the cyberwire

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

DC Metro Cyber Security Summit

June 3, 2015 McLean, VA

The FBI's Morning Security Briefing.

Donald Good, the Deputy Assistant Director of the Federal Bureau of Investigation's Cyber Division, delivered a threat briefing and described the Bureau's cyber mission. He characterized it as a global mission that will combine the FBI's unique national security with law enforcement authorities.

The Bureau's mission is to investigate, attribute, disrupt, and prosecute cyber crime. Each of the FBI's fifty-six field offices has a cyber unit, and its more than sixty overseas offices also deploy significant cyber law enforcement capability. Good was at pains to emphasize the importance that the Bureau places on collaborations with local, state, Federal, and international partners.

Having outlined his organization's mission and some of its capabilities, Good summarized the anatomy of a typical cyber attack using the familiar "kill-chain" model. He noted that spear phishing was the attack method in some 80% of the cases that the FBI investigates. Threat actors include hacktivists, criminals, insiders, espionage services, terrorists, and warfighters. Organizations that hold large amounts of personally identifiable data (PII) are currently being heavily targeted.

The FBI, Good said, engages the private sector to prevent crime by disrupting and dismantling criminal nets, and also seeks to educate and inform (sometimes such information includes one-day read-in security clearances). The Bureau tailors its assistance to specific sectors: it recently conducted nationwide threat briefings for the healthcare sector, and conducted GRIDEX as a cyber exercise for the energy sector. Good used InfraGard as an example of a particularly effective program for on-going information sharing; he also touted Joint Advisory Bulletins and FLASH reports as examples of the FBI's commitment to cyber threat information sharing.

Good believes that the Sony breach was instructive in two ways. First, it was an example of a trend toward increasingly destructive attacks. Second, attribution and recovery were made easier by the prior relationship the FBI had established with Sony. Good invited other companies to get to know their regional FBI field office.

He advised companies to undertake network preparedness measures: education, network topology mapping, logging, access control, continuity planning, and disaster recovery planning. In a rapidly changing threat environment, security controls and patching are vital. Speed matters in incident response, and preparation serves speed. That preparation should include not only a working relationship with law enforcement, but also a well-rehearsed plan to bring in legal, media, and security company help. The value of tabletop exercises cannot be exaggerated, and Good said the Bureau was able to help companies prepare them.

He closed by entreating those in attendance to "share [information] by rule, not by exception," and to regard the FBI as a "non-disruptive partner."

Keynote: Learning Cyber Security.

Kris Lovejoy, IBM's Global Chief Information Security Officer, delivered the conference keynote. She began with an anecdotal account of studies of learning in rhesus monkeys—it turns out they can not only learn to recognize signs of unpleasant events, but can also transmit their learned recognition to other monkeys. We, of course, need to do likewise. Everything we know about cyber, she argued, we've learned from having it passed on to us, and it was her intent to pass on some of what IBM has learned.

The reality is that our twenty-year-old defense-in-depth model is flawed. We thought in terms of a castle or a fortress, but this image is profoundly misleading. We should instead think in terms of a biological model. "Our organizations are organisms, and should be understood as organisms." The immune system is a much more useful metaphor than the castle.

Lovejoy quickly ran through some statistics to provide context for understanding cyber risk and response. The average organization, she said, will see about 1.7M events per week—and these are security events, not attacks. Some 324 of those events are attacks, and 2.1 of these, per week, will result in an incident. Yet only one out of every one hundred security compromises are ever detected.

So, she argued, we should try to build "herd immunity." 95% of malicious incidents (excluding, of course, what Lovejoy called "oops" errors) show some exploitation of human error as a contributing factor. 56% of attackers are outsiders, 17% insiders, 22% represent some combination of the two, and 5% are undetermined. So one approach to building immunity is to focus on privileged users. An example is IBM, a company that locks down both IT admins and developers.

Organizations that are good at security see more attacks and incidents because of the superior visibility they have in the state of their environment. Adherence to ITIL principles is the best protection—it's basic hygiene—and it's found in best organizations. ITIL also improves resiliency, reduces error, and cuts costs.

