

OSINFO - Open Sources Information

Crime, Intelligence, Terrorism, Foreign Affairs, Technology, Defence & Security

Unisys Identifies Five Security Issues Likely to Emerge Across Multiple Industries in 2008



Increased Use of Mobile Devices Will Pose New Security Risks and Challenges for IT Professionals; Further Convergence of Physical and IT Security Needed to Keep Pace with Evolving Security Threats

15 January 2008

14:00

BLUE BELL, Pa. - (BUSINESS WIRE) - Unisys Corporation (NYSE:UIS) announced today its security predictions for 2008. In the rapidly evolving world of corporate and government security, forecasting future risks and trends is essential to planning, preventing and managing risks that could compromise the integrity of an organization's assets. Emerging security threats, combined with the increased use of and dependence on new technologies, leave many corporate and government IT professionals with a degree of uncertainty in how to plan and forecast.

"Many organizations have a tendency to view security in the rear view mirror – scrambling to find a solution to a security problem after it's happened," said Tim Kelleher, vice president, Enterprise Security, Unisys.

"To combat new threats and to cater to the evolving demands of their end users, IT professionals must convince their organizations to treat security as a core business function - one that anticipates user demand, predicts future risks and develops workable solutions to potential security events."

To assist government organizations and corporations in preparing for and managing potential security threats in 2008, Unisys experts predict the five following trends in the coming year:

1.) Protecting data on mobile end point devices will demand more attention and become increasingly difficult

With the exploding use of mobile consumer devices (such as cell phones and personal digital assistants), organizations are scrambling to address security issues via passwords and other protective measures at log-in. By doing so, however, many enterprises miss the real threat. They neglect to look beyond the physical device and often fail to protect the data stored in the

device, which is not only valuable to owners but a growing target for criminals to commit identity fraud and theft.

Data protection is an increasing concern among consumers. In fact, the Unisys Security Index found that nearly 70 percent of Americans are extremely or very concerned about the unauthorized access or misuse of their personal information.

“Digital signatures and encryption are crucial to protecting data, but they must be woven into a holistic security plan that addresses issues such as whether and how the data can be transferred from one device to another,” Kelleher said.

“Without such a plan, an enterprise will find that the data on its mobile devices either are too vulnerable to potential breaches or so secure that they become inoperable. Striking a balance between the two is necessary to devise a secure solution that still allows the user to be productive.”

2.) Banks will face significant challenges in protecting consumers’ data and financial assets as more clients turn to mobile devices to conduct transactions

Mobile banking is gaining traction and will continue to emerge as a significant banking channel, with more than 35 percent of online banking households using mobile devices for financial transactions by 2010, according to a recent Celent report.(1) As this trend continues, security risks will increase.

This is particularly the case for mobile phones embedded with radio frequency identification and “near-field” chips, the latter of which enable transactions similar to gas station speed passes. Because of the design of near-field technology and the way in consumers use it, such devices could be open to attacks such as “phishing” (i.e., fake e-mail messages to lure accountholders to reveal personal data). Another threat is malicious code designed to bypass security technology, allowing unauthorized users to steal someone’s identity credentials.

Such e-banking attacks could wreak havoc on already shaky consumer confidence in the banking and financial sector, while also making banks vulnerable to increased insurance premiums as insurers seek to hold banks more accountable for security breaches. The Unisys Security Index found that 40 percent of Americans are extremely or very concerned with the security of banking or shopping online.

As financial institutions continue to grow their audiences for e-banking, they must better integrate business processes and solutions to prevent these fraudulent activities and consider new business models. Banks must build better alliances with telecommunications companies and share security knowledge for the benefit of their customers. Service providers also must build comprehensive, interactive consumer education programs about the risks and protections bank customers must take.

3.) Organizations will seek continued convergence of physical and electronic (i.e., IT) security measures for enhanced protection against **espionage**

The convergence of physical and electronic security will continue to drive new economic efficiencies into organizations while improving the safety and security of people, IT systems and mission-critical physical assets.

“Convergence is one of the most efficient and effective ways to keep pace with security threats that are most likely to inflict harm on the people, data and physical assets that comprise the lifeline of any corporation or government organization,” said Kelleher.

Ensuring the identity, authenticity and integrity of organizational assets, both physical and electronic, will require robust data fusion capabilities that integrate diverse sensory and remote monitoring technologies such as instant authentication, motion sensors, intelligent video applications, GPS, wireless environmental sensors and RFID. This convergence will continue to enable public and private sector organizations to manage and respond to risks that affect their physical and electronic borders, brands, identities, personnel, products and high-value assets.

As the global supply chain continues its expansion, 2008 will see greater use of converging security technologies to safeguard land borders and ports, protect sensitive data, and reduce opportunities for **espionage**. Organizations will integrate physical and IT security measures that, until now, largely had been kept separate.

