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

Cyber Maryland 2013

October 8-11, 2013 Baltimore, MD

October 8

CyberMaryland opened today, and the CyberWire will be reporting the proceedings live. The conference opened with a keynote on the past, present, and future of cyber security, followed by sessions on the business and governance of cyber, cyber technology and innovation, and training and educating cyber professionals. We'll provide a full summary of the day's events in tomorrow's issue of the CyberWire. In the meantime, follow the conference with us on Twitter @thecyberwire.

October 10

Among many interesting sessions and presentations, we will be highlighting two likely to be of interest to our readers. And, of course, we finish with an account of the National Cyber Security Hall of Fame induction ceremony for the class of 2013. We'll wrap up our CyberMaryland coverage in tomorrow's issue.

Building an Effective Cyber Risk Culture

Mark Gilbert of COPT moderated presentations on cyber risk culture and the forces shaping the cyber insurance market, which, he noted, represents the fastest-growing insurance sector.

Tom Finan (Sr. Cybersecurity Strategist and Counsel, US Department of Homeland Security (DHS) National Protection and Programs Directorate (NPPD)) spoke of the state of the developing cyber insurance market.

NPPD is responsible for assisting federal civilian agencies with securing themselves against cyber attack. Its vision is a safe and resilient infrastructure, which, Finan explained, means looking ahead at emerging threats. In this context, DHS leaders asked for a look at cyber insurance market.

Such insurance can be expensive and hard to get. We might usefully compare it with fire insurance, for which there is a well established and functioning market. Taking protective measures—putting in sprinkler systems, etc.—is a prerequisite for obtaining fire insurance. There might well be a cyber-insurance parallel, not only in terms of opening availability but also in terms of establishing a market that drives increased security (and security innovation).

There's currently a reasonably functional cyber insurance third-party market that benefits from a sizable actuarial data set. The real problem lies in the first-party market—a market for insuring against loss of reputation, loss of market, and the restoration of systems. Here, there's very little actuarial data because companies are understandably reluctant to disclose cyber attacks and the complex losses they inflict.

According to Finan, the NPPD thinks that an appropriate role for the DHS is to sponsor conversations with a cross-section of stakeholder groups. As we studied the problem and talked with stakeholders, we identified two unresolved issues: assignment and market.

With respect to risk assignment, stakeholders differed. Many felt risk should be assigned to the federal government. Others thought assignment of risk to utilities (for example) provided

© 2015 The CyberWire

a model by which risk might be assigned to the private sector. The new and rapid growth of cloud services raised significant risk-assignment issues. Active defense has also become a factor in assignment: many companies are interested in extending their self-defense rights to cyberspace.

The market issues naturally fall into supply- and demand-side categories. On the supply side, many see a role for the federal government in developing actuarial data. On the demand side, many wanted a cyber version of the SAFETY Act. They want a safe space for companies to report what's happening to them, and the ability for them to do so anonymously. Many asked for a set of well-founded risk-reduction best practices.

The business case for insuring (and investing) against cyber risk has, generally, yet to be made. In many sectors, cyber risk is still considered a purely IT issue, and it hasn't been reduced to costs that business leaders can understand. More research into costs and benefits of cyber risk would surely help.

Risk management strategy falls naturally into four stages: accept, avoid, mitigate risk, and, only then, transfer it (through insurance).

We see, according to Finan, a movement on the part of insurance carriers away from elaborate checklists to an assessment of a company's risk culture. Some carriers now essentially rely entirely on risk culture to craft a policy specific to each business that is seeking insurance. Risk culture is seen as having four pillars: (1) the role of executive leadership, (2) education and awareness, (3) technology, and (4) information-sharing.

Insurers now generally survey companies with 20 or so high-level questions, and they do this "to eliminate the clueless from their pool of the potentially insured." Carriers want to see an engaged cyber risk culture, and companies with such cultures are the ones that they want to insure. This is a very positive sign: the process of companies getting their own houses in order will ultimately drive an effective first-party insurance market.

Dismas Locaria (Partner, Venable LLP) spoke about the SAFETY Act, which is intended to encourage innovation through systems of risk and litigation management. This law arguably already covers cyber as a special case within its definition of "act of terrorism."

The SAFETY Act establishes a process that helps companies limit their liability at two levels: (1) designation (which requires demonstration of a product, system, or technology's efficacy) and (2) certification (which requires a higher degree of proof of efficacy). Designation caps liability at a certain level; certification affords effective immunity from 3rd party liability.

The act also affords a company with government review and the approval that what it does is effective and constitutes a reasonable precaution against risk. The application process is very involved, requiring a lot of upfront work.