Turning to the motivation behind cyber attacks, Lovejoy made the obvious point that the bad guys go after data because data can be traded in black markets. The trade in stolen data on a carding forum is a good example of such criminal market activity: you can buy Bitcoins with a stolen card, buy malware with Bitcoins, and then move on to your next victims. The black market, Lovejoy explained, really does function like a market. She illustrated this with attacks-as-a-service pricing models, noting that such services often come with many of the trappings that surround legitimate transactions: guarantees, discounts, service level agreements, and so on.

To understand the future of cyber crime, Lovejoy referred the companies attending to UN studies of the effects of rising web access. When you bring broadband into developing countries that have significant populations of under-employed young males, you see the rapid growth of a cyber-criminal subculture. That subculture is showing an increasing predilection for destructive cyber attacks that threaten systems and, perhaps, lives. We've recently seen the growth of wipers (common in state-sponsored sabotage) and in tools like CryptoLocker, which combines destruction with greed-motivated cyber crime.

So what can organizations do? Practice sound digital hygiene, of course. They can increase the "security IQ" of their personnel. They can prepare and exercise response plans. They should secure endpoints. They should define, protect, and monitor their "crown jewels." And they should leverage security intelligence to improve their ability to prepare for and respond to the attacks they'll inevitably sustain.

In response to a question about what danger points—"trigger events"—companies should recognize and prepare for, Lovejoy noted two in particular. Mergers and acquisitions are

particularly attractive events for cyber threat actors. Entrance into a new geographical market is another. Both tend to be points of increased vulnerability, and attackers know this.

Answering other questions, Lovejoy reminded the audience that their supply chain presented an important attack surface (with marketing and public relations firms also forming part of that attack surface). She also advised them to pay close attention to legal restrictions on user behavior monitoring—she suggested that European Union data protection laws effectively rule this out for companies doing business in Europe.

The Relationship Among Cyber Security, the C-Suite, and the Boardroom.

The day's first panel, moderated by Phillip E. Lacombe (Vice President, Parsons Information Systems & Security Sector), took up the challenges involved in getting corporate leaders to engage cyber security challenges effectively. Panelists included Nick Leshock (CISO, Director, Cyber Security Services, General Dynamics Information Technology), Richard Bejtlich (Chief Security Strategist, FireEye), Paul Ferrillo (Counsel, Weil, Gotshal, and Manges), and Mark Shaw (Senior Executive Director and Branch Chief, Cyber Security and Investigations, ManTech).

"Cyber is a true shared responsibility," Lacombe began, and noted that it's also not an engineering problem. The threat is constant, and he asked the panelists to give their assessment of where we are today.

Doing his best imitation of Strother Martin as the Captain in "Cool Hand Luke," Ferrillo said that what we have is a failure to communicate. CISOs don't get enough attention from boards, and in turn CISOs don't communicate effectively with boards. They aren't presenting the cyber risks to the boards, and the boards don't ask for enough discussion of risk. After a paltry show of hands in response to his pugnacious demand as to how many in the audience had adopted the NIST Framework ("So why haven't all of you adopted the NIST Framework?") he finished by saying "we suck at cyber security" because we don't communicate.

Leshock demurred: "I don't know about 'sucks,' because, after all, what are we comparing ourselves to?" Telling people they "suck" smacks of FUD, and that's a worn-out approach that has, itself, become a barrier to communication. Leshock thinks that businesses are starting to address cyber, explicitly, in important public documents. SEC enforcement has become a very positive sign: it's forcing a conversation. CISOs should leverage this new recognition of cyber's importance by making it personal for the board. Invest in realistic breach exercises, he advised, and walk the C-suite through what could happen.

Bejtlich explained that we're seeing new players with new motivations supplanting the traditional threat actors. These new adversaries see themselves as aggrieved, and are more destructive than the older actors. Businesses are seeing other pressures: regulatory bodies other than the SEC—particularly the FCC and FTC—are becoming more active. There's Congressional pressure from national security Republicans and consumer protection Democrats. Insurers want a close look at companies' cyber security posture. Leshock seconded the point about insurance: the annual renewal of cyber insurance has become a milestone event, even as the cyber insurance market remains relatively immature (actuarial data are still lacking, but this will change). Shaw discussed the importance (and difficulty) of quantifying an organization's cyber risk.

