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

Cyber 6.0 Conference

September 10, 2015 Howard County, Maryland

Thought leaders from the cyber security industry convened in Howard County on September 10, 2015, to consider the rapidly evolving nature of the cloud, and the way it's shaping cyber security. The CyberWire went to hear what they had to say.

The Cloud: Mitigating Risks, Creating Vulnerabilities

William ("Bill") Arbaugh, president and CTO, Five Directions, delivered the conference's industry keynote. He described the strengths and weaknesses of cloud technology today, and argued that cloud usage must be evaluated within the context of sound risk management.

He began with the glum observation that, "Mission will always trump controls and mitigation." Making money will always trump security, and "doing security right is expensive and often inconvenient." The cloud, essentially irresistibly attractive because of the efficiencies and cost savings it promises, is a good example of how business imperatives affect security.

The cloud carries with it several clear risks. A third party has control of your data (and possibly your computations and data manipulations). If your data are encrypted, who has the keys? Where and how do they have those keys? What ensures data integrity in the cloud? How available are the data? Do the data cross borders as they're used? Whom does the cloud provider trust? (And remember, trust isn't transitive.) Finally, what happens to your data, to your enterprise, if the cloud provider goes out of business?

Arbaugh discussed Box.com as a representative example of issues surrounding cloud data storage, illustrating his points with screen grabs from Box itself. He noted (with a hat tip to Ars Technica) several weak links in Box's data handling chain, including moments when data appear in plaintext. Encryption is also problematic: Box has the ability to generate (and thus have) users' encryption keys. It doesn't claim that your data can't be turned over to law enforcement (a common privacy concern), and its disclosure that it controls users' encryption keys is obscured by marketing language.

Box is not unrepresentative, Arbaugh suggested. He described the service to highlight the issues cloud users must address—all of the terms, conditions, and circumstances of any cloud provider may be fine for any given user, but the intelligent cloud user will carefully weigh them all. Cloud security, like all security, fundamentally comes down to risk management.

Identifying the Challenges and Problems of Cloud Security

The morning panel that followed the keynote featured experts who discussed how enterprises should assess the benefits and risks of migration to the cloud.

Markus Rauschecker (University of Maryland Center for Health and Homeland Security) opened the panel with a caution: "There are serious legal and policy issues in the decisions we make with cyber security." He also noted the importance of general involvement in cyber security, "from the CEO to the newest employee," because cyber security is inherently collaborative.

These challenges become sharper as an enterprise moves into the cloud. "What," Rauschecker asked, "are the standards for liability protection? Those standards are not necessarily clear, and how does a business show that they are following them? It's critical that you review every word of the agreement you have with your cloud provider."

Tony Sager (Senior Vice President, Center for Internet Security, the SANS Institute) saw cloud adoption as essentially a process of abstraction. "We create levels of abstraction to make computers easier to use. The more abstract, the less I worry. In the cloud I worry less about storage, about whether the bandwidth is big enough."

So the cloud actually relieves us of some worries. "But the flip side," Sager said, "is that I know less. By design, the abstraction takes that away from me. We generate confidence through the control model." While this may be a challenge for the cloud user, "remember that these abstractions are a challenge for the bad guys, too."

Sager closed with a general characterization of where we stand with respect to cloud security. "We are in the emergence from wizardry stage. The wizards come in and fix things, and then we send them on their way and go on with the business of democracy. We are moving from the notion of this being a technical problem to that of it's being an economic and social problem, and that's a good thing."

A third panelist, Brendan Fitzpatrick (CERT Cyber Risk Management, Carnegie Mellon Software Engineering Institute) took up resilience, and how that can be achieved in the cloud. "Resilience is an emergent property of an object to withstand stress over time," he observed. "For example, consider a slinky. It can bend and stretch, walk down stairs, and return to normal. But if you over-stress it, you'll damage it and it won't be able to return to normal."

He advocated a layered approach to technology, and also to the people responsible for implementing policies and procedures. He shared a story of an outdated call roster, waking a high-level authority in the middle of the night to alert him to a security issue, only to be told the officer had retired four years ago. "I can see nothing has changed since I left," the officer remarked, "including your call roster."

US Cyber Command's Lieutenant Colonel Matthew Dunlop enlarged on the challenges cloud technology posed military and government enterprises. They too face economic and social issues. To take one of them, low-bid contracts can induce providers to cut corners, forcing users to accept risks they'd otherwise prefer to buy down.

As the session concluded, Rauschecker reminded the conference that laws and policies lag technology, and that when technology advances as rapidly as it has, it becomes incredibly difficult to keep pace. Sager argued "We can only do this through collective practice. None of us has the expertise to make smart decisions about the cloud on our own."

The Cloud's Implications for Healthcare IT

Healthcare organizations are also grappling with the challenges of cloud migration. The CyberWire attended the special session on healthcare IT.

