



Emerging Technologies and Associated Risks

October 2009

KPMG LLP



Contents

Overview	2
Wireless Security	3
Teleworking	4
Virtualization.....	5
Storage and Hand-held Devices	6
Location-aware Technologies	7
Social Networking	8
Voice over Internet Protocol (VoIP)	9
Splashtop	10
Software Asset Management Tools	11
Password Management	12
Record Retention and Litigation Support Solutions	13
XBRL – Extensive Business Reporting Language	14

Overview

As technology continues to advance, or users find new ways to use existing technology, new risks to companies emerge. Identifying ways to mitigate new/enhanced risks should be continuously reviewed and discussed with management. This presentation provides a brief overview of various topics and identifies the associated emerging technologies, the risks involved, and ways to potentially mitigate the risks.

From SC Magazine; Feb 2008 issue:



- **35%** of respondents felt the need to work around established security policies to get their job done.
- **63%** of respondents send work documents to personal e-mail addresses to access them from home.
- **87%** of respondents work remotely over VPN, personal or corporate Web mail.
- **56%** have accessed their work e-mail via public wireless hotspot, such as Starbuck's.
- **52%** access their work e-mail via public computer, such as a public library.
- **34%** have held a secured door open for someone at work who they did not recognize.

Source: *The Confessions survey: Office workers reveal everyday behavior...*, conducted by RSA, the security division of EMC, during October and November 2007 in Boston and Washington, DC.

Wireless Security

Brief Description

- The securing of mobile wireless computing devices and applications, and wireless network security as it impacts those portable computing devices. Higher bandwidth wireless options are becoming available to users such that proprietary company networks may be switched utilizing these networks.

Emerging Technologies

- WiMAX, NFC, ZigBee, Wireless broadband

Risks Involved

- Wireless networks are by default an open access point. Physical media does not protect them and any device that implements the same radio interface can potentially access the wireless network.
- Attackers can connect into the network from anywhere and from any distance within the power of the transmitter.
- Attackers are anonymous and, although a valid user can be pinpointed with good accuracy, an attacker can use directed antennas to target a selected victim.

Mitigating Controls

- Strong user access administration to prevent unauthorized access to the wireless network
- Additional security controls placed within the access points to prevent unauthorized access
- VLANs are in use on the wired network
- Additional assurance (i.e. Systrust, ISO17799) from the service provider of security of the wireless network

Note: This could be a potential cost reduction opportunity with the use of vendor-supplied network infrastructure.



Teleworking

Brief Description

- Accessing companies' resources from home and/or public hotspots is a growing trend.

Emerging Technologies

- Use of wireless public access points via home or restaurants (i.e. T-mobile, Sprint Broadband)

Risks Involved

- Malicious/Adware/Spyware software getting downloaded
- Exposure of confidential information via shoulder surfing
- Theft of computers and information contained within them

Mitigating Controls

- Access and usage policies that address the use of home office and hotspots
- Use of screen savers, privacy screens, and security cables



Virtualization

Brief Description

- A virtualized desktop infrastructure includes a thin operating system and a browser.

Emerging Technologies

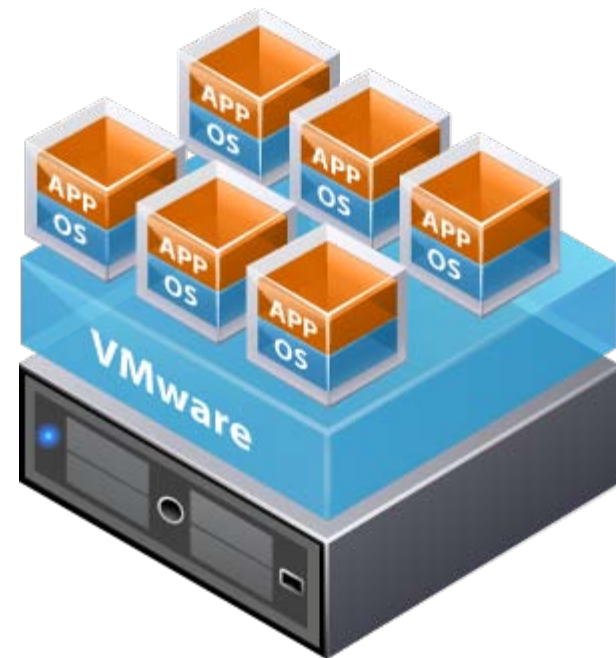
- Virtual desktop infrastructure, or VDI, speeds up bandwidth-intensive applications for remote workers and lets small IT staffs deploy new applications and perform reboots on demand quickly to large numbers of desktops in far-flung locales.
- VDI lowers operating expenses while providing an extra dose of security - users can't install software.

Risks Involved

- Significant back-end hardware and storage

Mitigating Controls

- Connection brokers
- Disk duplication to reduce the amount of storage needed to host VDI virtual machines



Storage and Hand-held Devices

Brief Description

- Thumb drives, backup drives, Blackberry, Treo, Smart Phones

Emerging Technologies

- Various providers, as listed above

Risks Involved

- Exposure of confidential data
- Privacy concerns
- Access to the network with improperly secured hand-held devices
- Ability to load malicious software on the computer
- Opening a corrupted file in a hand-held device can also infect the e-mail server

Mitigating Controls

- Access and usage policies that address storage and hand-held devices requirements
- Properly configured and secured hand-held devices which are procured thru the company
- The discontinuation of USB ports
- Use of PC backup techniques to discourage the use of thumb drives
- Remote wipe and kill features, which allow a network administrator to issue a remote "kill bits" order that wipes data and credentials from the device. Remote kill locks a device after a specified number of incorrect password entries



Location-aware Technologies

Brief Description

- Location Aware Technology is the use of GPS (global positioning system), Enhanced Observed Time Difference (EOTD), and other technologies in the cellular network and handset (or smart card/badge) to locate a mobile user.

