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

CyberMaryland 2015

October 28 - 29, 2015 Baltimore, MD

Day 1

Opening

CyberMaryland's first day, understandably, opened with the state showcasing its cyber security ecosystem — a big (biggest?) Government cyber customer, university and Government research capabilities, corporate capability (from the biggest integrators to the youngest startups), a regulatory climate that aspires to be business-friendly, and a growing venture capital community. Maryland's Secretary of Commerce Michael Gill hit all of these points in his welcoming remarks, and he was substantially seconded by Representative Dutch Ruppersberger (D, MD-2) who followed him in the program.

Representative Ruppersberger spoke at somewhat greater length, expressing his pleasure that Congress and the President appear to have avoided budget sequestration. Moving to the topic of cyber security proper, he made a plea for better information sharing. "China steals billions from us annually. But the Intelligence Community can't warn companies because of a 1947 law." He thinks this needs to change, and believes information-sharing legislation is a vital issue, and a bipartisan one as well (he expressed his displeasure, surprisingly, with the White House threat to veto such a bill that passed the House earlier this year).

He thinks that checks and balances are working in the Intelligence Community, and particularly in NSA. (In an excursus on Edward Snowden, no hero in Ruppersberger's view, the Representative praised NSA without reservation.) He concluded by inviting all to consider Maryland the "cyber security capital of the world."

Resiliency and Regeneration

The morning keynote was delivered by NSA's Philip Quaid, Special Assistant to the Director for Cyber and Chief of the Agency's Cyber Task Force. He began with preliminary remarks on the importance of cyber education. Texas and Maryland, he observed, are tied at sixteen as national leaders in the number Cyber Security Centers of Academic Excellence they host. He praised innovation from universities like Johns Hopkins and the University of Maryland, tech incubators, and companies of all sizes. All, he said, merited support, and — not least through their commercial off-the-shelf products — they were providing invaluable support to vital missions.

After this pleasant and sincerely intended praise of the Maryland workforce, Quaid moved to his main point: NSA doesn't want to see foreign capabilities turned against US citizens. Nor, alluding to Snowden as others have today, did NSA want to turn its own capabilities to domestic targets. He reiterated NSA's long-standing position that it hadn't, and doesn't, break the laws under which it operates.

Turning to the threat, he warned of a coming wave of new, sophisticated state threats. China's cyber objectives are economic, specifically enhancement of its own industry through theft of expensively developed intellectual property, but, he added, there are disturbing signs that

China is also attempting to gain effective control over elements of US critical infrastructure. He agrees, however, with Director of National Intelligence Clapper that Russia remains the biggest threat to US security (and to the security of US allies, as evidenced by Russian cyber attack against Polish stock exchanges and German steel production facilities). Quaid sees NSA authorization to share information about what it's seeing in cyberspace as crucial. He also called for greater precision in our discussions of risk (a product of threat, vulnerability, and consequence), discussions which he regards as unhelpfully loose. In particular, he believes people tend to underplay the importance of consequence in the risk management equation. In general we need to improve our understanding of consequences. He closed with a call for active cyber defense, in essence a cooperative defense partnership. He called for resiliency and a capacity for network regeneration. And wherever possible, resiliency and regeneration should be automated.

Risk Management and Decision Support for C-Suites and Boardrooms

This panel on risk management, chaired by PivotPoint Risk Analytics CEO Julian Waits, included Spencer Wilcox (Director, Information Security, Managing Security Strategist, Exelon) and Lon A. Berk (Partner, Hunton and Williams). Waits opened by asking, rhetorically, why cyber security should be a board- and C-level issue. Consider, he offered, the case of the Target breach. A CIO was out, and, more strikingly, so was a successful CEO who'd been with the company for thirty years. As business continuity and an array of threats like ransomware have become major issues, security managers need to learn how to communicate with boards. How do you do that?

Wilcox explained that Exelon used a "TIRE" framework for communication: Threat, Impact, Response, and Expectations. They find this a useful way to frame discussion with the Board. This approach, coupled with an intelligence capability, helped them build credibility. Wilcox noted how specific risks were to particular business models, and stressed the importance of preparation for an incident, and in particular of not neglecting public relations in undertaking those preparations. And boards now understand, he added, that the SEC will hold companies accountable for following their declared security procedures.

