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

SINET Showcase 2015

November 3 - 4, 2015 The National Press Club, Washington, DC

Day 1

The SINET Showcase opened yesterday with an afternoon of workshops on topics the cyber sector is following closely. We were able to attend three of them; here are a few of the highlights.

Security, Identity and Law Enorcement in the Age of Bitcoin, Crypto Currencies and the Blockchain.

This workshop's panel was moderated by David Jevans, CEO, Marble Security, Chairman, Anti-Phishing Working Group. Panelists included Tigran Gambaryan (Criminal Investigation, Internal Revenue Service), Andy Greenberg (Senior Writer, Wired), Ken Miller (COO, Gem), and Carol Van Cleef (Partner, Manatt, Phelps, & Phelps, LLP). Their topic was the legal challenges crypto currencies and their related technologies present both users and law enforcement.

Bitcoin is familiar as a means of "anonymous" (actually, the panel distinguished, "pseudonymous") payment: it now has millions of users. The blockchain technology that underlies Bitcoin is, according to Miller, a permanent shared general ledger. Anonymity's been Bitcoin's goal from the start, Greenberg noted, with a libertarian wish to keep government out of financial transactions. He explained that everything that happens in the blockchain is public, but is nonetheless possible to spend Bitcoins in a nearly anonymous way. He illustrated this with a review of SilkRoad's history, the now-defunct, Bitcoin-enabled, "eBay for contraband." SilkRoad's initial vision was to confine its activities to "victimless crimes," mostly drug trafficking, but it swiftly found itself on a slippery slope to more brutal, even less defensible commodities (among them murder for hire).

Although SilkRoad's been taken down and its founder jailed, other Dark Net markets continue to thrive, with annual revenues of approximately $1 billion. People tend to overestimate Bitcoin's anonymity, Greenberg explained, and that's actually led to some takedowns enabled by blockchain technology. The Dark Net economy continues to grow, and its nominally libertarian pretences of enabling victimless activities continue to erode.

Gambaryan picked up the discussion of SilkRoad. He worked the Drug Enforcement Agency and US Secret Service investigations into that market, including that conducted by Task Force Marco Polo. Marco Polo had successfully infiltrated SilkRoad, and became a trusted confidant of SilkRoad's leadership. (The temptations of the black market are tragically strong—the agent who conducted the inflitration eventually himself became enmeshed in the criminal opportunities to which his work exposed him.) The investigators were able to trace SilkRoad's activity, Gambaryan explained, because Bitcoin is not, as generally believed, fully anonymous. "We were able to de-anonymize the users by tracing financial transactions."

Bitcoin, as Van Cleef pointed out in her turn, is not the only crypto currency. Indeed, digital currencies have been attempted since the 1990s. "I've been around payments a long time," Van Cleef said, "and when Bitcoin appeared it felt familiar." Bitcoin may indeed have enabled a new group of people to get access to financial resources, but its price spiked from illegal activity. The

Bitcoin community absorbed the lessons of earlier, failed attempts to create a digital currency. It is, for example, decentralized: it exists without anyone being in total control.

Bitcoin's decentralization, Van Cleef believes, presents interesting challenges from a law enforcement perspective. "Criminal elements have tended to be early adopters of these new currencies. Entrepreneurs never think that criminals will be their early adopters. They think they've created something very good. And the last thing a start-up wants to spend money on is compliance and lawyers." This mindset renders them vulnerable, and Van Cleef closed by noting that US law prohibits anyone from facilitating money laundering for illegal activities, in Bitcoin or elsewhere.

Miller, giving the entrepreneur's perspective and some direct historical experience, recalled PayPal's early days as a start-up. They quickly saw security and anti-fraud capability as competitive advantages. Today, institutions don't want to use Bitcoin because its blockchain is too public. But it does have its use cases, including meeting collateral requirements, cross-country transactions (which obviate the need to hold multiple currencies). And such use cases have obvious supply chain utility. Greenberg concurred: "You must obscure transactions to keep your competitors from seeing them. There are benign uses of Bitcoin."

But criminal use cases remain unfortunately prominent. When asked, "What's the killer consumer app for Bitcoin?" Greenberg answered bluntly, "It's drugs. Bitcoin's a cumbersome way to spend money, but around $100 million in revenue accumulates in black markets." Gambaryan agreed that it was difficult to see consumer use cases for Bitcoin.

