

INSIGHT

Xerox's 2006 Boston Security Summit Reinforces the Importance of Intellectual Assets in the Enterprise

Kwon Chin

IDC OPINION

Xerox held its first-ever security summit to illustrate the importance of intellectual assets to the enterprise, and how the need to protect these assets is more important than ever. In addition, Xerox highlighted its offerings to help ensure information security as well as potential future developments in this area. Key highlights of this event are:

- ☑ The computer revolution and the Internet have become vehicles not only for the creation of trade secret assets but also sources of risk for the security of such assets to include traditional documents.
 - ☑ The full extent of losses arising from intellectual property theft is not known; the estimate is that it is well into the billions of dollars.
 - ☑ The concept of a security perimeter has disappeared and as a result, companies are hemorrhaging information and knowledge; firms need to know where their data is at all times.
 - ☑ Xerox is able to offer unique technology, such as DataGlyphs, GlossMarks, and Correlation Marks, to help mitigate the loss of information.
-

IN THIS INSIGHT

This IDC Insight provides a review of the information presented at the Xerox's 2006 Boston Security Summit.

SITUATION OVERVIEW

On May 12, 2006, Xerox held its first-ever security summit for existing and prospective customers. At this event, Xerox held a panel discussion on the implications of security in the workplace and how, more than ever, this should be top of mind for businesses of all sizes.

The summit kicked off with Jim Joyce, Senior Vice President of Office Services for Xerox Global Services, providing a keynote to describe the current security environment and the issues he has personally seen corporations face. The term security has to include in its definition information security as it is the critical lifeblood

of a business today. While information is critical, there is no "silver bullet" to solve the problem of security. While an organization can't prevent information from leaking outside, what it can do is the following: expect, plan, protect, defend, inform, and increase awareness.

Joyce followed this point with a few anecdotes, the first being that most organizations don't know how many output devices they have in their enterprise, and in fact, most neither know where they are located or how many impressions their devices make a year. Some examples that were cited included an investment bank that made 2.8 billion impressions a year on its output devices on the client side of their business alone, a global chemical company that made 1.8 billion impressions a year, and a pharmaceutical company that made 850 million impressions a year. Clearly, with this many impressions being made in organizations, and organizations not knowing where these impressions are being generated or how they are controlled, an information leakage risk certainly exists and companies need to be aware of this.

Joyce also highlighted the fact that Xerox, while generally viewed as an MFP company, has performed over 350 large client consulting engagements centered on the output environment and potential risks it poses. Based on these engagements, Xerox has learned:

- The average output device age is 5.6 years, and in many enterprises, is 8 years old or older, predating Y2K, the Sarbanes-Oxley Act, the USA PATRIOT Act, and other such regulations that have emerged.
- The departmental output device is really a server.
- Most firms think about securing PCs but not securing the output devices.
- Network output is a target for espionage via capturing the bitstream.
- Compliance is an issue with respect to output.
- Printed output continues to be one of the most common means to conduct corporate espionage.
- Sixty percent of non-Xerox customers studied say they do not have confidence they can print or fax securely.

Joyce also provided a few specific examples to illustrate the nature of espionage that occurs at companies:

- A global adhesives company that had developed technology and business plans to enter the Asian markets discovered that there may have been an element of espionage occurring internally. Sure enough, it uncovered a mole who was stealing information for almost a decade.
- A large medical research center that was working on for the identification of the DNA model for Alzheimer's disease found that the research information was taken overseas by a researcher and given to a foreign brain and neurological center.

- ☒ A global energy conservation company that had created new research found that a disgruntled employee faxed this research to all of the company's competitors.

In each of these cases, documents were at the core of the espionage that occurred.