A questioner asked whether hacktivism fell within the scope of the SAFETY Act. Locaria replied that this was a grey area and that it is ultimately the Secretary of the Department of Homeland Security who determines whether or not an act constitutes terrorism. He did note, however, that the language of the bill mentions eco-terrorism, which is surely akin to hacktivism.

Cyber Technology and Innovation: What's here, what's coming, and what to do about it.

Beau Adkins, CEO of Light Point Security, moderated a panel of industry leaders: John Harmon (Partner, Tactical Network Solutions), Jeff Huegel (Executive Director, Cloud, Hosting and Applications Security, AT&T), Jason Taule (Chief Security and Privacy Officer, FEI Systems), and Dana Pickett (CISO and CPO, Allegis Group). Adkins invited the panelists to share their take on the cyber landscape.

Tactical Network Solutions' Harmon explained that embedded devices on networks pose an overlooked risk. There's lots of advanced persistent threat fear, uncertainty, and dread—FUD—but the FUD has a bit of truth in it. Consider hospitals; entire medical centers are now wireless.

© 2015 The CyberWire

How long will it be before someone from a parking lot can shut down every medical pump in a hospital? FEI Systems' Taule suggested segregating embedded devices on different networks. Harmon observed that vendors in this space remain inattentive to security in what is now a commodity market. Tactical Network Solutions demonstrated ten zero-days on IP cameras at BlackHat. Not one of the affected vendors contacted them about the vulnerabilities.

AT&T's Huegel described de-parameterization as approach to cyber security. AT&T has been considering de-parameterization for some time. We all have multiple roles and multiple identities, making walls not only impractical, but an actual risk. We should consider putting rings around things, not networks – let devices protect themselves.

Allegis's Dana Pickett strongly advised businesses to assess what's on their network. Baseline it and assess risk. Taule urged companies to demand, from vendors, a baseline of what constitutes normal behavior from the systems that they're selling. You don't need source code, but you do need a behavioral baseline.

Taule, who's "tired of the term 'APT'" and prefers to call such things "weaponized threats," shared a lesson from the experience of being acquired by a larger business. As a small company you may not have been of great interest, but attackers read press releases and once you've been bought, you're a target. As soon as the press release is out, attacks spike.

The trend toward BYOD (bring your own device) elicited considerable discussion. Pickett advised that, in a BYOD environment, you need to be sure the business and personal are separated and make sure that the business data are easily wiped.

This, Huegel pointed out, is all the more reason to put rings around things. When the real threat arrives in mobile, it won't look the way we expect it to. There's a lot of intelligence exposed on mobile devices. They are becoming primary endpoints in corporate networks. Note, too, that phones are becoming means of authentication.

Be sure to get policies, disclosure, and permissions in place before adopting BYOD, advised Taule, who also suggested securing legal advice. BYOD, he reminded the audience, is about economies. Consider applying controls only where necessary.

Pickett offered sound summary advice: do the simple, obvious things—like using strong security software—to protect endpoints.

National Cyber Security Hall of Fame Induction

The Hall of Fame's Class of 2013 was inducted in Baltimore yesterday. See the link below for full biographies of the pioneers honored. In brief, they are David E. Bell (co-author of the Bell-La Padula model of computer security), Jim Bidzos (CEO and Chairman of VeriSign, Inc.), Eugene H. Spafford (Professor of Computer Science, Purdue University), the late James Anderson (pioneering student of intrusion detection and founder of the CIA's "Brain Trust"), and Willis H. Ware (Computer Scientist emeritus at RAND Corporation).

Lieutenant General (retired) Kenneth Minihan, former Director of the US National Security Agency, welcomed and congratulated the class of 2013. He described the National Cyber Security Hall of Fame's vision as building a bridge from the past to the future by educating, stimulating, and commemorating cyber achievement. He spoke of Maryland's happy convergence of science, technology, engineering and math (STEM) education with government requirements in the center of an East Coast tech corridor running from Boston to Atlanta. He closed by commending the example of the Cyber Security Hall of Famers to all young people thinking about their future careers.

US Representative Charles Albert "Dutch" Ruppersberger III (Maryland 3), Ranking Member of the House Permanent Select Committee on Intelligence, delivered the evening keynote.

© 2015 The CyberWire

Cyber threats, Congressman Ruppersberger asserted, are, along with weapons of mass destruction, the greatest threat that the United States currently faces. He described congressional efforts to pass effective cyber security legislation and their concern for doing so in a way that respects privacy and civil liberties. (He parenthetically described the media's recent coverage of the National Security Agency as both sensational and distorted.)

The House cyber bill seeks to address the threat of, among other things, economic warfare and industrial espionage being carried out against the United States by hostile or competing foreign governments. The bill would enable information sharing, revising restrictions on information sharing passed into law in the late 1940s. The government's cyber operators are, he said, currently in the position of a meteorologist watching the progress of a hurricane but prohibited from warning anyone who's in its path.