Noting that Bitcoin is byproduct of a distributed network, Van Cleef saw the legitimate use cases really lying in securities trading, not consumer transactions. Miller agreed: "It's not hard to envisage land titles, stocks, energy futures, medical records, and so on being stored in the blockchain."

Partnering for Tomorrow.

Chaired by Ronald Green (Group Executive and CSIO, MasterCard), the panelists included James Katavolos (Citigroup), Jarrett Koulthoff (Spear Tip), Elias "Lou" Manousos (RiskIQ), Robert Novy (US Secret Service), and Greg Touhill (US Department of Homeland Security). The gist of the workshop was one specific kind of partnership: intelligence sharing.

Touhill opened with a description of DHS efforts to anonymize and share the information on cyber threats it receives from its partners. Particularly important here, he said, is the Department's ongoing push for rapid declassification of actionable intelligence.

As an executive at a private-sector intelligence company, Kolthoff emphasized that "there's always someone behind cyber attacks," and that knowing who they are and what their goals are is central to effective defense. Manousos added that it was valuable to "build a picture from the bad guys' perspective."

Katavolos described the value of sharing info collected in the last few years' big hacks, notably those of Nasdaq and JPMorgan. Citigroup is seeing "industrial-scale cyber crime emerging from Eastern Europe and (especially) Russia."

Green asked the panel for their lessons learned. Manousos offered two: "The essential first step is hiring the right people, getting the right leaders. The second lesson is the importance of explaining how and why it's safe to share information." Kolthoff thought cross-validation of information critical. The Secret Service's Novy thought that the value of information sharing was an old lesson, one the Secret Service learned as long ago as 1865, when it was given the mission of fighting counterfeiting, a national problem that had to be dealt with at the local level. So the Secret Service began its work, a century and a half ago, by bringing local police

and banks together. In the cyber age, the Service has expanded that legacy of partnership into the Electronic Crimes Task Force—which brings law enforcement, business, and academia together. This he sees as "training the law enforcement supply chain."

Addressing workforce issues by working with universities to prepare grads to hit the ground running has been important for Citigroup, Katavolos said. He also noted that so much—most—of the informtion enterprises need, globally, resides in their own CISOs' networks.

Taking up pending US Federal legislation, Green asked the panel what effects they believed the Cybersecurity Information Sharing Act (CISA) will have. Katavolos thought that informaiton sharing has been a system at risk, yet it hasn't been tested in any significant legal way. He hoped CISA would foster sharing by putting effective liability protections in place. Privacy fears he characterized as "a bit of a red herring." Information sharing should actually protect privacy.

Novy, alluding to the Five Eyes, reminded the panel of the importance of being able to share intelligence with international partners, and to deconflict operations with them. Green picked up (with alacrity) on the importance of deconfliction. "MasterCard sees all the big breaches," he said. "And there aren't a lot of different criminal groups behind them." MasterCard sees one agency working one case, another a different one, yet unknown to both agencies, they're looking at the same actor responsible for each of them. A questioner pointed out that Government uses a heavy hand on the victims of cyber crime. Katavolos thought this heavy hand flowed from attribution failure.

Touhill closed by asserting that sharing information requires that the Government be a good custodian of information. The Government hasn't always been that good custodian, and it's received a wake-up call.

2015, the Year of Cyber Insurance: Breaches, Business Continuity, and the Boardroom.

This workshop on cyber insurance was led by Mary Beth Borgwing, Chief Strategy Officer, LemonFish Technologies. The panelists included Anup Ghosh (CEO, Invincea), Gideon Pell (former Chief Risk Officer, New York Life, Yonesy Nunez (Senior Vice President, Information Security Leader, International Business, Wells Fargo), and Bill Russell (Executive Director and CISO, Cummins, Inc.).

Borgwing opened by asking the panel about board understanding of infosec risk, enterprise risk, and risk transfer. The tone of her question suggested that such understanding is generally poor. Russell said that, as Cummins' CISO, he advises the Chief Risk Officer on cyber risk transfer, but he finds this task problematic. It's an immature area, lacking actuarial data. "Consider automobile insurance--there aren't many accidents we don't know about. This isn't the case with cyber incidents. So cyber risk isn't well understood, yet. We can provide metrics, but we have difficulty telling whether a premium is worth the cost."

Pell stressed, from the point-of-view of the insurance industry, cyber risk is an operational risk, and should be understood from an enterprise-wide perspective. It's difficult to quantify: one must consider compliance, legal exposure, operations, and so on. One must also consider all the many stakeholders, which include senior executives and board members. "They need cyber translated into language they can relate to."