Such integrated access control systems could include motion sensors to monitor grounds; access cards and biometric credentials to authenticate workers; and RFID tags, both to identify containers and their contents and reveal suspected breaches.

Other convergent applications that can help minimize threats to complex security challenges: Electronic e-pedigree that ensures the integrity of products such as pharmaceuticals, highly meshed wireless-enabled sensory networks for border and port security, and intelligent monitoring and surveillance applications.

4.) Public and private sector entities will pay more attention to paper and electronic records

The global economy is dependent on the efficient distribution of electronic and paper records within and between organizations. For example, in the United States alone, the payments industry is seeing double-digit monthly growth in the number of checks processed as electronic images. The Federal Reserve Bank today processes approximately 12.7 million electronic check items per day compared with approximately 25.3 million paper checks. Expectations are that by the end of 2008, the Federal Reserve will process 20.5 million electronic items per day compared with 13.5 million paper checks.

The growing use of electronic record exchanges creates fundamental security issues. For example, many individuals readily share critical personal or organizational data without thinking about the security ramifications that exists when a document is passed among multiple individuals.

“Many people would be surprised how often the wrong information ends up in the wrong hands because data is inappropriately shared, copied, printed or just forgotten on a portable drive or in a printer feed,” added Kelleher.

Kelleher predicts that in 2008, companies will be more diligent about setting more stringent controls over documents and data that are sent electronically or via U.S. mail. This is likely to result in greater focus on encrypting information on shared portable drives and discs and increased investment in enterprise rights management solutions. The latter enables content owners to encrypt sensitive data and control users’ ability to print, forward, copy or amend a document.

5.) Popular social networking sites will become increasingly vulnerable to privacy breaches

The broadening use and reach of Web2.0 technologies will increase the chances of a major privacy breach via social network sites such as MySpace, LinkedIn or Facebook. In 2007, a few of the major social networking sites experienced their first taste of privacy breaches, a trend that is likely to increase as many of these sites begin to connect to one another for information sharing purposes.

Peer-to-peer (P2P) networks create an array of security risks and vulnerabilities for end users. Unauthorized file shares, unintended duplication of personal e-mail and address books, data leakage, password and IM interception and installation of malware programs via P2P clients are just some of the risks that end users can experience.

"As these sites connect to one another, many will cross-reference a member's credentials. If a hacker can compromise one account, he could end up compromising many. And, because these sites are social in nature, the environment is conducive to divulging information – oftentimes, too much," Kelleher said.

P2P users can minimize risk by improving password complexity; implementing security measures such as personal firewalls, anti-spyware, anti-phishing features and up-to-date antivirus application; and installing the most current P2P client software, browsers and operating system patches and updates.

As technology evolves, end users will be able to minimize risk through trusted federated directory structures and stronger authentication and cryptographic applications.

Kelleher noted that while 2008 will bring opportunities to leverage the tremendous communication and collaboration capabilities of the Internet and Web-enabled applications, "the challenge, as always, will be balancing freedom of information exchange with protecting information and people's identity and privacy."

(1) "Corporate Mobile Banking: The Times They Are a-Changing," Nov. 8, 2007

About the Unisys Security Index

Conducted periodically throughout the year, the Unisys Security Index provides ongoing insights into the attitudes of global consumers on a wide range of security related issues. International Communications Research (ICR) conducted the survey in the United States and Europe; Newspoll conducted the research in Asia-Pacific.

About Unisys

Unisys is a worldwide information technology services and solutions company. We provide consulting, systems integration, outsourcing and infrastructure services, combined with powerful enterprise server technology. We specialize in helping clients use information to create efficient, secure business operations that allow them to achieve their business goals. Our consultants and industry experts work with clients to understand their business challenges and create greater visibility into critical linkages throughout their operations. For more information, visit www.unisys.com.

RELEASE NO.: 0115/8848

http://www.unisys.com/about_unisys/news_a_events/01158848.htm

Unisys is a registered trademark of Unisys Corporation. All other brands and products referenced herein are acknowledged to be trademarks or registered trademarks of their respective holders.

Unisys Lisa Meyer, 703-439-5887 lisa.meyer@unisys.com or Peppercom for Unisys Jenny Grendel, 212-931-6107 jgrendel@peppercom.com

Posted on Tuesday, January 15, 2008 at 20:51 by [PF](#) in [Security](#), [Technology](#), [ICT](#), [Analysis](#) | [Comments Off](#)

[View Printer Friendly Version](#)

[Email Article to Friend](#)



www.PowerStockTrades.com [Feedback - Ads by Google](#)



This work is licensed under a [Creative Commons License](#).