Berk, in response to a question about cyber insurance, noted that "'cyber insurance' may be a misnomer. There are special products called 'cyber insurance,' but they're just part of a mix." Remember that cyber incidents have effects beyond cyberspace--physical damage, personal injury, and other losses. Some of those losses won't be covered by a "cyber insurance" policy. Actuarial data may be scarce, Berk observed, but it's really not that scarce — rather, it's closely held. Waits pointed out in closing that such information asymmetry means that the cyber insurance market is not yet a classically efficient market.

A Look at the Cyber Criminals' World from the Secret Service's Perspective

Stuart Tryon, US Secret Service Special Agent in Charge, Criminal Investigative Division, delivered the afternoon keynote. Some may be surprised by the Secret Service's role in investigating cyber crime, but Tryon noted that in fact this mission has its roots in the Service's earliest days, when in the 1860s it was tasked with fighting counterfeiting. The Secret Service works on cyber crime through Electronic Crime Task Forces (ECTF). The local Task Force meets quarterly in Baltimore, and it has its counterpart in numerous other cities.

Tryon described the Verizon Data Breach Summary and asked why sophisticated, well-defended companies continue to be breached. He sees a particular vulnerability arising from

what he called a general, ongoing war between companies' IT and marketing departments. The ECTFs are trying to broker a peace in that war.

He turned to trends the Secret Service is seeing among the criminals it investigates. Crime changes, but it continues to rise even as its attack modalities change. Attackers go after new and different things. Right now, Tryon said, "Lucrative data on corporate innovations is the wild, wild west." In particular, the acquisition or theft of such data serves market manipulation.

Criminals tend to shift away from targets as they become better protected. Hackers don't go after CEOs; they go after sysadmins. They want the sysadmins' credentials. Once they're inside, then they've gained real, legitimate access. "Hackers tell us, 'If I'm not successful, I don't get paid.'" Criminals have become not only persistent, but increasingly specialized, becoming experts, say, in attacks on one particular kind of system. And the specialization is likely to make the persistence pay.

Tryon closed with what has become a familiar invitation from Federal law enforcement agencies: he encouraged businesses to get to know, and to work closely with, their local Secret Service Field Office.

Cheap to store, but expensive to secure

A session on "Corporate Espionage and Insider Threats," moderated by Paul Rogers (Editor-in-Chief, Security Ledger) took up questions of "monitoring behavior, valuing data, quantifying risk and assigning accountability." Panelists included Gautam Aggarwal (CMO, Bay Dynamics), Casey Corcoran (Vice President of Strategy, FourV Systems), Gregg Smith (CEO, OptioLabs), and Leo Scanlon (Acting Director of IA Security, US Department of Health and Human Services).

Aggarwal, CMO, Bay Dynamics' Aggarwal reviewed what counted as an insider, and asked the audience to recognize that they no doubt have insiders whom they may not know. Risks are posed by both malicious and well-intentioned but misguided insiders. And malicious insiders come in at least two varieties: outsiders with stolen credentials, and true insiders who are intending their enterprise harm.

HHS's Scanlon stressed the importance of the basics: identifying assets, and identifying legitimate behavior. You have to begin with policy, with separation of duties. "Data are cheap to store, but expensive to secure." This paradox affects our ability to deal with espionage.

FourV Systems' Corcoran observed (to general agreement) that it's easier to recognize risky behavior than to have complete, well-structured systems of data. OptioLabs' Gregg Smith noted that BYOD has made it essentially impossible to control where your data are. (He also said his product would have caught Edward Snowden; we're going to ask him about that tomorrow.) The panel saw a trend away from BYOD ('very chic-y" as it's been) and back to enterprise-owned devices.

The panel concluded by observing that we tend to conflate very different things in our assessment of risk. Consider the difference between losing an easily replaced paycard and losing hundreds of millions worth of research invested in drug development.

Day 2

CyberMaryland 2015's second and final day featured presentations by, and discussions with, innovators in the field of cyber security. We were able to speak at length with five of those innovators. But the day opened with the launch of LifeJourney's and NSA's Day of Cyber educational initiative.

Educating a Cyber Generation

Dr. Freeman Hrabowsky, President, UMBC, opened the proceedings with his morning keynote on the 21st century cyber curriculum. "There's now a global struggle in an entirely manmade 5th dimension," he began, and argued that this struggle would dominate the current century. He suggested we think of cyber security as we now think of auditing — something that's not confined merely to the experts, but something everyone in an enterprise has a stake in.