Borgwing thought that no one in the insurance industry had the pricing right. It's difficult to manuscript a policy, because we don't know all the costs. "The insurance industry needs first-party data. How do we create that sharing without giving away someone's risk profile?"

We need, Nunez thought, to understand how much informaiton we should share, and how we can standardize such sharing across industry. He strongly advocated that every enterprise stress-test its own environment. Insurance is now priced for black swan events, and Nunez suggested that this predeliction for black swans cannot continue.

More optimistically, Ghosh saw cyber insurance as an indicator of the industry's maturation. Underwriters will demand better controls and better reporting. "Insurance is driving a virtuous cycle. This raises everyone's game, and helps produce real results. So cyber insurance is a real positive for the industry."

CISOs have work to do before they're insurable. Insurance, Ghosh said, reduces security down to a number, which is something all boards understand, and that's the beauty of it. Nunez demurred—this requires continuous reporting from your baseline. How do we know (the board will ask) that our risk has been reduced? And that question is difficult to answer without testing your network. "You need to know your adversary, sure, but also your internal environment." This knowledge should be used to create sound scenarios for testing, and these will make people think about where the investment should go. Discussions of risk cannot occur in a vacuum.

Pell returned to his point that one must look at cyber risk as one does other operational risks: identify threats, vulnerabilities, and impact, then consider likelihood. He also noted that insurance is only one mode of risk management—there are other tools that may be more cost effective. Risk mitigation must be aligned with organizational goals and strategy. (And here, Pell noted, reputational risk is particularly important.) Key risk indicators differ for every organization. Insurance, Borgwing argued, should help you keep the business running.

"We've got a long way to go," Russell thought, "in terms of transparency. Reporting legislation will prove an important factor in understanding general risk." Some risks aren't going to be easy to transfer in this market. Russell warned that cyber insurance won't help much at all with risks to intellectual property, as much as IP is a common target for cyber espionage. Cyber insurance will help much more with regulatory risk.

Ghosh expressed the hope that "we'll transition form a time in which you're caned for having a breach to one in which you're disclosing it." Lamenting the punitive measures currently driving disclosure, he pointed out that more disclosure will make markets more efficient. He hopes for more attribution, for more disclosure of what threat actors did and what they're after. Russell saw signs for hope in the emergence of new tools for risk management. "When tools people get interested, you know you're getting somewhere." The emergence of tools for estimating value-at-risk is a very positive sign.

To questions about how one should handle the real-world aspects of actuarial data, and whether such data shouldn't drive insurance pricing, Ghosh replied that real-world intelligence about threat actors should certainly figure in risk profiles, along with an organization's mitigations of its threats. Borgwing noted that the markets can only bear so much, and right now what they can bear is about $500 million. Pell explained that life insurance is predictable because mortality itself is predictable. Cyber risk is, however, not yet predictable. Ghosh took the last work with an analogy between cyber security and end-of-life healthcare. "If security money were better spent, we'd minimize the black swan, expensive events."

Day 2

The SINET Showcase concluded with plenary sessions dealing with its themes of partnerhsip and innovation. The highlights, of course, the presentations by each of the SINET 16—start-ups recognized for their technology and their potential. The themes we heard were the importance of automating security as much as possible (particularly because of the shortage and expense of skilled labor, but also because of the need for increased speed and the ability

to scale), and the continuing effects of general migration to the cloud. We heard an consensus that cyber security was a species of risk management, that it was a business issue (and had to be understood as such), and that the ability to communicate about it as a business issue was crucial to any Chief Information Officer's success.

Jerry Archer, Senior Vice President and Chief Security Officer of Sallie Mae, opened the day's proceedings with his take on the familiar Cyber Risk Index: in Archer's view the Index suggests that we're not making progress against the adversary. "And so," he concluded immediately before introducing SINET Chairman and Founder Robert Rodriguez, "it's time for some true innovation."

Rodriguez himself reviewed the history of SINET, an organization founded to foster and directly contribute to public-private partnership for security. Entrepreneurs "are the heart of SINET" precisely because entrepreneurship is the sector's fount of innovation. (Calling them "vendors" he finds unfairly dismissive.) He described recent trips to Tel Aviv and London. In both he found a growing innovation ecosystem; in both he found government seeking to play a positive role in fostering entrepreneurship. He closed his introductory remarks by commending two challenges: we need faster innovation to get inside, and stay inside, the adversary's own innovation cycle. And in the United States there continues to be a strong need for Federal acquisition reform.

