



## **Benefiting from Cybersecurity Info Sharing**

by Mickey McCarter

Thursday, 14 October 2010

### **Panel explores incentives across and between public and private sectors**

A panel of public and private sector cybersecurity experts called for increased collaboration between and among federal agencies and private companies Wednesday, noting that proper incentives were the best way to motivate officials to share information.

Many businesses do not fully understand the financial benefits that come from embracing good cybersecurity practices, several of the experts agreed during a panel sponsored by the Homeland Security and Defense Business Council in Washington, DC.

Far too often, cybersecurity is viewed as a technical matter by business when in fact it is equally a financial matter, said Ty Sagalow, chief innovation officer (CIO) at Zurich North America. President Barack Obama acknowledged as much when he unveiled the US Cyberspace Policy Review in May 2009.

"Traditionally, cybersecurity is viewed as a technology matter to be handled by the chief technology officer and the chief information officer. And it certainly is in part a technology matter," Sagalow acknowledged.

He added, "But we are here today to talk about the fact that in a fundamental sense, network security is an economic matter. It is simply not in my view a technology matter to be solved by the chief technology officer and the chief information officer standing alone. It is fundamentally a financial matter."

According to various statistics cited by Sagalow, 95 percent of corporate CFOs are not involved in network security and 87 percent of companies do not have a cross-functional cyber risk team that bridges technical, financial, and other sides of a company.

Between 2008 to 2009, US businesses lost more than \$1 trillion in intellectual property in cyber attacks, according to the Cyberspace Policy Review. IT security company Symantec Corp. reports that the number of cyber threats jumped nearly 500 percent from 2006 to 2007 and doubled again 2007 to 2008, the Zurich CIO said.

In 2009, about 47 percent of enterprises were reducing or deferring their budgets for information security, according to PriceWaterhouseCoopers.

A multi-departmental cybersecurity task force would boost effective communication between a CIO and a CFO, enabling them to manage risk more effectively, Sagalow argued.

Just as companies must spur collaboration, so must federal agencies, declared Bruce McConnell, counselor to the deputy undersecretary for the National Protection and Programs Directorate (NPPD) at the Department of Homeland Security (DHS).

DHS must examine four factors, McConnell said: Is security improving in the dot-gov domain? Is security improving across sectors of critical infrastructure? Is the United States ready to respond to inevitable cyber incidents? Is awareness about threats and responsibilities in the United States increasing?

To further these goals, DHS is hosting National Cybersecurity Awareness Month in October, encouraging teenagers in American households to think defensively about their online activities.

DHS also put the National Cyber Incident Response Plan through its first major test during the Cyber Storm III exercise at the end of last month, McConnell said. The test was largely a success.

"We found out lots of things, mostly about communications and procedures--things that we need to do better," he reported. "We also found out that we were actually able to respond pretty well. The response community was surprisingly ingenious and innovative in figuring out ways to get around and through the problems that were being thrown at them..."

Moreover, DHS and the Department of Defense (DOD) announced enhanced collaboration in dealing with cybersecurity threats Wednesday, McConnell noted. The National Security Agency (NSA) has unparalleled assets that the federal government could bring to bear in an appropriate way, with respect to laws and traditions, to boost cybersecurity nationally, he said.

Separately, Homeland Security Secretary Janet Napolitano issued a statement Wednesday explaining the increased collaboration between DHS and DOD as outlined in a memorandum of understanding signed by Defense Secretary Homeland Security Today - preparedness and security news Robert Gates and herself.

"With this memorandum of agreement, effective immediately, we are building a new framework between our departments to enhance operational coordination and joint program planning," Napolitano said. "It formalizes processes in which we work together to protect our nation's cyber networks and critical infrastructure, and increases the clarity and focus of our respective roles and responsibilities."

The agreement is intended to synchronize DHS and DOD efforts to support US cybersecurity. Under the agreement, a representative of NPPD goes to NSA to collaborate with DOD and serve as the DHS liaison to US Cyber Command. In addition, a representative of NSA goes to the NPPD National Cybersecurity and Communications Integration Center (NCCIC) to provide DHS with Defense perspective on cybersecurity measures and methods.

### **Financial incentives**

Other panel members emphasized that businesses must receive and recognize the appropriate incentives to cooperate with federal authorities.

Brandon Milhorn, minority staff director and chief counsel at the US Senate Committee on Homeland Security and Governmental Affairs, described how Sen. Susan Collins (R-Maine) worked to build incentives into pending legislation, the Protecting Cyberspace as a National Asset Act (S. 3480).

The act seeks to expand the capacity of the federal government to boost cybersecurity across sectors, gathering good information from the private sector, which must have freedom to decide which cybersecurity mechanisms work best, Milhorn described.

To provide the private sector with appropriate freedom to act, the Protecting Cyberspace Act only places mandates on companies dealing with covered critical infrastructure, where damage to systems or assets could lead to a regional or national catastrophe that costs lives or compromises national security, he continued.

Businesses have incentives to work with the federal government as they would receive liability protections for compliance, Milhorn remarked.

"We don't want to be in a situation like we were after 9/11 where the government came to service providers, asked those service providers to take certain steps to protect national security, and then when those programs were exposed, the industry was exposed to significant liability..." Milhorn commented.

Without a firm legislative foundation, the telecommunications industry was put in an untenable position when complying with federal orders to monitor suspected terrorist communications, he argued. The federal government had to step in after the fact to protect companies after they were faced with billions of dollars in lawsuits.

Michael Merritt, assistant director of the US Secret Service Office of Investigations, said companies also must realize the benefits of sharing information with law enforcement.

The Secret Service, for example, has been able to leverage its relationships with the private sector and academia to identify hackers and to protect propriety information.

Should companies join a Secret Service Electronic Crimes Task Force, they would benefit from information on current cyber attacks that would enable them to defend their networks, Merritt commented. The Secret Service shares attack info with all partners in the task forces, assisting them with identifying and stopping cyber criminals.

Companies therefore should trust law enforcement and be willing to share information, Merritt said, despite fears of a negative impact on a company's credibility, a drop in its stock value, or fears of a lawsuit when a company reveals it suffered a cyber attack.

Finally, Robert Fecteau, CIO at BAE Systems Information Technology, revealed that DHS was strengthening cooperation between the 16 sectors of critical infrastructure through the Information Technology Information Sharing and Analysis Center (IT-ISAC) and other sector ISACs.

Each ISAC is placing an analyst in the DHS NCCIC to increase cross-sector visibility, he said. In that way, the IT-ISAC could learn if companies participating in the WaterISAC, for example, are suffering from cyber attacks and share information to protect its members and deduce patterns in the attacks.