Developing a curriculum to meet the needs of this century will require considering hitherto unknown possibilities, and doing so will itself require a cultural change. Hrabowsky spoke to what he saw as the necessity of redesigning the educational experience itself. With respect to cyber security education, he argued that we need to, first, change how people are introduced to cyber, second, add new pathways into cyber careers, and third, strengthen partnerships. Soft skills, particularly those related to communication, cannot be neglected here, and transforming the curriculum must include pre-college education.

K-12 programs with a cyber focus are a promising place to begin, and we might begin by recognizing that rigidly tracking young people into or out of STEM fields is a dangerously misguided mindset. Thus he closed with a call to teach anyone anything they're prepared to learn, and not to discourage them, or write their abilities off.

With the keynote concluded, LifeJourney and the National Security Agency launched their "Day of Cyber," a free, web-based, interactive experience available to students, teachers, schools, and organizations throughout the United States.

Interviews with Innovators

The CyberWire had the opportunity to talk with five companies on the second day of the conference. We were struck by the ways in which they approached anomaly detection, by their realistic conception of what counted as actionable intelligence, their focus on support for rapid recovery and remediation, and the way in which they've thought through the implications their offerings have for customers' risk management.

Scoring Risk and Scoring Performance (FourV Systems)

We caught up with FourV Systems' Vice President of Strategy Casey Corcoran after hearing his contributions to Wednesday's panel on "Corporate Strategy and Insider Threat." He gave us an overview of the company's history and technology.

FourV's Greyspark Reasoning Engine is an answer to the challenge of measuring the threat level on the basis of what an enterprise sees in its networks. A machine-learning, big-data platform, Greyspark takes the session data (typically already being collected and reported to a SIEM) from a network and runs them through a machine-learning engine to arrive at a picture of overall risk. FourV's original vision was to use its technology for business risk management ("we wanted to end the use of spreadsheets for business management") but prospective customers liked the cyber security aspects of FourV's demo, which was a "hackability index." So the company now offers a security performance metric in terms of key performance indicators.

FourV looks for behavior, not signatures. "Chasing signatures is a losing game, because they go out of date so rapidly," Corcoran said. "More significantly, they don't give you a picture of the overall risk posture." Overall behavior should generate an overall risk score. " Our risk score is residual risk. That is, a product of threat, vulnerability, and consequence, minus mitigated vulnerabilities."

The case for FourV's solution is the CISO's need for credible metrics. CISOs need to know how their team is performing and where to put their resources. So FourV not only gives a risk score,

but attaches a dollar value to it. Once they know that, CISOs can calculate security return-on-investment and make an informed risk management decision. "You can avoid, mitigate, transfer, or accept risk." The dollar value attached to the score informs this decision.

Corcoran thinks actuarial data overrated in many discussions of risk management. Considering, for example, how retailers manage the risk of loss through "shrinkage" (shoplifting, pilferage, etc.) "retailers don't use actuarial data either." The old, familiar metrics are good predictors: footfall, items in basket, size of basket, and so on.

FourV's approach uses no modeling. It is, Corcoran stressed, completely statistical. They use six subindices: defense effectiveness, technical debt, total surface area, length of score history (do we have enough data for confidence?), opportunity risk (how severe and how likely are the events we're seeing?), and the appearance of novel risks.

They develop a background of normal activity against which anomalies may be recognized and assessed. FourV collects data every ten minutes, not on an audit basis, and their goal is to move to a continuous monitoring capability.

Recognizing the Face in Front of the Screen (OptioLabs)

Also participating in the "Corporate Espionage and Insider Threat" panel was Gregg Smith, CEO of OptioLabs, Inc. We wanted to hear more from him about his claim that OptioLabs' technology would have caught and stopped Edward Snowden.

Optio was founded in 2012 to bring to market technology developed at Virginia Tech (the company maintains a close relationship with researchers at Virginia Tech, and also at Vanderbilt and the University of Maryland Baltimore County). The researchers were responding to a DARPA challenge: how do we let senior officials walk into a SCIF without having to leave their devices in a box outside? The company's initial technology, then, was a capability to lock down an Android device.

