put its money (in the form of its July cover) where its mouth is. Norse's Kurt Stammberger (Norse's Senior Vice President, Market Development) delivered the results of his company's investigation of the incident.

After an introductory description of Norse's services (and a display of its famous threat map) Stammberger said that Norse concurred with Sony and the United States government that the North Koreans showed up at the breach. "The NORKs came to the party," he said, but—and this is a very big "but"—they showed up late. Stammberger explained that many people misunderstand not only the Sony breach but major hacking incidents in general because they falsely imagine them along the lines of, say, a bank robbery or a boxing match: "A did something to B." But this is deeply misleading. The Sony hack wasn't like that; "It was more like looting after Hurricane Katrina than a boxing match."

According to Stammberger, Sony thought of cyber security properly in terms of risk, but they badly misunderstood their risk. One Sony executive said that the company wasn't going to spend $10 million to prevent a $1 million loss. Their actual losses in the breach amounted to some $200 million.

Stammberger reviewed a timeline of events surrounding the breach. Before Sony was hit, South Korean financial institutions were hit by the DarkSeoul malware, which was fairly clearly tied to North Korea. In March 2014, Sony announced the upcoming release of "The Interview," the

movie whose depiction of Kim Jong-Il's assassination (and buffoonery) was generally cited later as the cyber attack's casus belli. In May 2014 Sony began a series of massive layoffs, and thus generated a large pool of very unhappy, soon-to-be former, insiders. (Stammberger noted that many of the workers terminated were women who were subsequently replaced by their less-expensive male subordinates. He observed that this will be important in understanding the way the breach unfolded.) Between July and August 2014, the North Korean government began objecting to "The Interview." Over this same period, Norse captured DESTOVER-A malware.

DESTOVER-A was compiled English-only, with evidence of Sony internal network details, embedded USB drivers, and four-month-old IP addresses. This strongly suggests that its authors were using old lists, which would be characteristic of disgruntled ex-insiders as opposed to a remote access Trojan. Norse's entropy analysis showed no connection between DESTOVER-A and DarkSeoul. For one thing, DESTOVER-A's command-and-control nodes were well known, and this would tend to be uncharacteristic of a nation-state's operation. "But we did see connections to LizardSquad, JKT48, A-Team, SEA, Coup de Main, and others. But not a connection to the NORKs."

Data exfiltration began in August 2014 and ended on 22 October of that year. Some 113 terabytes of data were exfiltrated, appearing on a host physically located about ten miles away from a known Canadian LizardSquad bigwig.

On 13 November 2014 DESTOVER-B ransomware appeared, compiled with both Korean and English components. On November 21, the first extortion demand appeared.

On 22 November 2014 DESTOVER-C was compiled, with comments in Korean. And on November 24, tens of thousands of Sony machines were wiped. Some claims appeared online that the hack was done for the cause of equal rights. And, of course, Sony suffered its embarrassing email dump. In February 2015, Sony Pictures CEO Amy Pascal lost her job.

Stammberger summarized the attack as having been conducted in three phases: DESTOVER-A aimed at humiliation, DESTOVER-B wanted cash, and DESTOVER-C was after destruction. He then showed sanitized dossiers of two persons of interest. Both were women disgruntled over the layoffs. Both had technical ability. Both were connected to online gaming (including association with the "Frag Dolls" gaming circle). There was evidence of acquaintance with both LizardSquad and Anonymous (South African version).

Sony's cyber insurance wouldn't, Stammberger said, pay off on insider hacks, which gave the company a powerful disincentive to look beyond North Korea. And once the US Government publicly implicated the North Koreans, it would find it very difficult to walk back its attribution.

In Stammberger's view, the Sony breach started with disgruntled insiders, but snowballed out of control as others (including eventually the North Koreans) began to attack the company. "The instigators freaked out, and tried to go underground." This, Stammberger concluded, is typical of messy, dirty hacks. "They spin out of control." And so, when considering attribution, we should stop thinking that all cybercrime is like a stick-up. Often, it's more like looting.

Cheers and views from government (local, state, and federal). Elected officials gave foreseeable, if gratifyingly bipartisan, support to the creation of a favorable business climate. Montgomery County Executive Ike Leggett, after offering a broad overview of the threat landscape, gave a shout-out to local industry, academia, and the important role NIST plays in cyber security.

US Representative John Delaney (Maryland Sixth District) outlined prospects for cyber business development. He advocated tax incentives to sustain cyber industry growth. Drawing on his experience in business before he held elected office, he noted the consensus view that 10% of IT budgets should go to cyber security. Given forecasts that IT spending would reach $6 trillion in

ten years, he observed that this suggested cyber spending should itself grow to $600 billion over that period. He hoped Maryland would sustain and increase its leadership in the cyber industry.

Maryland's Secretary of Business and Economic Development, Michael Gill, delivered the closing keynote. After thanking cyber firms and their customers for doing business in the state, Secretary Gill described what pro-business tax policy and regulatory climate would look like "reflecting a state that gets it." He commended university research for its emphasis on transitioning to the marketplace, and he concluded with a call to attract "relevant capital" – that is, capital that knows how to evaluate opportunities in cyber security.

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