Keynote. Dr. Liz Sherwood-Randall, Deputy Secretary, US Department of Energy, delivered the conference's keynote. He described one of her Department's missions, and the one likely to be of greatest interest to the symposiasts: leading Federal efforts to enhance reliability, availability, security of energy. Cyber threats have dramatically raised the importance of cyber security innovation in this sector. After describing the broader threat environment, she reviewed Energy developed or sponsored cyber security products, and the National Laboratories' prominent role in transitioning these products to market. (Most of the technologies she reviewed concentrate on power grid security and resilience.) Public-private partnerships involving the National Laboratories have proven particularly strong. Sherwood-Randall believes cyber information sharing is still too slow, and she reviewed Department of Energy programs intended to remedy this. She closed with an invitation to engage the Department with questions, suggestions, and challenges.

The SINET 16 present. The Showcase's highpoint was, as always, the introduction of the SINET 16. Each member of the class of 2015 gave a six-minute presentation on themselves and their solutions. We describe them here in their order of presentation.

Bayshore Networks: context-aware protection for the industrial Internet-of-things. Bob Lam, Co-Founder and President of Bayshore Networks, delivered his company's presentation. Bayshore protects against industrial cyber attacks—examples of which, he noted, we've already seen. Bayshore's solution is not a conventional firewall. Rather, it offers a "cloud-based, patented IT/OT Gateway™ [that] enables organizations to rapidly build and enforce extremely granular content-aware policies for OT and IIoT cybersecurity, secure machine-to-machine communications, industrial operations/safety, and industrial automation."

The solution is both behavior- and policy-based, and its openness enables it to support a wide variety of systems. Lam closed by noting that Bayshore is proud to have CIsco as a go-to-market partner.

BehavioSec: recognizing the 21st Century operator's "fist." Olov Renberg, Chief Operating Officer and Co-Founder of BehavioSec, described his company's behavioral biometric solution. He set the approach in context: it isn't that new. Behavioral biometrics (like a Morse operator's fist) have been in use for a good century. But it's time to bring the approach from 1915 to 2015. BehavioSec applyies machine-learning algorithms to behavioral data (like keystroke patterns,

mouse movement, and so on) to identify the operators behind systems. The solution is context-independent and device agnostic. It's also proven to give a credible score. Transparent, dynamic, and adaptive, it has gained some fifteen million users worldwide, as it seeks to move consumers from being a security problem to becoming part of the security solution.

Lastline: easier to fake your look than your behavior (and that's how they'll catch you). Engin Kirda, Co-Founder and Chief Operating Officer of Lastline, began with a review of how motives have evolved in the course of the relatively short history of cyber attack: malicious hacking began in vandalism, moved into crime, and ultimately found its way into espionage and warfare. Lastline's approach to breach detection looks at behavior before attacks reach end users. (You can fake how you look, Kirda noted, but it's much tougher to fake how you act.) Lastline prides itself on its solution's flexibility, scalability, and correlation capabilities, which it sees as well-suited to detecting the incoming wave of increasingly complex targeted attacks. Their software is designed to integrate smoothly with existing security tools and operations. "Lastline is your last line of defense."

Netskope: cloud yes; fog and shadow no. Krishna Narayanaswamym, Netskope's Co-Founder and Chief Scientist, noted that the typical enterprise has over 750 apps in use. Of that total, around 90% are shadow IT, and most of that shadow IT is not enterprise ready. If you consider recent big data breaches, he argued, you'll find that cloud apps contributed either directly or indirectly to most of them. Netskope discovers cloud apps, assesses their risk, safely enables sanctioned apps, and then provides governance for all apps and the data they touch. The company's solution offers data loss prevention, surgical visibility of and control over cloud apps, and future-proofed architecture. "Netskope empowers organizations to direct usage, protect sensitive data and ensure compliance in real-time, on any device, for any cloud app."

Onapsis: attackers know what runs the US economy (but Onapsis knows the attackers). Onapsis Chief Executive Officer Mariano Nunez explained that his company saw SAP applications as presenting unaddressed vulnerabilities. SAP apps are pervasive, but they've been poorly served by security solutions. "SAP and Oracle apps run the US economy, and attackers know it," He said, and invited the conference to "think how a bad guy runs his business." The bad guy will look for a high-payoff attack. Consider case of USIS—the Chinese attackers who hit that company used an SAP-specific exploit to break in. Onapsis closes this gap in security coverage by offering a platform that automatically maps an enterprise's SAP deployment and continuously monitors activity on it to detect "advanced threats, cyber risks and compliance gaps."