"Think of the Android binder as its post office," Smith explained. "Any app has to flow through the binder.' Optio's technology is built around the binder to selectively lock down functions. That lockdown can be significantly context aware (geolocation and temporal contexts are easiest to discuss, but these don't exhaust the system's contextual awareness). They're currently working on automating policies for devices used in regulated sectors. "We're going to make market-specific policies. For example, HIPAA compliance would become a check box on a server."

Smith described two of the company's products, PrivateEye and Chameleon. PrivateEye leverages a device's camera to provide continuous authentication that the current user is in fact the authorized, authenticated user. "It protects the last two feet" against visual hacking and physical loss. The system ties into credentials — stolen or borrowed credentials won't match the face in front of the screen (and this, explained Smith, is how the technology would have quickly flagged Snowden's romp through the enterprise). PrivateEye uses facial recognition as its biometric modality, and it features "continually updated facial learning" to account for slow changes over time in a user's visage.

The sister product, Chameleon, is intended as protection against visual hacking — the deliberate or inadvertent look an unauthorized person might take at a screen. The system uses a gaze-tracker and can obscure a screen or display a bogus screen to anyone other than the authenticated user working at the device.

Asked about the downsides of using device cameras for security systems, Smith noted that one obvious downside is the tendency of many government organizations to exclude, as a matter of

policy, cameras from their spaces. But this, he said, is changing, and cameras are returning to many of those workplaces. And of course, he added, OptioLabs recommends a suite of security measures to protect the cameras themselves.

OptioLabs also anticipates an Internet-of-things role for its Android technology — they're working on extending their work to "Brillo," Android's IoT operating system. Smith sees considerable potential in this market.

Removing Network Blind Spots (Damballa)

The problem Damballa sets out to solve, according to Stephen Newman, Vice President, Product and Strategy, is the rapid identification of compromised systems. "We're a network security monitoring solution."

Newman distinguished Damballa's solution from signature-based approaches. The company studies the behavior of devices over time ("and no single event is behavior" in this sense) and builds machine-learning models to reveal, with statistical significance, how a compromised system behaves. One might try to aggregate logs and pull signal from noise to achieve this result, but that, Newman said, would be "overwhelming." Instead, one might profile how a device is communicating to recognize a compromise.

It's difficult to apply machine learning to an enterprise network, Newman said. The typical approach people take is to build a machine-learning capability inside a customer network. Rather than do this, Damballa brings its models into the network. Their solution used two layers of analytics. The first layer looks for statistical similarities to models of compromised systems. "This level is aggressive." It picks the centroid as its statistical model, then brings that model into the customer network. (Eight detection techniques are used to develop the models.) The second layer takes the analytics from the first and uses them to "build a case," thereby significantly reducing the false positives the aggressive first layer would otherwise generate. They're not looking for malware; rather, they're looking for compromised machines.

In risk management, he recommended that people think about their risk from a disaster recovery perspective. "What's of more risk to you? An attack that's blocked, or one that's successful and unrecognized? Clearly the second." Quick recognition of compromised systems should trigger recovery, and timeliness comes from continual checking.

As it works to reduce blind spots, Damballa doesn't work from logs. "We work from a notion of studying the behavior of a device over time. This both develops and sharpens the signal." Newman compares this to criminal investigations. When police investigate a crime, "they don't bring in Sherlock Holmes; they bring in a team." That team assembles evidence into a case. This is essentially what Damballa does: it sees a case, and investigates it for compelling evidence of compromise. The case analyzer looks at an event, considering threat intelligence (including information on threat actors and their infrastructure), content inspection (examining the content of communications between device and destination), and behavior (especially indicators of either automated or evasive behavior). Sometimes it concludes there's no compromise at all.

Damballa's customers include financial companies, universities, oil and gas companies, chip foundries, and media companies. Newman closed our talk by distinguishing Damballa' approach from some others common in the industry: "We're not focused on the malware. We're focused on the behavior."

Endpoint Security for Resilience and Regeneration (Triumfant)

On threat intelligence, at least when it comes to the panel he sat on earlier in the day, Triumfant's President and CEO John Prisco described himself as a contrarian, but he thinks

more people are considering moving over to his side. "Now, people are starting to realize that the endpoint is important. A majority of attacks are now engineered for their targets, and so many of them don't appear in threat intelligence databases. Threat intelligence is a solution, but it's not one that stands alone." New attacks take from a week to three weeks to find their way into threat intelligence databases, and that, of course, is slower than one would want. He sees a similar limitation in schemes for sharing threat intelligence: "You can't do it fast enough. CISA will be obsolete by the time it's passed."