Lacombe observed that cyber isn't just an IT issue anymore—it's become an OT - or operational technology – issue as well. And OT is less prepared to handle it than IT. Ferrillo took the last word and ended on a hopeful note (with which there was general agreement): "It's good to see companies who are hacked treated as victims, not knuckleheads."

The Real Costs to a Company's Brand and Reputation After a Cyber Attack.

Panelists included Jason Maloni (Senior Vice President & Chair, LEVICK), Jeanmarie Giordano (Chief Underwriting Officer, Professional Liability at AIG), James Reagan (Enterprise Practice Director / Cybersecurity & IT GRC, Global Knowledge Training), Tom Resau (Vice President, W2 Communications), and Derek Gabbard (President, FourV Systems).

The panel advised businesses to take a look at the costs of a cyber attack and to carry cyber insurance. Giordano explained that having a response plan lowered the cost of a breach. Malone observed that, counter intuitively, stock prices actually bounced back fairly quickly after a breach (so quickly, he noted, that a speculator might well take positions in companies that sustained one). The more important cost is of customer perceptions. The panelists also pointed out that companies' recruiting also took a hit from increased perceptions of cyber vulnerability.

Giordano said that underwriters looked closely at response plans and organizational resiliency. The panel as a whole agreed that plans were essential. They should be holistic, comprehensive, tested, and not too bulky.

NIST on Cyber Security.

Paul Ferrillo (Counsel, Weil, Gotshal & Manges) interviewed Matthew Scholl, Chief of the Computer Security Division, National Institute of Standards and Technology (NIST).

Scholl began with a description of NIST's standards mission. He noted the vast amount of data organizations held, and the complexity of determining whether you're winning or losing in cyberspace. Cyber attacks are increasing, they have global reach, and they offer criminals a huge return on investment.

Ferrillo said that it was a truism that the "only way to fight is to know your adversary," and asked about the government's role in distributing threat analytics. Scholl answered that technology, policy, and law are all still immature. In fact, at present, he thought the government learned more from the private sector than it taught that sector.

Scholl summarized the background of the NIST framework. It originated in an executive order that charged the government to cooperate with the private sector on cyber security. The goal was to reduce risk without imposing crippling constraints. Since NIST isn't a regulatory body, it was able to serve as a non-threatening broker. The Framework that it evolved, in consultation with the private sector, has become a superstructure used to organize cyber security with a well-structured taxonomy and a common understanding. It was not intended to be coercive, and Scholl believed they'd found a way to avoid such an interpretation: the framework isn't mandatory.

Responding to Ferrillo's question if it should become mandatory, Scholl thought not. "There's no lack of regulation. We'd like people to use the framework as a Rosetta Stone for compliance, and we'd love to see resources move from compliance to security. We don't want to force people to do more."

Ferrillo asked that, if IT is in fact shifting to the cloud, whether we can protect the cloud. Scholl noted that we all have data in the cloud; the cloud is ubiquitous. "There's a huge trust extension when you give your assets to someone else. But there are huge advantages to the cloud as well." The ability to use virtualization, for example, is a huge advantage.

Ferrillo asked if Scholl saw a movement toward data encryption in the cloud. Scholl said, "Yes, absolutely. NIST will never argue against encryption." And the discussion concluded with strong advocacy of strong encryption.

Mitigating Cyber Risk to Contain the Human Element.

The panelists included J.P. Wilson (CEO, Global Compliance Consultancy Group), Julian Waits (President & CEO, CyberPoint Risk Analytics), James Walter (Director Advanced Threat Research, Intel Security), Jim Hansen (Executive Vice President, PhishMe), and Christopher Budd (Global Threats Communications Manager, Trend Micro).

Hansen said that we tend to focus on technology and (sometimes) process at the expense of the human element. He urged companies to empower their people to enhance security. Budd agreed that the more we can make people the frontline of defense, the better.