Palerra: good security equals cloud security. Rohit Gupta, Palerra's Founder and Chief Executive Officer, described his company's approach to cloud security automation. "Good security now equals good cloud security," and Palerra delivers security management as a service. The company "helps enterprises obtain visibility into user activities, detect insider and external threats, and maintain compliance." Their solution also automates incident response, and extends security management that can cope with the growth and evolution of customers' data centers.

PFP Cybersecurity: you can't cheat physics. Steven Chen, Chief Executive Officer of PFP Cybersecurity, described PFP's Internet-of-things (IoT) security solution. The problem with the IoT is its detection gap, and that gap is getting worse as the IoT universe undergoes its own inflationary big bang. PFP's analogue monitoring solution can watch and inspect both legacy and new IoT systems, and detect anomalies in hardware or software from its analysis AC, DC and EMI signals. "PFP Cybersecurity adresses a digital problem with an analogue solution" that can be either built in or bolted on. Their approach is designed to meet the stringent requirements of simple IoT devices: "When there's only one chip, you have to be in the chip." Chen concluded by saying, "We're physics-based, and it's hard to cheat physics."

Pindrop Security: by their phoneprint shall you know them. Pindrop Security's Chief Executive Officer, Vijay Balasubramaniyan, began by saying that the phone is now the weakest link in security. Call centers have no good way of screening out fraudsters. They can't relaibly determine who or what are legitimate and who or what are not. This is important when you consider how stolen data are actually monetized. However the data were extracted in a breach, the final cash transfer that gives the thieves their payout usually takes place over the phone. Pindrop has stopped losses of up to $750,000. It does so through Phoneprinting™, which analyzes one hundred-forty-seven audio characteristics of a call to determine the specific device over which it's made, and the caller's specific location. "Every device has a distinctive acoustic signature, and we measure that."

Quintessence Labs: making breaches irrelevant. Mark Crowley, Quintessence Labs President, described how his company protects an enterprise against data breaches by overcoming obstacles to effective encryption. The usual reasons for not encrypting data are that doing so may not be legally required, is time consuming, and cannot be readily done in legacy systems. Quintessence makes it easy to encrypt data by offering centralized and interoperable key management, a high-speed true random number generator, one-time pad encryption with automatic key destruction for storage devices, and quantum key distribution. It delivers its solution in one hardened appliance that protects mobile data, cloud storage, databases, and file systems. The company's military, financial, and private cloud provider customers use Quintessence's solution to make the breach irrelevant.

RedOwl Analytics: protection against malice, compromise, and sloppiness. RedOwl Analytics' Chief Executive Officer Guy Filippelli talked about interactions and critical data sources. CISOs, he said, are concerned about what humans do with their devices, and so what CISOs ultimately want is visibility into human behavior. RedOwl's software platform exposes bad behavior and anomalies by tagging events, running statistics on metadata and content, and applying learning to the results. It takes data sources and delivers actionable information to key leaders. RedOwl built a tool that fits the analyst's workflow and thought process. Beginning with customers in financial services, RedOwl now has about twenty deployments across a variety of sectors. Their differentiator? Their focus on, and ability to handle, content.

Secure Islands: immunizing data against the consequences of loss. Yoel Knoll, Marketing Director of Secure Islands, described how his company protects and controls unstructured data. Most organizations still focus on perimeters and access points. But this no longer works, for a variety of reasons. "The story," he said, "is data." Secure Islands intercepts, inspects, classifies, and applies encryption to data. Thus, even the data should be lost, data so immunized is valueless to the data thief, whereas the authorized user can access and manipulate the data as necessary. Secure Islands' process is automated, but it can also incorporate user-driven classificatiom and user recommendations if doing so makes sense for the enterprise. He concluded by asserting that "data immunization makes the threat of data loss irrelevant."

SecurityScorecard: you can't know your risk until you know the risk third-parties bring with them. SecurityScorecard's Chief Executive Officer, Aleksandr Yampolskiy, reminded the audience that many of the big breaches they all know were in fact accomplished by supporting attacks on third parties. The old methods of assessing third-party risk—which range from ignoring it, to relying on subjective questionnaires, to using subjective questionnaires suppolemented by penetration testing—aren't adequate to today's threat environment. SecurityScorecard non-intrusively monitors the Internet for signals of danger, and then benchmarks companies from those signals. Results are fast, continuous, and non-intrusive, with scores calibrated on basis of quality of defenses. Because scores are meaningless without

actionable intelligence, SecurityScorecard delivers that, too, in an integrated Security Risk Benchmarking Platform that enables an enterprise to estimate its risk posture.