Security Q&A Panel

Dave Drab, principal with Xerox Global Services, led a panel discussion on critical information assets and how to protect them. Drab, a 27-year veteran with the FBI, investigated economic espionage matters and was on the team that arrested one of the first successfully prosecuted Al Qaeda members. He joined Xerox in 2002 to work on content and document management security. Also on the panel were:

- ☒ Dan Verton, Author and Vice President and Editor, Homeland Defense Journal
- ☒ Mark Halligan, Principal, Wolf & Katz LLC
- ☒ Craig Morford, Deputy Assistant U.S. Attorney

Before delving into the Q&A, Drab also cited other statistics, including a survey of 8,200 IT professionals in which respondents were generally in a reactive versus a proactive mode and only 37% of the respondents had any sort of information security plan in place.

Some of the key highlights from the Q&A panel are:

- ☒ While information is the new currency of the 21st century, the problem is that businesses don't think that way.
- ☒ The computer revolution and the Internet have become vehicles not only for the creation of trade secret assets but also for the theft and destruction of the assets.
- ☒ We are still depending on old accounting systems. In a new economy company, 80–90% of assets are intangible assets; even computers are leased. The oldest intellectual property right is trade secrets. The birth of every patent starts out as a trade secret.
- ☒ The problem with trade secret assets is that there is no patent protection on them. The moment trade secrets are disclosed to third party, the patent protection is gone. Corporate espionage is conducted in bars, first-class sections, and trade shows. The biggest losses are the inadvertent divulging of these assets to others.
- ☒ The full extent of losses arising from intellectual property theft is not known; the estimate is that it is well into the billions of dollars.
- ☒ Economic advantage is key; whoever gets to market first will succeed in the new international marketplace, and what the United States now brings to the table is information, not labor.

- ☒ As work technologies are escalating and evolving rapidly, it is increasingly difficult to distinguish the difference between the external and internal. Doors in and out of the enterprise now exist that didn't exist in the past.
- ☒ The average user is handling and managing information that makes it more vulnerable to not only viruses and worms but also to other threats as many of the worms exist purely to harvest information from the enterprise.
- ☒ Up to 80% of attacks on the enterprise are from insiders.
- ☒ A distinction must be made between those who are looking for economic gain in the company and the large portion of law-abiding, loyal employees who are unwillingly putting info at risk.
- ☒ The concept of a security perimeter has disappeared; firms need to know where their data is at all times as information is hemorrhaging without the firms' knowledge.
- ☒ In terms of external threats to the enterprise, in the past, employees were recruited to physically steal paper files from competitors. Now, however, physical access is no longer necessary as a hacker can sit at a keyboard and get access to a company's information.
- ☒ Large criminal enterprises in underdeveloped countries have arisen to provide virtual cybercrime and information espionage services to terrorists and to competitors of U.S. companies to penetrate their information repositories. Companies are now just beginning to sense the severity of this.
- ☒ It is extremely difficult to fly overseas to prosecute, especially in countries that lack corporate intellectual property protection legislation.
- ☒ National security data, customer data, and employee data is being lost a rapid rate, as 48-hour monitoring periods reveal. For example:
 - ☐ The average "superuser" can get around anti-Webmail tools.
 - ☐ A government healthcare organization saw 2,000+ HIPAA violations in 48 hours of monitoring.
 - ☐ A 48-hour snapshot of NASA uncovered an individual on the inside who was trying to figure out how to help al-Qaeda.
- ☒ When a security breach occurs, time is of the essence.
- ☒ There is a quandary around fortifying business, but IT professionals often get vilified for impeding business as well. Unfortunately, this is the situation in most enterprises today. One notion is setting up a data security council to meet regularly with all important groups in the company (sit-down meetings with business managers help them carry out their processes securely).
- ☒ Offshoring and outsourcing provide more entrée for economic espionage. While opening a subsidiary in China is economically attractive, it is also akin to saying goodbye to trade secrets as China does not have American-style law enforcement for intellectual property.

Xerox's Security Offerings

After the Q&A panel, Larry Kovnat, product security manager of the Xerox Office Group, spoke as to why Xerox was sponsoring this summit. The key message Kovnat provided was that while Xerox is regarded primarily a maker of MFPs, it was important for those in the audience to keep in mind that MFPs are sophisticated network citizens, and as such, while they offer plenty of benefits, there are also multiple securities vulnerabilities that can be exploited. As such, if there were a successful attack on one of these systems, they can be used as vehicles to harvest information on the network. Kovnat communicated that Xerox wants the equipment on a company's network to enhance its compliance plan; security is about much more than PCs and firewalls.