There's a place for this kind of intelligence, Prisco said, particularly in prediction and attribution, but attribution is not important to his customers. Triumfant detects anomalies on its customers' endpoints. "People aren't terribly well suited to diagnose computer problems." It's particularly hard for them to figure out the extent of an infection. Triumfant automates the diagnostic process, and then presents the results to incident responders. It also provides remediation, and this remediation can be automated.

The company benefited greatly, Prisco said, from its four years of pilots at NSA, and its solution is consistent with the Agency's goal of regeneration Philip Quaid described in the previous day's morning keynote. Prisco noted that Triumfant's ability to detect in-memory attacks, and volatile attacks that only instantiate in trusted, running processes, is a distinctive feature of its solution. The company holds six US patents on its algorithms, including donor technology that finds and clones uncorrupted files automatically.

Triumfant uses an agent (available for Linux, Mac, and Windows devices) that scans constantly, collecting machine attributes and creating adaptive reference points. A fast scan runs every thirty seconds to collect a subset of data, looking for indicators to trigger a more complete scan. The solution baselines endpoints by taking machine outputs, digesting them into a database, using a pattern-matching algorithm to compare endpoints within an enterprise. A new adaptive reference model is generated every seven days.

So, while threat intelligence must be part of an overall security approach, with network protections and sandboxing, "on the endpoint, we are the solution," Prisco said. Many of Triumfant's customers are media companies who came to them after the company found the October 2011 attack on the New York Times.

Looking to the future, Prisco said that Triumfant is exploring automated whitelisting, "intelligence whitelisting," which he sees as holding promise for improved prevention. "For this to work on the endpoint, you've got to automate patching." We'd also like to add the ability to rapidly answer customers' questions about the security of their enterprise.

What one kind of actionable intelligence looks like (Terbium Labs)

Founded in October 2013 by alumni of the Johns Hopkins University Applied Physics Lab, Terbium focuses on bringing privacy and automation to data intelligence in actionable, useful ways.

Matchlight is Terbium Labs' flagship data intelligence platform, and Terbium CEO Danny Rogers explained how that platform generates intelligence that's clearly actionable. Matchlight is a fully automated Dark Web scouring solution: it finds stolen data in a fully private way.

Terbium's approach is data fingerprinting. A proprietary data-hashing algorithm enables Terbium to search for customer data on the Dark Web without the need (or ability) to read the data. Thus no trust is required. The solution also doesn't increase the customer's attack surface: the only part of it that exists on the customer side is the fingerprinting algorithm, with the hashes uploaded to Terbium through an API.

The crawling, collection, and comparison Terbium does is accomplished through proprietary big data technology. The kinds of data fingerprinted for searching might include customer records, employee records, payment information, or proprietary code. Matchlight offers monitoring, data feeds, and retrospective private search.

Asked about the Dark Web, Rogers explained that this is often taken to mean simply the anonymous Internet, included such precincts as the morally neutral TOR. "But the Dark Web isn't just TOR. The criminal parts of the Internet are actually a pretty small fraction of the whole, but they're far from insignificant, and it's too expensive to have human beings keep up with them." Stolen data are likely to turn up in the Dark Web, which is why Terbium searches it.

Rogers said Terbium's approach to finding stolen data differs from the fraud detection conducted by, for example, the pay card industry, because such fraud detection operates at the transaction level, and therefore lags. Dark Web search offers quicker detection of data exfiltration. Their results are actionable because of the timeliness Terbium's continuous monitoring provides. A card issuer, to take one use case, would warned within thirty seconds to fifteen minutes of data appearing on the Dark Web. And once warned, the customer can then do what makes sense from a data-risk management perspective.

Rogers stressed that Matchlight isn't an encryption solution. Its data fingerprinting enables private querying of a database without the need to actually see the data. This is a one-way protocol that enables private queries of sensitive data. "Banks like that," he concluded.

Breakout Sessions and Panels

We were able to attend several of the second day's breakout sessions. Here's what we heard.