Sqrrl Data: a hunter, not a gate guard. Ely Kahn, Sqrrl Data's Co-Founder and Vice President, Business Development, described his company's big data technology. They focus on threat hunting. You need threat hunting because the old notion that you can put your enterprise inside a moated, walled, and locked perimeter is obsolete. A castle won't protect you, but roving patrols can. Even a SIEM-based approach is fatally reactive. Hunting, by contrast, focuses on continuous learning. Threat hunting uses linked data searches, behavioral analytics, and big data performance. Linked data includes extracted entities with their relationships, which enables those entities to be profiled. Threat hunting with linked data enables analysts to track down, investigate, and analyze data breaches associated with cyber-espionage, insider threats, and advanced attacks.

TaaSera: induction and deduction are fine, but to see the threat coming takes abduction. Srinvas Kumar, TaaSera's Founder and Chief Technology Officer, talked about how to see an attack in depth. His company's Preemptive Breach Detection uses abductive reasoning in its analytics engine to spot advanced,multistage attacks. It recognizes "patterns of malicious coordinated network and endpoint behaviors without the use of signatures or sandboxes." TaaSera's solution integrates an Active Risk Dashboard, forensic evidence, lateral evidence, preemptive action, and endpoint evidence into a comprehensive map of the "threat DNA."

Vectra Networks: the truth lies in the packets. Hitesh Sheth, President and Chief Executive Officer of Vectra Networks began by reviewing some recent high-profile breaches at big companies. Why, he asked, were these companies, all of whom were smart, alert, and well-resourced, successfully attacked? The cyber security gap lies here: "prevention-centric strategies are obsolete," yet they continue to consume most IT spending. The average time between infection and clean-up is six months, but you want to see the breach as it happens. Vectra's solution looks at the packets to extract behavioral signals, then presents contextualised results. "The truth lies in the packets." Vectra looks at packets in completely automated way, and correlates what it sees (also in a completely automated way). Correlation yields priorities. Vectra's goal is to be the friend of the security analyst, and its real-time detection of in-progress cyber attacks has now been installed by more than one-hundred-fifty customers.

Gurucul: identity-centric risk management. Gurucul's Chief Security and Strategy Officer Leslie Lambert explained how her company helps its customers detect insider fraud, IP theft, and external attacks. It does so by applying data science to user behavior analytics, addressing identity, access, and activity to recognize identity compromise or misuse. Users have accounts, and each account has entitlements. "Identity is the new threat plane," she said, "and that threat plane is real." Gurucul's solutions manage access (identity and access intelligence) and monitor use (user behavior anslytics). They handle these as data science problems, and their customers have found that approach effective across a range of use cases. "Data are dumb," she said, "but algorithms deliver value."

Online Identity Athentication: Trusted Transactions with Government and Across Government. Chaired by Terry Roberts (President and Founder of WhiteHawk Inc.), this panel included Gregory Crabb (CISO, US Postal Service), Janice Haith (CIO, US Department of the Navy), and Michael M. Johnson (CIO, US Department of Energy). The panel shared their general consensus that basic cyber hygiene, implementing cyber security best practices, and investing in cyber security research and development all figured prominently in their strategies. Johnson noted that remote access has become the default way in which employees access networks and do their work. This has pushed the evolution of security technology. He thought

that traditional two-factor authentication was reaching the end of its usefulness, and that other, mutlifactor, approaches to authentication were now of intense interest.

The US Department of the Navy, Haith explained, has both a business and a tactical environment. While the business environment uses industry standard technologies and practices, the afloat, tactical environment is the tough one—solutions that depend on access to big servers won't do. We're not, she said, seeing innovation fast enough in tactical environments. "So our challenge is taking care of our ships, ensuring they've got current capabilities in a disconnected environment. And DoD's biggest problem is our inability to rapidly insert technology into our systems."

Crabb gave an overview of the Postal Service's role in cyber security, taking pains to point out that replacement of compromised credit cards by mail was one easily overlooked example of that role. The Postal Service also has a significant role in federated identity pilots.

