the cyberwire

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

Sahouri Speaker Series: the Cyber Threat

April 28, 2015 Baltimore, MD

The Cyber Threat: A Business Perspective

Sahouri Insurance and Financial convened a panel discussion yesterday to address cyber threats to the business community, and in particular their financial and liability ramifications. The session's objective was to give the business community a sense of how cyber security affects them — too many in that community, Sahouri suggested, retain an unjustified sense of immunity to attack. Panelists were Michael Echols (Director of the Cyber Joint Program, US Department of Homeland Security), Robert Ellison (Hanover Insurance, Regional Technology Director), and Karl Gumtow (co-founder and CEO of CyberPoint International). Michael Sahouri moderated the panel.

An overview of the cyber threat

In response to an opening question inviting panelists to give businesses some overall advice on how to approach cyber security, Echols said they might begin by usefully analogizing it to physical security — a way of reducing risk to their business. CyberPoint's Karl Gumtow noted that lapses in basic IT hygiene could cause business problems. Cyber security is now an issue that touches every human being — everyone who has a phone, drives a car, uses email, is the subject of any public record — and it is a global issue, not confined to localities or nations. Hanover's Ellison said, from his perch in the insurance sector, that he thinks businesses need to understand that the burdens of litigation driven by cyber events are severe. It's important to work with the right partners, because as of yet there is no standard insurance coverage in this area; instead, policies tend to be highly tailored to specific circumstances.

Whenever we introduce a new technology, Echols said, we introduce a new threat. Therefore, the definitions of "cyber" and "cyber threat" shift. Wearable devices and smart phones ("now powerful computers") all expose businesses to attack. He reviewed stories of phones being compromised and turned on remotely by third parties in order to eavesdrop on business meetings. Wherever you have a signal, he concluded, you have cyber.

Gumtow pointed out that there's no cyber without information technology. Everything can be exploited. CyberPoint does a lot of security assessments and they find issues at all levels, from nation-states to small businesses: they find poorly written websites put onto single, third-party servers (along with thousands of other sites) without any particular attention paid to those servers' security. But in the end, users remain the biggest threat — Gumtow guarantees that if you drop a malware-laden USB stick in a parking lot, someone's going to pick it up and plug it into their device (especially if the USB dongle is "cool-looking"). Every time you click on a new thing, you face a threat. You're susceptible to spoofing in social media, and in email.

What's happening to small businesses?

Small and mid-sized businesses, Echols stressed, are under attack. You may not hear about the mom-and-pop store getting hacked, but it happens all the time with devastating business

consequences to the victim. He recommended that all businesses take a good look at the NIST cyber security risk framework and use it as a baseline for their security. He recommended that business communities and others (from the chamber of commerce "to the pastors of twenty Baptist megachurches") look into forming the Information Sharing and Analysis Organizations (ISAOs) facilitated by the President's recent executive order.

When sked what insurance claims he's seeing at Hanover, Ellison said that Echols is right: small businesses are indeed under attack. "The bad guys run programs that look for weaknesses." A third-party study of data breach insurance claims showed that most come from small businesses with revenues under $50 million. The average payout on such claims is $733 thousand. And $698 thousand of that amounts to legal expenses. "Litigation is costly. You don't have to be guilty, just accused." He seconded Gumtow's earlier point about the seriousness of the insider threat. Sometimes that threat is malicious, but more often it's just careless or ignorant.

What about disclosure? What about compliance?

Echols described pending legislation designed to limit liability in ways that would promote the timely disclosure of data breaches. Companies, he said, certainly have an ethical obligation to disclose breaches to their customers, but many don't – precisely because they fear being sued by those customers. Liability protection might therefore prove a spur to information sharing. He wanted people to realize that their data are valuable, and that there are criminal outfits on the Darkweb making a fortune from stealing those data.

Ellison called "What's my obligation to disclose?" the "million dollar question." Forty-seven states, plus Puerto Rico and the District of Columbia, have laws governing disclosure, and all of them are different. So, the question is complex. He urged businesses to think hard about the information they hold, and the risk to which it exposes them. Consider both first-party and third-party coverage. And notify stakeholders of a breach as soon as possible.

"Companies want to do the minimum to be compliant," Gumtow observed. "And if you're doing the minimum, you're probably being exploited." Companies don't want to share when they're attacked, but attacks happen to everyone. "If you're required to do it, do it right. Don't do the minimum." Ellison agreed and cited the State of South Carolina revenue system breach of a few years ago, for which the state itself was out of compliance with its own laws. He also noted that, in response to a question from the audience, a sound third-party expert assessment with appropriate action taken could indeed help your coverage rates go down.

How do I know I'm in the middle of a cyber attack?

Everyone, Echols said, has been hacked. We invite people into our networks — we have to, in order to do business — but that brings with it a risk. "Make sure your employees understand that, if you're out of business, they're out of work." It's a question of risk management.

Gumtow pointed out the difficulty of detecting a damaging attack. "If you have intellectual property on your computers, and someone copies the file, they don't delete it. You've been hacked. You've lost your IP, and you may never know you've been hacked." He strongly recommended basic IT hygiene, such as whole-disk encryption and encrypted email, as a way of beginning to mitigate risk. "It's not that hard or that expensive."

Ellison added that small businesses should work with a company that does penetration testing.

Closing takeaways

From Michael Echols, Department of Homeland Security. “Leave here thinking about cyber security the same way you think about accounting and physical security. It’s about risk management: deciding what’s important to you. We can’t protect everything, because we also have to live. Do the things a non-expert can do, and then call in an expert.”

From Karl Gumtow, CyberPoint. “Focus on how you quantify your risk, and arm whoever serves as your CIO or CISO to talk to the CFO and CEO about making informed risk decisions.”

From Robert Ellison, Hanover Insurance. “We’ve all got an affinity for small businesses. We don’t all have the wherewithal to write a $1 million check. Insurance, remember, offers risk transfer: the opportunity to not to have to write that check. Have the right conversations with the right partners.”

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 8.5.15