Emerging Technologies

- Garmin, Tom Tom, Magellan

Risks Involved

- Privacy infringement

Mitigating Controls

- Policies that address the usage of Location Aware Technology
- Employee acknowledgement technology usage



Social Networking

Brief Description

- A Web technology once seen suitable only to consumers, which is now becoming more compelling for businesses

Emerging Technologies

- MySpace, Facebook, Linked-In, YouTube, Bebo, Orkut, Perfspot, Friendster, Neighborhood, Zope, etc.
- Web 2.0 or Enterprise Portal Systems, Microsoft's Share Point Server 2007



Risks Involved

- “Networking” can easily turn into “not working” and decreased employee productivity
- Locking the bandwidth and storage
- Employees may post or blog about sensitive information
- Potential legal liability
- Threat from spammers and hackers to trawl through social networking sites to steal personal or commercial data
- Exposure to malware
- Employees disclosing too much information, negative discussion about other employees, harassment, etc.
- Providing confidential information to potential hackers

Mitigating Controls

- Access and usage policies that address social networking requirements
- Monitoring mechanisms

Voice over Internet Protocol (VoIP)

Brief Description

- A fast-growing technology for voice communication over the Internet

Risks Involved

- Exposure of voice communications and the ability to “listen” in via telephone microphones
- Privacy of transmission and possible violation or disclosure of confidential information
- System service breakdown caused by outside hackers
- No service during power outage
- Locks bandwidth
- Exposure to malware

Mitigating Controls

- Encryption of communications
- Removal of implementation-related accounts and user ids
- Backup plan for power outages
- Turning on of additional security features within the VoIP software

Note: With proper controls, VoIP can reduce costs due to the elimination of duplicate voice networks.



Splashtop

Brief Description

- Allows you to enjoy instant access to commonly used functions like accessing the Internet, VoIP, and Web e-mailing without entering the OS

Emerging Technologies

- Splashtop Web Browser, Splashtop Music Player, Skype, Splashtop Photo Manager

Risks Involved

- Malicious/Adware/Spyware software getting downloaded since OS is still inactive (firewall and antivirus)

Mitigating Controls

- Access and usage policies that address use of Splashtop technology
- Monitoring mechanisms



Software Asset Management Tools

Brief Description

- More robust software asset management (SAM) tools are available to identify duplicate or unused licenses as well as identify where companies are out of compliance with existing agreements.

Emerging Technologies

- Microsoft SAM, Altiris, IBM Tivoli, LandDesk, ZENWorks, and HP
- Smaller vendors include Centennial Software, Integrity Software, and Sassafras Software

Risks Involved

- Financial exposure to unlicensed software
- Duplicate licenses
- Unused licenses
- Service interruption if existing licenses expire

Mitigating Controls

- Use of a software asset management tool
- Access and usage policies that address license of software

Note: Use of SAM tools can reduce costs due to the elimination of duplicate licenses as well as identification of additional needed licenses can offset litigation exposure.



Password Management

Brief Description

- Single Sign-on (SSO) is a mechanism whereby one action of authentication and authorization can give access to appropriate computers and systems without entering passwords multiple times.



Emerging Technologies

- Enterprise Single Sign-on, Web Single Sign-on, Federation (for Web applications, two technologies are growing – SAML and WS-Security)

Risks Involved

- A single password that unlocks/locks the entire enterprise is compromised
- SSO is more help to the user community than the security administrators of an enterprise with approximately 20 applications.

Mitigating Controls

- User access administration
- Security controls in place to monitor/prevent unauthorized access

Record Retention and Litigation Support Solutions

Brief Description

- With an increase in lawsuits, corporate investigations, and regulatory audits, electronic record retention and the burdensome litigation support is causing companies to look for supporting solutions to electronically index and analyze electronic files in order to meet the short deadlines set by the regulatory boards and law firms.



Emerging Technologies

- Electronic Discovery, iBlaze, WebBlaze, Casevault

Risks Involved

- Inability to address the regulatory requirements
- Increased cost of storage to retain all records

Mitigating Controls

- Define retention periods for electronic records
- Establish and follow a working electronic record archive policy
- Establish a security policy that defines the process to follow in case of any litigation

Note: This can also be a cost avoidance opportunity.

XBRL – Extensive Business Reporting Language

Brief Description

- XBRL can be viewed as a system of bar codes for financial statements. It allows companies to use nationally and internationally common “tags” to identify individual reporting concepts that exist in a corporate report. Information that is coded in this way can be instantly and accurately exchanged between systems. XBRL allows context to be communicated along with content.

Emerging Technologies

- Companies other than investment companies will be required to submit XBRL-formatted financial statements, notes, and financial-statement schedules based on a three-year phase-in schedule. The first phase-in period applies to domestic and foreign large accelerated filers that file financial statements presented in accordance with U.S. GAAP and have a worldwide public float above \$5 billion, beginning with the first quarterly report (or annual report for 20-F or 40-F filers) for fiscal periods ending on or after June 15, 2009.
- The SEC determined that XBRL-formatted financial information submissions initially will have limited liability. The limited liability provisions will be phased out over a two-year period for each company with complete termination of the limited liability provision on October 31, 2014.
- The SEC also adopted a rule requiring mutual funds to submit the risk/return summary sections of their prospectuses in XBRL format effective January 1, 2011.

Risks Involved

- Inaccurate mapping between source system and XBRL format
- Mapping tool is not validated resulting in inaccurate data

Mitigating Controls

- SDLC methodology to convert format





Questions