The Cyber Defense Toolbox

Dr. Avi Rubin, Professor of Computer Science and Technical Director of the Information Security Institute, the Johns Hopkins University, moderated this panel. Panelists included Robert Lord (Co-Founder, Protenus), Andre McGregor (Director, Cyber Security, Tanium, and former FBI Cyber Special Agent), John Pirc (Chief Strategy Officer, Bricata LLC), Dr. Anuja Sonalker (VP Engineering & Operations, North America, TowerSec Automotive Cyber Security), and Dr. Daniel J. Rogers (CEO, Terbium Labs).

The panelists gave short presentations on their company and the challenges their products solve.

Protenus's Lord argued that "We need to bring trust and transparency back to health care." Since 2010, healthcare breaches have doubled, driven by a criminal market for fraud and identity theft. He noted that electronic medical records sell for around $1000. 70% of hospital breaches are caused by the hospitals' own employees, affecting their reputation for trustworthiness — even "benign snooping" can cost millions. Only about a third of hospitals, Lord said, are equipped to handle breaches, and he thinks fully half of all hospitals are "delusional" with respect to security. Protenus stitches data with an access logo, analyze for anomalies or variations, and generate an automated report. Its customers include the Johns Hopkins Hospital, INOVA, other hospitals.

Tanium considers itself a self-aware whitehat botnet. McGregor claimed his company can provide 100% visibility of all endpoints in less than fifteen seconds. They do this live, without building a huge database, and prompt immediate incident response without significant investment in human labor — the traditional and prohibitively expensive approach. Their customers include Target ("post-breach," he clarified), Visa, and Amazon, and their services include patch management and incident response.

Saying "visibility is everything," Bricata's Pirc described his company's solution as a next-generation intrusion prevention system (NGIPS), distinguishing it from a next-generation firewall. It incorporates over twenty-eight-thousand signatures and performs file based detection with over one million MD5 checksums. Its sensors are spread out across an architecture with a threat isolation engine and multiple analyzers. He described it as the fastest NGIPS and packet capture system on the market.

Sonalker described TowerSEC, a vehicle protection startup founded in 2013. Cars now present, with increased connectivity, entertainment features, and so on, "a modern connected attack surface" ill-equipped to handle attacks, and the fact that cars have been shown to be hackable is, to say the least, "disturbing." Typical attacks include telematic compromise, sensor input compromise, and loss of critical control. A layered security approach, Sonalker explained, is essential, and should include vulnerability management, Intrusion detection and prevention, security by design, and routine penetration testing.

Daniel J. Rogers, of Terbium, pointed out that on average breach discovery takes more than two hundred days, and that over eighty percent of breaches are discovered by some third party. No enterprise is happy with this situation. So how can a company recognize that it's been breached before hearing about it from someone else? Terbium's Matchlight provides data fingerprinting for private search, a Dark Web crawler, and automated alerts. The system's key innovation is a search capability for sensitive information.

Rubin asked the panel what they viewed as the biggest technical challenge in cyber defense. Lord thought it was accessing highly sensitive data, even with the purpose of protecting it (and that this is also a political challenge). McGregor's thought the challenge lay in responding to the increase in the IoT, and related phenomena that introduce size and complexity to attack surfaces. Pirc chose managing storage and keeping up with the relevant and important; Sonalker thought the absence of global standards and the resultant need to customize security solutions. Rogers saw the big challenge as big data.

Rubin then asked the panelists what would improve or hurt cyber security in their areas of interest. Rogers thought technologies that could handle large data volumes would help, and that the black market for stolen data (and the "perpetual game of cat and mouse" that comes with it) would (and does) hurt. Sonalker again advocated global standards for automotive cyber security, and acknowledged with regret that these seemed unlikely to emerge. McGregor (without going full-Luddite) concentrated on the hurt: mobile devices hurt — everything is on people's mobiles, and this creates a very wide threat landscape. Lord believed improvements in data analytics would be positive, and that disruption of hospitals medical records is a significant potential threat.

Not Just Tech: Why Greater Emphasis on the Law and Policy of Cybersecurity is Critical

Michael Greenberger, Professor, University of Maryland Francis King Carey School of Law, and Founder and Director, University of Maryland Center for Health and Homeland Security, moderated this panel. Panelists included Dan Caprio (Co-Founder and Chairman, The Providence Group), Jonathan Litchman (Co-Founder and CEO, The Providence Group), Markus Rauschecker (Senior Law and Policy Analyst, University of Maryland Center for Health and Homeland Security), and Mark Cather (Chief Information Security Officer, University of Maryland Baltimore County).

