the cyberwire

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

IT Security Entrepreneurs Forum (ITSEF) 2015

March 17-18, 2015 Computer History Museum, Silicon Valley

March 17

Tuesday's workshops at ITSEF included tracks on the next-generation security operations center, venture capitalists' look at the cyber market, the impact of the software-defined perimeter, CISOs and the risks they take to mitigate risk, the speed of cyber innovation (and its frontiers), and advice on breaking into the Federal marketplace. Here are a few highlights.

What big commercial enterprises are looking for in security solutions. Facebook's CSO, Joe Sullivan, described his company's search for out-of-the-box solutions, and stated that he would rather work with startups than established companies. Usability and non-signature-based detection are of particular interest. HP's CISO Brett Wahlin described needing mature products on their network. They're less receptive to new, high-risk products, and anything they adopt needs to integrate well with their existing products stack. Analysis of data, not just mere collection and sharing, is critical.

The irreducible human element of cyber defense. Blackstone's Jay Leek argued that security has an irreducible human element, focused on changes, patterns, anomalies, and correlations. Recognizing this leads naturally to an approach that focuses on visibility, intelligence, and response (which Leek noted was equally applicable to insider threats). Adobe's Brad Arkin described taking a DevOps approach to building servers — rebuilding pristine environments every few hours — as a way of enhancing security. Doing this changes attackers' cost equation, particularly in the way that it reduces low-hanging fruit. CISOs on the panel generally agreed that traditional layered security would not keep up with swiftly advancing threats.

Next-generation SOCs: automation, information sharing, and anonymity. Panelists thought that barriers to SOC success tend to lie outside the control of the SOCs themselves. Executive clarity with respect to goals and direction is necessary (and often missing) for effective SOC operation, but all SOCs face the challenge of finding adequately skilled staff: here, too, the human dimension is crucial. Automation could relieve SOC watchstanders' routine workloads, freeing them to concentrate on analysis and anomaly recognition: information sharing at machine speed should, panelists thought, be the goal. Dell's Russell Murrell framed the SOC's well-known false alarm problems as essentially a big data analysis issue. But whatever automation emerges, recruiting staff will continue to remain a challenge. Stronger differentiation of roles and better-defined career paths would help. The panel concluded with observations about anonymity, which they agreed had to be the default position in information sharing. The Secret Service's Eduardo Cabrera argued that only anonymity would allow information sharing to scale. Homeland Security Deputy Assistant Secretary Greg Touhill called anonymity essential. He also hoped for legislation that would remove liability barriers to information sharing.

March 18

The second and final day of SINET's ITSEF 2015 opened with welcoming remarks by LifeJourney CEO and session moderator Rick Geritz, who took the opportunity to remind the symposiasts that cyber security has reached an inflection point.

Cyber collaboration's inflection point. The US Department of Homeland Security's Doug Maughan, who reviewed SINET's history (and the support its received from DHS), followed Geritz's introduction. He noted that more small businesses are interested in pursuing government funding than ever before, and that his department seeks to help them navigate these often unfamiliar waters. Describing the continuing shortage of cyber labor, he held up the DHS Science and Technology Directorate's support for the National Collegiate Cyber Defense Competition (NCCDC) as an example of how collaborative efforts to ease that shortage might succeed. He closed by predicting that 2015 would see considerable support, in both policy and legislation, toward better information sharing and security collaboration.

Robert Rodriguez, SINET's founder, welcomed conference participants and thanked the sponsors. He agreed with Rick Geritz that cyber's time is now. Cyber collaboration appeals to the human drive toward community and the natural desire to serve. But corporate CEOs have too often absented themselves from the development of cyber partnerships. He pointed to the Sony hack (less than war, but more than vandalism) as a transformational event. As the cost of security investments continues to rise, driven to a great extent by massive shortages of security professionals, enterprises need to move toward sense making.

High-functioning cyber security collaboration, technical debt, and the rise of malvertising. NIST's Nathan Lesser addressed the characteristics of high-functioning cyber security collaboration. Prominently among these is simply overcoming the shelfware phenomenon: there is a wide array of readily available security technologies that simply aren't used. How do we ensure users turn on the safeguards they've purchased? He promised more NIST cyber practice guides in the near future.

N. Shevelyov, CSO and Chief Privacy Officer of Silicon Valley Bank, spoke on the subject of "technical debt." This traditionally meant bad code, but today its meaning has shifted to encompass "unloved systems": the unpatched, unmanaged, and the forgotten. All systems on a network are often thought of as assets, but this is a mistake: many of them are liabilities. Enterprises are effectively managing a portfolio of assets and liabilities. Good change management is an important way of managing that portfolio. The bigger and older an enterprise is, the greater its technical debt load.

E. Manousos, CEO, RiskIQ, discussed malvertising. The ad ecosystem powers (and pays for) the Internet as we know it, but that ecosystem is also extremely attractive to bad actors, largely because of its powerful ability to target individuals. Targeting breaks down into geolocation, IP address, interests, intent to buy, and so on, which in the aggregate offer a good representation of an individual. Ads also scale across thousands of websites and millions of people. The ad ecosystem provides all the tools an attacker needs to operate at a distance. Malvertising is the ability to deliver a payload through an ad. It dramatically reduces the incremental cost of attacking a target. Malvertising doesn't need spam, botnets, etc. It's also hard to detect, not very noisy. Ad networks are typically compromised through social engineering, he argued, and so we need to think about transparency in the ad ecosystem. He concluded by framing malvertising as a community problem to be addressed through discovery, transparency, and reputation management.

