The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE
Washington, DC // Brussels // London // www.ici.org

ICI VIEWPOINTS

JUNE 6, 2014

Adapting to the Rapidly Evolving Cybersecurity Environment

By Todd Bernhardt

Because external hackers typically try to "look like an insider" when attempting to penetrate IT systems, "every cyberattack is likely an 'internal' attack," according to Mark Clancy, managing director of technology risk management at the Depository Trust & Clearing Corporation (DTCC). He gave this advice, and more, as part of a panel at ICI's Operations and Technology Conference, which ran concurrently with the Institute's General Membership Meeting in May.

Joining Clancy on "The Evolving Cybersecurity Environment: An Operations and Technology Perspective" were Jason M. Weinstein, partner at Steptoe & Johnson, who moderated the panel; Carl W. Herberger, vice president for security solutions at Radware; and Brandon Hines, manager of information risk and security at Dimensional Fund Advisors.

Something to CHEW On

Clancy led the discussion by introducing the acronym CHEW, which indicates the four basic types of threats that cybersecurity experts must face: criminals, "hacktivists," espionage, and war.

Though criminals exist in every country and are focused on making money, hacktivists have other motivations, including the opportunity to publicly protest—or take revenge against—the organizations they target. There are large numbers of both these groups, with hacking skills that range from basic to advanced.

Espionage includes private organizations or governments spying for their economic benefit, while war includes countries—or even non-state actors, such as terrorist groups—seeking to disable infrastructure or capabilities. The number of countries with these capabilities is relatively small, but growing, as is a larger array of "supported" or "tolerated" groups that act with implicit state sponsorship.

Decreased Costs, Increased Vulnerabilities

Herberger looked at trends in cybersecurity, including how the move to open-source software and the "cloudification" of technology—which have reduced costs for organizations—have increased vulnerabilities.

In addition, he said, "Attacks are no longer 'single-threaded'—they're multi-vector, availability-based attacks that can overwhelm systems" because multi-vector attacks force an organization's security software to spend time evaluating all threats when only one is real.

Hackers rely on the fact that the majority of attacks take minutes to compromise a system, but can take hours, days, or months to discover and defeat. "Bad guys know that the tools you use have gotten pretty good—but they take time," he explained. "During that time, they can do what they need to do."

Getting Out in Front of Threats

In his introductory remarks, Hines acknowledged the threats while focusing on the positive, saying "there are practical strategies...things we know better than the people outside. We'll never be smarter than all of them, but we know company assets and processes better than they do, so we can get out in front of them and build reasonable security measures to protect against them."

He also emphasized that though it's important for company employees to know how to avoid or respond to threats, it's also critical that organizations "examine processes that are prone to failure or easily exposed to bad actors." Clancy agreed, adding that "a lot of business processes evolved from the paper age—you've got to examine and update them so they're appropriate for the interconnected digital age."

Mapping Out Risks

Weinstein quizzed the panel about the risks of "interconnectedness," which he said potentially means "you have to be worried about vendors, partners—even clients. Their platforms could be used as a launching pad for an attack on yours. How can you protect against this?"

Herberger led off, explaining that cybersecurity professionals have to be concerned about risks that could accompany three macro-level trends:

- cloudification, which increases risks by placing you next to other unknown "tenants" on shared servers;
- the rapidly expanding mobile environment, which includes not just cell phones, but the burgeoning "Internet of things" (the connection of everyday objects to the Internet); and
- software-defined networking, "which changes everything about how we inspect our network and the people who come to it."

Hines agreed, saying that organizations should identify which critical resources are outsourced, and map out the risks. He and Herberger recommended reviewing contracts with service providers to ensure that security requirements are spelled out, and that there are processes for communicating about and addressing risks and attacks.

"You have to know who's attached to you and why," explained Clancy. Citing the security breach at the retailer Target, where hackers gained access to the company's IT system through a vendor account, he asserted that "you need to rethink your environment and act proactively, before you get attacked and have to retool everything."

Plan, Test, Train—and Adapt

The panelists agreed that having incident-response plans and testing those plans are essential cybersecurity measures. Hines pointed out that it's key to engage all parties involved (internal and external, on both the IT and business sides) in planning and testing, while Weinstein added that it's essential to include your legal counsel in planning and to work with law enforcement if any security breaches do occur.

Herberger warned that organizations can't take a "set it and forget it" approach to planning—instead, they should "constantly monitor and update plans, to be able to keep up to date with evolving technology and macro-level trends."

"Look at it like war," Clancy concluded. "When things don't go according to plan, you fall back on your training. If [that training] is good and extensive, then you'll be able to flexibly and capably respond to an ongoing attack."

Todd Bernhardt was senior director of public communications at ICI.