He closed by urging people to understand that the US is being attacked all the time. And, of course, he ended by congratulating and thanking the Hall of Fame class of 2013.

October 11

This issue concludes our coverage of CyberMaryland. We wrap up with a look at a recurring theme at the conference: the importance of education and training to the rising cyber generation and its place in the workforce. Yesterday, we interviewed conference participant Haden Land, Vice President of Engineering and Chief Technology Officer, Information Systems and Global Solutions-Civil, Lockheed Martin. And don't miss Dark Reading's interview with 2013 National Cyber Security Hall of Fame inductee Eugene Spafford, linked below.

Interview with Lockheed Martin's Haden Land: Engagement with Education

The CyberWire: *What would you like to tell us about Lockheed Martin's philosophy of, and involvement with, education?*

Haden Land: *I'd characterize our involvement with STEM (science, technology, engineering, and math) education as being K-J: "Kindergarten through job." We think success in STEM education depends on collaboration among industry, educators, policy-makers, and families. Since we're the number one IT services provider to the federal government, we think we have a responsibility to inspire students and help deliver STEM education. We gave $10M last year to education initiatives with a strong emphasis on STEM, and we're committed to supporting programs, diversity, and both student and teacher development. With around 60,000 engineers and technologists, we're well placed to engage with not-for-profits and schools as partners. Sponsored activities, competitions, mentorship, curriculum development – they're all part of the mix.*

The CyberWire: *What is it about LifeJourney – a career-development platform launched Tuesday afternoon at CyberMaryland – that leads you to think it's a new and promising approach to mentoring students?*

Haden Land: *For us, it's important that LifeJourney scales. It provides a platform from which you can reach masses of students, and it's one of the better ways of connecting with students, parents, and teachers. Regular reports go to, and are tailored to, all those who have a stake in the student's development. It's a wonderful way of achieving additional outreach beyond traditional programs like career days at schools. With a career day you often see a lot of enthusiasm, but you also usually find that this flattens quickly. With LifeJourney, we think we can achieve continuing engagement that pays off in terms of the student's sustained interest.*

The CyberWire: *How would you describe LifeJourney's value proposition for Lockheed Martin?*

Haden Land: *We're very aware of the last twenty-five years' declining STEM (science, technology, engineering and math) metrics. Lockheed Martin is, of course, a science and technology company,*

© 2015 The CyberWire

and we need STEM skills. Tactically, we need to provide cyber security solutions and services for our customers, and we have to have a workforce qualified to deliver them. We're engaged with STEM education to raise awareness of the need for it among students and educators. Strategically, we're focused on the expansion of data science (and we're partnered with others to have data science subjourneys within the LifeJourney Field Trip we're leading). So our engagement with STEM generally makes a contribution to our future workforce.

The CyberWire: *How have your people responded to the opportunity to mentor students?*

Haden Land: *With LifeJourney, we're just beginning, of course, since it just launched this week at CyberMaryland. But we've seen a lot of interest. We chose two mentors – one woman, one man – from a pretty large pool of interested people. The first two mentors, by the way, are creative as well as scientific: they think divergently as well as convergently. As far as recruiting goes, there wasn't a need to say much. Our people get the point of what we're doing.*

The CyberWire: *How have the students responded to Lockheed Martin?*

Haden Land: *Quite well, given that LifeJourney has just begun. We've long participated in many career days, and we always see a lot of enthusiasm. But that enthusiasm doesn't always last, and it doesn't scale. Too often the conversation lapses once the career day is over. We see our Ambassador and Career Day programs using LifeJourney to keep the conversation going.*

The CyberWire: *When someone at Lockheed Martin signs up as a mentor, what kind of support does the company give him or her?*

Haden Land: *Our normal rhythms prepare our people to succeed as mentors. We work to provide career growth for our people, and that tends to make them a natural fit for this kind of program. They're willing to engage with students. Of course, our mentors represent Lockheed Martin, and we give them the help they need to be at the top of their game when they're guiding a LifeJourney.*

The CyberWire: *Is there anything else you'd like to share with our readers about LifeJourney and Lockheed Martin's role in the program?*

Haden Land: *Lockheed Martin is proud to be the first LifeJourney sponsor. We've done a great deal of outreach to agencies and customers to help grow the LifeJourney ecosystem. We also think turning STEM into STEAM – integrating the arts – is important, and, by the way, that's highly reflected in our choice of the Lockheed Martin Data Scientist LifeJourney Mentor. We hope to have other mentors in the future to highlight careers requiring multi-discipline STEAM degrees.*

The CyberWire: *Thanks very much for your time, Haden.*

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

© 2015 The CyberWire