Summing up, Roberts implored the conference, "Come on, everyone: do something about passwords."

Mergers and Acquisitions in Cybersecurity: Case Studies. C. Bryce Benjamin (Principal, Alta Ventures, and Chairman, CipherPoint Software) chaired the conference's panel on mergers and acquisitions. The panelists include David Canellos (Senior Vice President, Emerging Business at Blue Coat Systems, and former President and Chief Executive Officer of Perspecsys), Maria Lewis Kussmaul (Founding Partner, Investment Banking, AGC Partners), and Tim Sullivan (VP Enterprise Forensics Group, FireEye, and former president of Fidelis).

The panelists began by offering some lessons for entrepreneurs looking toward an exit. Canellos advised that you can't neglect product in favor of things like sales and marketing. Sullivan described Fidelis's ten-year path to exit. When General Dynamics bought Fidelis, Fidelis was venture-funded. Kussmaul, who's advised on some seventy-six information security transactions, advised that domain expertise and a network of contacts are key VC capabilities. Sullivan pointed out that "Exit" is usually means an exit for the investors, but not for the entrepreneurs.

Benjamin asked how an entrepreneur knows it's the right time to exit. Canellos saw an advisor's explanation of options as valuable guidance for timing. In one of his experiences, inbound interest was the catalyst for considering exit options. Kussmaul expanded on this: well-positioned start-ups entertain significant inbound interest, because mergers and acquisitions are the ways innovation enters the industry. So assessing the quality of the inbound interest is crucial to deciding when to exit. Sometimes the advisor will tell you to wait, because competitive interest is the key to optimizing valuation.

Startups like Fidelis often go through more than one M&A event—Fidelis has seen two, and will in all probability see another. One of Sullivan's startups, Impulse, saw employees significantly enriched, largely because of the small preference stack. Canellos drew a lesson: listen to your advisors, and listen to your board, but remember that the CEO's role is to return shareholder value. Sullivan's takeaways were that timing is everything, and that entrepreneurs should remember that great companies are bought, not sold.

Thinking forward—hacking vehicles. Matt Rahman, Chief Strategy Officer and Executive Vice President of Field Operations as IOActive, considered the implications of the connected vehicle. IOActive was involved in the now famous Jeep-hack demonstration, so Rahman is well-placed to offer some thoughts on the challenges of automotive cyber security. Cars are now 90% electronically controlled by electronics, only 10% mechanically controlled. An ordinary Ford has more lines of code than an F-22 Raptor. Today's connected vehicle presents challenges principally with respect to safety and privacy, and all vehicles share the same technology and challenges. Once closed systems are now remotely accessible. He considered cases involving both physical access to a vehicle (through, say, a maintenance access dongle and attacks via wireless interface (as was demonstrated in the Jeep hack revealed at BlackHat

demo). Autonomous vehicles are being pushed hard by trucking industry, and the modern vehicle has an extensive attack surface. A car is now an IoT device, and the more it's connected, the more vulnerable it becomes.

The Present and Future of Federal Cybersecurity. This interesting panel was chaired by Richard A. Russell (former Senior National Intelligence Service Executive, now of the Russell Group) and comprised of Casey Coleman (Group Vice President Federal Systems Civilian Agencies, Unisys, and former Chief Information Officer, Federal Acqusition Service), Douglas McGovern (Chief Information Officer and Director, IT Services, National Geospatial Intelligence Agency),and Jill Singer (Vice President, National Security, AT&T Government Solutions). Its discussions lend themselves to a simple summary—automate good hygiene. The panelists approved the conference's emphasis on authentication, on data security, and on the value of the seamless and easy-to-use.

Administrative law: what happens when everything goes wrong. Michael J. Daugherty (CEO LabMD) wanted everyone to understand how Federal regulators actually work, and took the Federal Trade Commission as his case study. He was concerned with the potential for regulatory abuse: "Villainy wears many masks. None more dangerous than the mask of virtue." Tracing the origins of the regulatory state to President Wilson, he noted that Wilson's goals were in many respects admirable: non-political regulation by experts. But an unintended consequence of this approach was, Daugherty argued, an erosion of the separation of powers.

Medicine and technology, he said, have come to share a common burden: their regulators are not experts. Collaborative regulation is generally good (Daugherty didn't use this example, but NIST's "aggressively non-regulatory" approach to standards development might be an instance of such an approach), but punitive regulation, Daugherty argued, hasn't been bengin. Failure to consent leads to investigation, and if you insist on your day in court, you may find that day comes at a very steep price. Noting ways in which regulatory agencies often work contrary to the interests even of the rest of government, he concluded with a please to challenges such agencies in court.