Kovnat went on to state that with the legislation and regulatory compliance policies and procedures in place, there must be common controls to address them, such as:

- Authentication of sender and receiver of personally identifiable information (PII)
- Audit trail of all transactions involving PII
- Use of encryption when sending data over an insecure medium (specifically the Internet)
- Office equipment with capabilities that support and enable compliance
- Information sent over a public medium being encrypted

Kovnat went into detail about how Xerox's devices are addressing the security risks and concerns in the output device requirement by citing such features as:

- Fax/network separation
- Image overwrite option
- Network authentication
- Scan-to-email risk and abuse
- Encryption
- Internal firewall
- Auditing controls
- Secure print
- Removable HD

Kovnat followed up with a description of common criteria and the positioning of Xerox's MFPs. Xerox is the only manufacturer that has sought and obtained certifications for its entire MFP line and all the corresponding subsystems; other manufacturers have pursued a security kit approach.

Afterward, Dr. Sophie Vandebroek, chief technology officer and president of Xerox Innovation Group, spoke on the security innovations currently under development in Xerox's global research labs globally to help eliminate the pain points of lost information. Vandebroek cited that Xerox invests \$1.7 billion dollars annually (with Fuji-Xerox) into research and development.

Vandebroek highlighted some of the technology that Xerox has developed to make paper more secure, including:

- DataGlyphs
- GlossMarks
- Correlation Marks
- Micro-Fonts

DataGlyphs, as defined by Xerox, is a two-dimensional symbology for encoding machine-readable data onto paper documents and other media. Used in conjunction with scanning, DataGlyph technology allows documents to carry information that is hidden in the gray patterns that can appear as backgrounds or images.

GlossMark technology is used to embed information such as date and name in the background gloss of output, and the glossmarks are created by the toner particles. Xerox believes this technology allows for true personalization of output, makes it difficult to counterfeit documents, and uses the gloss in an image for a purpose. GlossMark technology has already launched in Europe and Developing Markets Operations (DMO) but is not yet available in the United States.

Correlation Mark technology is also used to embed information in the document. However, the only way to see the embedded information is to possess the proper decoder overlay page. With this page, the user can see the embedded text and message hidden the document.

Micro-Font technology allows for ultrasmall type to hide data. With Micro-Font technology, 100 pages of normal text can be stored on a single 8.5 x 11in. page.

With respect to Xerox's view on the future of information security, some potential enhancements discussed by Vandebroek were:

- Embedding RFID in documents (in the cover page, etc.)
- Physically printing the RFIDs to lower costs
- Looking at "intelligent redaction" technology so when documents are stored or outsourced, the sensitive fields are hidden and can only be shown with the correct key

FUTURE OUTLOOK

Through the Xerox Security Summit, Xerox is attempting to raise the profile of output security in the enterprise. Although Xerox has been saddled with the image of being a "copier" company, through events like this, Xerox is clearly raising the profile of the firm to become a trusted partner in the output device environment as well as a leader in security and consulting services. With future summits planned for Washington, D.C., and Toronto, it is clear that Xerox is fully vested in educating the public on the security risks that exist in the enterprise and how they can be addressed. Whether or not companies become clients of Xerox's security features or purchase Xerox devices, those attending the event probably left with a newfound view on the importance of information security and the steps that need to be taken to protect the enterprise. In this sense, Xerox is clearly performing a public service by educating firms on the pervasive threat of losing intellectual assets.

Copyright Notice

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, telebriefings, and conferences. Visit www.idc.com to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit www.idc.com/offices. Please contact the IDC Hotline at 800.343.4952, ext. 7988 (or +1.508.988.7988) or sales@idc.com for information on applying the price of this document toward the purchase of an IDC service or for information on additional copies or Web rights.

Copyright 2006 IDC. Reproduction is forbidden unless authorized. All rights reserved.

Published Under Services: Hardcopy Peripherals: Document Solutions