Almost all of the famous breaches over the last decade began, Walter reminded the audience, with some human action—responding to a phish, visiting a waterhole, etc.

Waits argued that people are at once your greatest asset and your greatest vulnerability. He also noted that companies should look at cyber insurance the way individuals look at life insurance. "One day," he said, "you'll use it."

Hansen advocated crowd-sourcing detection as a way to shrink your window of vulnerability. Your model, he said, should be the detection of the attempted Times Square bombing: "Two guys selling six-dollar t-shirts noticed that something looked weird, and they told someone about it." You probably hire smart people, so educate them.

Active cultivation of people by criminals and intelligence services has significantly increased, Budd said. Phishing emails now contain really good and really convincing tech writing. Walter pointed out that more sophisticated campaigns now often included a long - sometimes years long - reconnaissance period. Training should sensitize people to distinguish what's legitimate from what's not. We also face trust issues: crooks and states alike recruit employees to work against their organizations.

Wilson observed that education and training have got to start from the top down. Budd argued that CEOs need to enable upward communication, and Waits explained that the market is waking up to the fact that executives are the biggest vulnerability there is. "People," he said, "fail to base their plans on what's important to them," and illustrated this with Target's failure to manage admin accounts. Leaders need to view security as part of their business, not a hindrance to it. Of course, Waits continued, do defense-in-depth, "but then absolutely protect the invaluable stuff."

Wilson asked whether encryption could become an organization's Plan B. Waits thought it should be in Plan A. "From an end-user perspective," Waits explained, "the best encryption is the one you don't know about. Your environment has already been compromised, so make sure the most important stuff is protected." Hansen suggested that Plan B should concentrate on detection and response. "You're not going to build a flawless defense. You've got to cut down the detect-and-respond time. That extends to vendors and the supply chain.

Budd offered a last word: "Structure your enterprise to reduce temptation."

Emerging Risks and Countermeasures Against Them.

The day's final panel included Jim Aldridge (Director, Mandiant), Ralph Kahn (Vice President of Federal, Tanium), Chris Coleman (Chief Executive Officer, Lookingglass), John Prisco (President & CEO, Triumfant), and Mike Spanbauer (Vice President of Research, NSS Labs).

Prisco, as had many others over the course of the day, emphasized that many breaches were attributable to failures of basic digital hygiene. Kahn argued that we want detection and remediation to get an order of magnitude faster. We want compliance to become continuous.

Coleman urged active monitoring of the environment as essential to preparing for emerging threats. He advised the audience to "be more aggressive in actively combing your internal network."

If technology by itself could solve our security problem, Kahn argued, then it already would have done so. "Your most important asset is your people. Invest in making them more effective."

Coleman said that security had a lot integration left to do, and a lot to learn from the networking space. Prisco concurred, observing that the cyber security industry was still in its infancy (or, at best, in its toddler stage). "I can't think of a targeted intrusion," Aldridge said, "that didn't rely on theft and abuse of legitimate credentials," to which Prisco added, "The average company isn't going to be hit by something that advanced or exotic. Do the basic blocking and tackling."

"Automation and routinization are the time-honored ways of dealing with skill shortages," Kahn observed in response to Spanbauer's question about when it's right to reach out for additional help. Kahn also advised businesses not only to plan, but also to test their plans."

Coleman warned against thinking that your work life and your individual life were unrelated, or that you're not of interest to both criminals and states. Spanbauer agreed, and told companies not to underestimate the information correlation being done in the underground.

Sharing is an improvement, but it needs to get faster. Prisco said that the IRS breach was probably not the IRS's fault—the attackers probably came in with SSANs stolen from a healthcare insurance provider—and that this incident showed how one attack can cascade into other victims. Coleman thought that too many don't share because they feel they've got more to give than to gain, and Kahn said that sharing depended upon trust. "It would be good to have a mechanism for establishing trust."

Coleman pointed out that there was a lot of nefarious sharing going on as well: "We also don't, in our industry, think enough about how the adversary could use sharing against us."

And with this panel the conference concluded. The next Cyber Summit will convene in New York on September 18.

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 6.10.15