2006 Washington Security Summit

By Janelle Julien
Associate Editor, AIIM
July 25, 2006

WASHINGTON, DC— The International Spy Museum served as the clandestine backdrop for a meeting of the minds gathered by Xerox to discuss security threats presented by state-sponsored economic espionage and economic warfare.

Security is a priority for organizations and government agencies of all sizes. They must keep ahead of the growing number of security threats by protecting intellectual property through document security. A major vulnerability to an organization is the unprotected documents within. Proprietary information can fall into the wrong hands, which poses a threat not only an organization, but also to national security.

Xerox gathered a panel of experts to discuss the challenges organizations face today in the ongoing battle to protect critical information, which included:

- David Drab (Moderator), Principal of Information Content Security of Xerox Global Services. Before joining Xerox, Drab spent 32 years in law enforcement, 27 of which were with the FBI. His expertise includes economic espionage, foreign counterintelligence, terrorism, and organized crime.

- Dan Verton, author, vice president, and executive director of *Homeland Defense Media*, which publishes *Homeland Defense Journal* and *IT Security Magazine*. A former U.S. Marine Corps intelligence officer, he has written extensively on national security, the intelligence community, and national defense.

- Andrew Colarik, information security consultant, author, speaker, and inventor. He has over 25 years of experience utilizing computerized information systems and has a thorough knowledge of the foundations, architectures, and protocols of computer and Internet fundamentals and their associated vulnerabilities.

- Terry Gudaitis, Director of Open Source Monitoring Services for Science Applications International Corporation (SAIC). SAIC identifies information on the Internet that represents a threat, risk, or vulnerability to an organization's assets, employees, market share, stock price, or reputation. She became the first cyber-crime profiler in the commercial information security that provided a business differentiator for her incident response teams.

The overarching themes of the panel discussion were the lack of employee/employer loyalty, accountability, and understanding of technology as the vehicles for security threats. According to Colarik, "Digital security breaches occur because technology is not used properly to protect assets. Employees are an organizations greatest risk or asset."

Gudaitis also emphasized this point: "It's a changing workforce due to downsizing and outsourcing, which has decreased loyalty levels to zero. Today's employees don't care about the company's security."

Verton echoed the sentiments of the panel: "Internal threats come from everyday workers either with malicious intent or are law-abiding employees who discover ways to cheat security controls. Also, there is much hatred and anger over IT outsourcing. Disgruntled snitches make the best sources."

Is there too much monitoring? Gudaitis disagrees: "There's not nearly enough monitoring. Companies monitor inside the physical perimeter but ignore the outside. Companies lose interest in employees who have been terminated and don't keep tabs over smoking guns."

Colarik agrees, "There must be the establishment and maintenance of trust or else you have a long-term disaster in the making. It is recommended to change passwords for departed employees." He also advises handling remote access requests with extreme care, "There is no control over the home environment. If the information is non-sensitive, then it's OK; if the information is sensitive, then the answer is NO."

Concerning accountability, the panel all agreed that management should set the example. Gudaitis believes "a top-down management approach is necessary for accountability and the enforcement of consequences and behavior."

Verton said, "People aren't excused because of the actions of strategic employees [strategic IT, strategic receptionist]… the boardroom is usually excluded and protected, whereas managers are held accountable for their subordinates actions."

According to the 2005 Computer Security Institute/FBI Survey,

- It is estimated that as much as 50 percent of company computer security breaches are perpetrated by insiders.

- Unauthorized access is the second most significant contributor to computer crime losses, accounting for 24 percent of overall reported losses, showing a significant increase in average dollar loss from the previous year; and

- The average loss due to the theft of proprietary information more than doubled between 2004 and 2005.

Xerox has achieved ISO/IEC 27001* certification for its document imaging and hosted repository operations, which supports the standards set forth in The Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley, Gramm-Leach-Bliley Act, and FDA 21 CFR Part II.

**ISO/IEC 27001, a global industry standard created by the International Organization for Standardization and the International Electrotechnical Commission, validates service organizations that maintain a sound and secure information management system. Introduced in October 2005, the standard is an upgrade to the British Standards Institution's BS7799-2 certification.*