Looking at the future of the cyber threat. Marc Goodman, Chair for Policy and Law, Singularity University, gave his professional futurist's take on crime and security. The bad guys, he said, "are out-innovating us." Systemically, things are working in the attackers' favor. Technology advances exponentially, and that gives us scalability problems: offense scales, but defense so far hasn't. Criminal markets increasingly resemble legitimate ones, with the familiar trappings of crowdsourcing, tech support, customer service, and so on. The human is disappearing into the criminal background, because so much crime can be committed by software, or

even algorithmically. And dependence on algorithms (in, e.g., securities trading) opens up considerable vulnerability (to, e.g., market manipulation). The Internet-of-things also opens up vulnerabilities we have no idea how to mitigate. Wearables, ingestibles, and implants open the human body itself to hacking. We're not, Goodman concluded, going to police ourselves out of this jam. The human immune system is a more fruitful metaphor. We're building our society on computers, and therefore (from a security perspective) we're building it as a house of cards: a hackable civilization. We can meet the crisis, Goodman concluded, but we need a Manhattan Project or a Project Apollo to do so.

A panel on the Internet-of-things, chaired by Reynold Schweickhardt (Director of Technology Policy, Committee on House Administration), included Peter Esser (General Representative, Washington Operations, NXP Semiconductors), Richard Hale (Deputy CIO, US Department of Defense), Tom Patterson (Vice President/General Manager, Global Security Solutions, Unisys), and Dr. Peter Sweatman (Director, University of Michigan Transportation Research Institute and the Mobility Transformation Center). Without minimizing its inherent risks, panelists offered a calming perspective on the Internet-of-things: technology has a way of keeping up with troublemakers. We do (and should) seek dependable mission execution in the face of capable cyber adversaries, and this is a feasible goal. The Internet-of-things is still young enough to permit us to design security into it.

A panel of industry experts including Robert Carey (Vice President Public Sector, CSC Global Security), Sam Glines (Co-founder and CEO, Norse), George Kurtz (CEO Crowdstrike), Stuart McClure (CEO, Cylance), and Kevin Walker (Vice President, Assistant Chief Information Security Officer, Walmart) – and moderated by CyberPoint's CyberWire Editor John Petrik — offered their views on the kinds of cyber attacks they see trending over the next three years. All agreed that we should expect to see attackers continue to use the methods that have worked for them so far. (And, more disturbingly, they suggested it's unlikely that the more sophisticated hackers have shown their hands — why should they, given the success familiar attack techniques have had?) Malware, as traditionally conceived, will continue to be eclipsed by the abuse of credentials, and social engineering will remain a principal form of attack. There was some difference on the value of attribution, but panelists generally agreed that understanding attackers' goals could guide enterprise protection in important ways.

US Government cyber initiatives. Dr. Phyllis Schneck (US Department of Homeland Security Deputy Undersecretary for Cybersecurity, National Protection and Programs Directorate) described her department's vision for industry, technology, and trust. DHS seeks to build situational awareness through near-real-time information sharing.

Brian Pierce (Deputy Director, Information Innovation Office, DARPA) reviewed his agency's history of investment in new technologies. He seconded Marc Goodman's suggestion that the human immune system should serve as a model (or metaphor) for cyber security. Pierce was followed by Peter Tseronis (US Department of Energy CTO), who described Energy's cyber technology roadmap.

Cyber security as a business imperative. Phil Zimmermann (Silent Circle President and Co-Founder) argued that digital privacy should be seen as a business requirement. He advocated putting human beings into the middle of authentication processes.

E. Salem (Bain Capital Ventures) addressed investing in cyber security. Business drives the infrastructure that in turn depends on security. Business pressure drives workflows away from proprietary systems to a public infrastructure. Any security system that depends on prior knowledge of an attack will be compromised. Bain is looking for alternatives to SIMs, which they feel have failed their promise.

An afternoon panel focused on communicating cyber risk management to boards, with

Feris Rifai (CEO, Bay Dynamics) moderating contributions from Lamont Orange (CISO, Vista Consulting), Jim Routh (CISO, Global Information Security, Aetna), and Myrna Soto (CISO and Chief Infrastructure Officer, Comcast). Panelists recommend communicating in terms of key performance indicators as opposed to traditional metrics.

Machine learning and big data problems. George Hoyem (In-Q-Tel) moderated a panel on data fusion and machine learning. Paul Grabow (US Senate CISO), Bob Pratt (Caspida), and Sriram Ramachandran (CEO, Niara) served as panelists. In-Q-Tel sees no less than 10 startups devoted to analyzing machine-generated data. Data are being analyzed against machine-learning tools for anomaly detection (another framing of anomaly detection as a big-data problem). Panelists noted that recent major data breaches, when examined retrospectively, all showed early signs of problems, but those signs were lost in the noise. An advantage of machine-based learning is its ability to detect anomalies that would escape rule-based systems.

Managing risk at NSA. Novetta CEO Peter LaMontague interviewed NSA Chief Risk Officer Anne Neuberger. Chief Risk Officer is a new position at NSA. Its role, post-Snowden, is to deal with increased complexity and to rebuild trust with stakeholders. The risks the agency wants to manage systematically include those of the Snowden type (compromise) or the 9/11 type (intelligence failure). They also usefully include disclosure risk — if something NSA did were disclosed, would it still have been worth doing? NSA also operates in an environment of compliance risk (because it indeed has a considerable compliance burden).

After a final interview with DocuSign's Keith Krach on the role of the CEO in advancing security, Robert Rodriguez closed ITSEF 2015 by thanking all participants, recognizing Shark Tank winner Picus Security, and congratulating the young 14-year-old entrepreneurs of the YES Club.

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