"Why," Greenberger asked, "should there be greater emphasis on legal policy in cybersecurity?" Rauschecker took the question. "We've come a long way in recognizing law and policy in cybersecurity — before, people just let IT take care of everything. Now, we

recognize this is no longer an IT issue, and that everyone has a role to play in cybersecurity, from the CEO to the newest hire." It's an "interdisciplinary problem." There's a practical benefit to having everyone know policy because it helps them adapt their cybersecurity strategy and adhere to laws, but there's also a "knowledge gap" here: We don't know enough about the legal and policy ramifications of our cybersecurity actions.

Lichtman noted that, when we look at risks and business decisions, we need consistency in our strategies. Cyber security sometimes suffers from conflicting laws and policies. Instead of a unified policy for cyber security, we see a patchwork of organizations and regulatory bodies creating varied policies, and we also see ever-changing torts in ever-changing courts. This situation makes companies unsure, and uncertainty affects strategy, general counsel, personnel, procurement, and so on.

"Risk," Caprio said, "drives the need for law and policy." We need to build a framework to manage risk. Policy drives where a cyber security organization deploys its resources. This need has become sharper as critical data have been pushed into infrastructure (thereby building risk), as people bought tools without understanding them, and as the introduction of the cloud and multiple devices have continued to spread data widely.

Greenberger sought the panel's opinions on holding companies liable for cybersecurity breaches, and for their impressions of CISA's probable effect on policy. Lichtman saw a shift in presumption of liability toward business whose data have been exposed. Such liability has made businesses more sensitive to the financial and reputational risks of negligence. Rauschecker added that people whose identities were exposed by their employers formerly lacked standing because they couldn't prove harm, but now the Seventh Circuit has found substantial risk of harm from such breaches, and companies now must show they're doing everything they reasonably can to protect their data. But given that there's no general standard for information protection, demonstrating such care is difficult.

Cather saw liability as putting the focus on the need to have your house in order — you need to follow all standards and frameworks. It motivates companies to secure their infrastructure, and laws help prove and show both responsibility and due diligence.

Shedding Light on the Dark Side of the Insider Threat

Larry Letow, President/CEO, Convergence Technology Consulting, moderated this panel. The panelists were Jim Mazotas (CEO, OnGuard Technologies), Tom Glaser (Vice President for Information Technology, Howard Community College), and Jeff Six (Vice President, T. Rowe Price).

Letow began with the observation that insider threats can be an order of magnitude more destructive than outside attacks because the insider is so familiar with the company. Given that, he invited the panel to give their views on the importance of knowing the insider threat. Six acknowledged that exposure to insider threats was growing even as the nature of technology and how businesses use it is changing. Outsourcing has increased the number of people from different backgrounds who are exposed to a company's inner workings. And insiders, he reminded the audience, can be tricked or exploited without being themselves malicious. Glaser argued that even part-time and casual staff must be trained and managed. Carelessness is always an issue — he offered as an example the many students who have just one password that unlocks all their information. Mazotas thought there was lots of confusion about what an insider threat was. The complexity of products and mobile devices creates a world of unintended consequences. This threatscape changes constantly, and it's hard to make policies and processes that can navigate its complexity. Six thought the biggest current insider

threat was susceptibility to phishing ("very simple and easy to do"). Phishing makes unaware employees — people without malicious intent, but who are just unfamiliar with technology and its risks — into insider threats.

What, Letow asked, of data governance? Glaser advocated a base standard of entrance for everyone. Different levels of people allowed different amounts of access based on security requirements, and people should be kept informed of different levels of access. Data governance, Six thought, shouldn't be driven by technology, but by people. "It's very compliance-driven — more of a business process." Getting access levels right is essential for protection against insider threats. Nor should marketing be left out of the conversation.

Building Your Light House: Cyber Risk Intelligence in Your Risk Management Program

Adam Meyer, Chief Security Strategist, SurfWatch Lab, spoke about a role for threat intelligence in cyber security. "There is," he began, " a technology component everywhere." We are, however, spending more to achieve the same outcome, which suggests we're applying our resources in the wrong places. So, how can we defend ourselves properly if we don't know what our risks are?

Brands suffer after cyber breaches and need threat intelligence to change poor outcomes. They need to "change unknown unknowns into known knowns."