Darren Lacey, Chief Information Security Officer & Director of IT Compliance for the Johns Hopkins University, began with an observation about the sector as a whole: "Electronic health records providers are consolidating, so it's a good time to be a cloud provider for health care."

While it might appear that healthcare organizations are still deliberating about moving their IT to the cloud, in fact this transition is practically inevitable. Jason Taule (CSO and CPO, FEI Systems) explained, "The horse is out of the barn. You are likely already using the cloud. You are sharing information, so we need to recognize that." Sheer economics drive this. "We would like

to spend limited resources on providing care, rather than management. The cloud can help us realize real savings."

Tim Falls (Senior Project Manager, Honeywell Technology Solutions) said that full-scale cost analyses have yet to be done in some of the biggest healthcare networks. "From a care provider it's really risky. I've heard it described as 'pervasive fog of war'."

Part of that fog of war may be regulatory uncertainty. Consider HIPPA (the 1996 Health Insurance Portability and Accountability Act). "Cloud providers are subject to HIPPA,

Taule observed. "They're pushing back on this. It's not just a matter of choosing the right vendor, it's working with that vendor on and ongoing basis."

Also contributing to the fog are the many issues surrounding encryption. As Lacey explained, "Vendors have to have a crypto story. You can't see my data. S3 encryption isn't good enough. I know what it feels like to have a breach downstream, being on pins and needles not knowing if your data has been hacked."

Cyber security standards of care, currently emerging in a complex, cross-grained legal and regulatory environment, also are beginning to drive cloud providers and users toward certain practices. For example, as Lacey continued, "You have to have logs, and I need to be able to read them. If I can't see the logs, there's no dice. They have to be in real time, and they can't just be on request. We're all going to get hacked; we're all going to get sued. No CFO is going to go against the CSO, because it's indefensible in the deposition."

The panelists were asked, what keeps you up at night? What scares you? "What worries me," Lacey said, "is that we're making too many copies of the data. Somebody's using their personal DropBox account, then the data shows up years later because someone misconfigured their settings." Taule worried about the difficulty of managing security. "We can no longer achieve the desired secure end state. The end is moving further away from us faster than we can catch up to it. Knowing that, the breach is inevitable." Falls took the last word: "What we like about the cloud is also all of the things that scare us about it. There's a cultural shift happening in our society; we're getting used to our data being out there."

Lessons Learned and Opportunities to Achieve Resilience

Lieutenant General (retired) Rhett Hernandez (West Point Cyber Chair, Army Cyber Institute, first commanding officer of Army Cyber Command and President of CyberLens LLC) delivered the afternoon keynote.

Hernandez began by characterizing movement to the cloud as necessary—"an opportunity we can't miss." Speaking about the Army, he described its former culture as one that cared about the services needed, not about threats to the network. Changing that culture has been, in many ways, the primary cyber security challenge facing the service.

The network serves situational awareness, enhancing it by "putting the right information in front of the right person at the right time." Data are merely data, he observed, but data are the first step on the way to information, and then to knowledge.

With respect specifically to the cloud, Hernandez argued that "Users need access, but they also need controls. No operation is risk-free. The cloud is no different from the world we live in."

He closed with a warning about the risks the rapid proliferation of the Internet-of-things is imposing, and he called for a multidisciplinary approach to cloud security that would conceive of cloud challenges as risk management problems.

Identifying Cloud Security Opportunities and Solutions

Given the apparent inevitability of migration to the cloud, what security solutions and opportunities are worth pursuing? The afternoon panel of industry and government experts took up this question.

Cameron Chehreh (Chief Technology Officer, Dell Federal) began by asserting that cloud security is not a technological problem, but a human one. It calls for "an active defense policy, and a continuous hardening policy."

"Focus on what your mission needs are first, not the technology," advised Mike Thomas, Technical Director, Information Assurance Directorate, National Security Agency. "Public cloud providers, the big ones, probably do a better job of security than you could do in your own server room. It's critical to have standards across your network to enable analytics. This is part of what makes open source powerful."

George Economou, (Chief Technology Officer of Custom Solutions, Akamai Technologies, Inc.) said that he operates "under the expectation that anything I write, anywhere, will be readable by my grandchildren" (with the implicit suggestion that you ought to operate that way, too). He noted the paucity of resources many of Akamai's customers are able to bring to security: "A large number of our customers have limited security personnel, even just one person. We have no easy solution to the need to educate our customers on the need for security."

Marcus Ranum (Senior Strategist, Tenable Network Security) brought some good news and some bad news. "If your security is bad, going to the cloud will probably make it better. If your security is good, going to the cloud will probably make it worse. I think moving to the cloud is a great idea. But in order to use it, we need to reinvent our practices. If we suck, we're merely going to push our suck into the cloud. We're not going to be able to forklift our problems out to the cloud." And he closed with a warning: "Think what it's like when someone else owns your data."

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 9.11.15