Cybersecurity and the role of the board. Lisa Davis (Chief Executive Officer, Vicinage) chaired this panel, whose participants included Summer Fowler (Technical Director, Cybersecurity Risk and Resilience, Carnegie Mellon University), Jay Leek (Chief Information Security Officer, Blackstone), Christopher Hetner (Cybersecurity Lead, Technology Controls Panel, Office of Compliance Inspections and Examinations, US Securities and Exchange Commission), and Craig Rosen (Chief Security Officer, FireEye).

Davis opened by observing that cyber risk has brought very disparate communities together into effective collaboration in ways that other forms of risk have not. Fowler, noting the Carnegie Mellon CERT's long history in building and assessing capabilities, also noted that boards must invest for any solution to have effect. Hetner said that the securities industry is roughly a $60 trillion market, and the SEC wants to make that sector unattractive to hackers. Thus the SEC focuses on board-level support for cyber security. Without such support, resources expended on security are futile.

Remarking that he sits on various boards, Leek said that on those those boards he works to get the right CISOs in place, to put security into practice. In his capacity as a CISO, he recalled questions from a board member: Are we tracking attackers to see if we've seen them before? Who's attacking? Why are they attacking? Leek found this dialogue gratifying—it's good to see boards paying attention. Our challenge as CISOs is to participate in such dialogue in a form that's useful and accessible to the board.

"Boards," Rosen said, "want to know how big the cyber risk bubble is, and how to shrink it." His challenge to his own team, in preparing them to inform the board, is to ask them "so what?" To answer that question successfully is to accomplish the big communication task.

"You want the board to understand risk. Simplicity of message is important, but simplicity cannot compromise any underlying complexity."

Davis asked if the panel thought the boardroom now realized that cyber is a business risk, and not merely an IT issue. Fowler thought it did. "Now we need to work with the board to understand the risk appetite—what risk can we tolerate?" "The media have helped a ton," Leek said (words seldom uttered by CISOs, we think), "but they've created some problems, too," specifically by fostering the illusion that a final fix is possible.

The SEC has called dealing with cyber security a fiduciary responsibility, Davis noted, and asked Hetner to comment. It's important, Hetner answered, for the board and security to have a business dialogue. The CISO needs to understand the business, and needs to communicate the business implications of cyber risk to the board. The question,"Do we have it covered?" usually doesn't arise in, for example, a financial discussion. You want the cyber security discussion to be analogous to the financial discussion.

Risk appetite is one of the toughest things to discern, and constant communication is necessary to doing so. Risk appetite is indeed set continuously, but it must be set initially so it can be appropriately adjusted. The CISO should sit where the organization's structure and culture can best empower him or her to secure the enterprise. Hetner took the last word: "You've got to get intelligent about defining the risk universe." And your metric can't be removal of vulnerabilities.

Security as a Service (SaaS). The conference's final panel was chaired by Terry Halvorsen (Chief Information Officer, US Department of Defense) and included David Cass (Chief Information Security Officer, Cloud and SaaS Operational Services, IBM), Valmiki Mukherjee (Chairman, Cloud Security Alliance North Texas, and Chief Security Architect, Cognizant), and Myrna Soto (Corporate Senior Vice President and Global Chief Information Security Officer, Comcast). Halvorsen asked, "how much can an organization reasonably outsource its cyber security?" "A lot," Cass thought, "but it depends on the organization." He explained that IBM is looking at what the next-generation of security services would look like, what we do for rapid deployment of tools, and so on. Mukherjee thought that SaaS gave you the ability to do things you formerly couldn't, and Soto believed that SaaS gave a core advantage to a lot of companies. It will, and should continue to be, prevalent. "We look," Soto explained, "at what our investment would be if we did it ourselves, and what it would cost us to sustain and develop a capability over time."

So, to a question from the audience about what should be outsourced, and what should never be outsourced, Cass replied that you don't outsource your core competencies. Halvorsen summed up that outsourcing decisions come down to your business area, what core competencies you have, and what competencies you need against the threat. "And in DoD, I've got to look to automation," he concluded, to general agreement from the panel.

Robert Rodriguez closed the 2015 SINET Showcase's formal proceedings with thanks to speakers and participants, and, above all, with congratulations to the SINET 16.

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 11.17.15