Meyer divided threat intelligence platforms into three categories: strategic platforms for general executive use, operational platforms for IT and security executives, and tactical platforms for incident response teams.

Every company has a different threat threshold, and every company needs to know and analyze that threshold. Intelligence gives situational awareness. (And his examples were retrospective: How were they breached? What was the outcome of the breach?)

He closed with another military metaphor: threat intelligence should look at the "avenue of approach."

The National Cyber Security Hall of Fame, Class of 2015

After the conference wrapped up many of its participants reconvened for the induction of the National Cyber Security Hall of Fame's Class of 2015. The ceremonies were highlighted by Facebook Chief Security Officer Alex Stamos, who addressed the impact of the recent voiding of the US-EU Safe Harbor framework. He characterized this as evidence of a loss of trust, a loss he thought both misguided and avoidable, founded largely on international misunderstanding of the realities of the relationship between US tech companies and the US Government. He made a strong case for data privacy, and for the widespread adoption of strong encryption (without backdoors).

The Class of 2015 was recognized, with each inductee offering brief, gracious, and informative remarks as they accepted. Here are the newest members of the Hall, with their official profiles:

Cynthia E Irvine, Distinguished Professor of Computer Science at Naval Postgraduate School. "Cynthia E. Irvine is a Distinguished Professor of Computer Science at the Naval Postgraduate School. Her research has focused on developmental security as applied to the creation of trustworthy systems, and more recently, on cyber operations. She is a champion of cyber security instruction designed to ensure that the foundational concepts of constructive cyber security are integrated into academic courses and curricula. Through curriculum development, educational tools, the supervision of student research, and her professional activities, Dr. Irvine is a true leader in cyber security education."

Jerome H. Saltzer, Professor Emeritus of Computer Science Massachusetts Institute of Technology. "Jerome H. Saltzer has been a faculty member at MIT since 1966, where his teaching and research interests have been about principles of computer system engineering. His involvement in cyber security began with the discovery in 1964 that it was surprisingly easy to break into the MIT Compatible Time-Sharing System. He helped design the security aspects of the Multics time-sharing system and he led the development of a security kernel for Multics; later he led the development of the Kerberos single-login authentication system. His paper with Michael D. Schroeder 'The Protection of Information in Computer Systems' collected a set of security principles that have been widely cited for four decades."

Ron Ross, Fellow, National Institute of Standards and Technology. "Ron Ross is considered the 'Father' of the Federal Information Security Management Act (FISMA) security standards and recognized as one of the world's leading experts on cyber security. He is the principal architect of the NIST Risk Management Framework and led the development of the first set of unified cyber security standards for the federal government, including the Department of Defense and the Intelligence Community. Dr. Ross has received the NSA Scientific Achievement Award, Defense Superior Service Medal, Department of Commerce Gold and Silver Medals, and three Federal 100 Awards. He has been inducted into the Information Systems Security Association (ISSA) Hall of Fame and is an ISSA Distinguished Fellow."

Steven B. Lipner, Director of Software Security in Trustworthy Computing Security at Microsoft (Retired). "Steven B. Lipner is recently retired as the Partner Director of Software Security in Trustworthy Computing Security at Microsoft and serves as a board member and chair of SAFECode. He led Microsoft's Security Development Lifecycle team and was responsible for its corporate strategies and policies for supply chain security and for strategies related to government security evaluation of Microsoft products. He is named as an inventor on 12 U.S. patents with two pending applications in the field of computer and network security, and is co-author of the book, The Security Development Lifecycle."

Susan Landau, Professor of Cybersecurity Policy at Worcester Polytechnic Institute. "Susan Landau has been a twenty-year leader in the 'Crypto Wars.' Her books, Privacy on the Line: The Politics of Wiretapping and Encryption, co-authored with Whitfield Diffie, and Surveillance or Security? The Risks Posed by New Wiretapping Technologies, testimony in Congress, and technical and policy research have helped ensure the widespread availability of strong encryption. Landau has been a long-term advocate for NIST's Computer Security Lab, including during her tenure on the Information Security and Privacy Advisory Board. She is a strong advocate for women in computer science, and has organized workshops for women students and young faculty. Landau is Professor of Cybersecurity Policy at Worcester Polytechnic Institute, and has previously been a Senior Staff Privacy Analyst at Google and a Distinguished Engineer at Sun Microsystems."

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