ARTICLE COURTESTY OF LEXICON SYSTEMS, LLC | +1 281.280.8106 | lexicon-systems.com

Balancing Business Needs and Information Security

We use smart phones and handheld devices to stay connected when out of the office and flash drives to take files on the road. We log onto wireless networks and routinely back up notebook computers onto small, portable hard drives. We export data from enterprise databases to spreadsheets for further analysis or reporting. We want information at hand 24/7 for decision support, yet the technologies that make it accessible can let sensitive information leave the organization. Information security, part of a growing strategic initiative called "data governance," is a top business priority.

by Jill Barson Gilbert

Jill Barson Gilbert, QEP, is president of Lexicon Systems, LLC. E-mail: jbgilbert@lexicon-systems.com.

A Fine Balance

Information technology (IT) lets us work and collaborate in ways that we could not have imagined just a few years ago. Networks, hardware, and software provide anytime, anywhere access and data portability. We use networks to deploy, access, and use information, software applications, and resources. The amount of information grows each year, and we extend access to users within and outside of our organizations. Good data governance requires increased diligence in protecting information. The challenge is to provide access to information, applications, and systems, while balancing the acceptable level of risk and optimizing costs (see Figure 1).

Enterprise information is a precious commodity that helps businesses gain competitive advantage. Likewise, IT can provide an advantage. As environment, health, and safety (EH&S) managers, as with other business functions, we must protect information assets from security vulnerabilities. We want to avoid threats such as e-discovery, business interruption, fines, and other legal actions that can result from information theft or loss.

Leaky Pipes

Think of information management as a system of reservoirs and pipes to deliver data when someone turns on the tap. Then consider that parts of the systems are not on a preventive maintenance schedule, so leaks may occur. Further, system users may fill a "to-go cup" with some of the information. Most organizations suffer from "data leakage," much of it unintentional. Data leakage can occur when notebook computers, smart phones, and other portable gadgets are lost or stolen. Data leakage can result from transporting data on CDs, flash drives, and portable hard drives or transposing data from one system to another. Portable data storage—particularly unsecured devices, opens the door to e-discovery (see *IT Insight* "E-Discovery Rules Reach Beyond Litigation," *EM* August 2007, p. 24).

Transparency

Thousands of internal and external EH&S compliance requirements call for good data governance—that is, managing information from cradle to grave, to put it in terms that EH&S professionals understand. We must know where the information resides, who has access to it, who modifies it and when, and what is reported. We strive for total data transparency (i.e., a single version of the truth). Common practices like using spreadsheets and one-off databases, using local hard drives, portable hard drives, and flash drives defeat transparency.

Potential business risk from data leakage makes a good case for using secure enterprise software. Information resides in a single database armed with security, backup, and recovery measures. People who need to access the information are issued a user ID and password. This works well, until someone decides to export data from the enterprise application to a spreadsheet. With today's robust ad hoc reporting tools and dashboards, this should not be necessary.

E-mail, Internet, and the World Wide Web

A 2005 study by research company IDC found that Web browsing is the single largest threat to information security. An EH&S professional's daily routine includes the Internet. We try to access a Web site, only to have it blocked. We find an article and can view, but not download it. As long as software contains security vulnerabilities, hackers will continue to generate malware. As viruses, Trojans, and other "malware" make enterprise information vulnerable to theft or attack, we have security software in place.

Keeping up with malware—generally conveyed via e-mail, the Internet, and the World Wide Web—is an uphill struggle. An entire industry exists, whose purpose is to identify malware, write programs to combat it, and distribute malware databases daily. Computer Associates, McAfee, and Symantec are some of the vendors who combat malware.

Until recently, the chief method to address the issue was to "blacklist" identified threats. This reactive approach has limitations; its effectiveness depends on identifying the malware before it invades computers and networks. Today, several vendors sell "whitelisting" software that takes a proactive approach (see sidebar "Malware 101" opposite).

Data Governance Helps Manage Risk

Sound data governance is the best way to manage risk associated with information. Organizations must develop, implement, and enforce data governance policies and procedures. They must educate staff—particularly those who access the information—about information access and security. And organizations must keep physical security, hardware, and software controls up to date. It does not matter how good your information security solutions are, unless they are active, up-to-date, and their use is enforced.

The Information Age and its technical capabilities have inherent risks. EH&S professionals must implement and enforce data governance policies and procedures to manage these risks, while balancing the needs of different stakeholders to access and share information. **em**

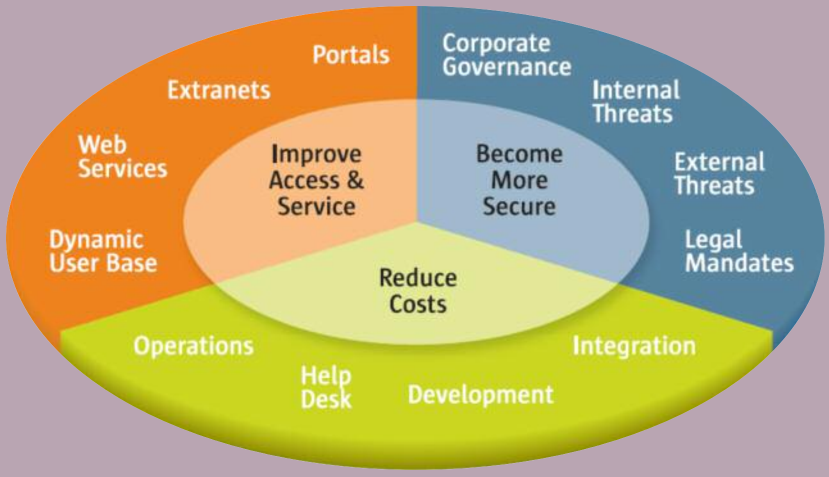

Figure 1. IT must address multiple, often conflicting, business goals.

Source: Sun Microsystems Inc., The Complete Buyer's Guide for Identity Management, October 2008.

Malware 101

Malware is not defective software, but software developed for malicious purposes. Here are a few common terms:

Malware: short for malicious software, a program or file designed to damage or disrupt a system, such as a virus, worm, or a Trojan horse. A general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code, computer viruses, worms, Trojan horses, most rootkits, spyware, dishonest adware, crimeware, and other malicious and unwanted software.

Computer virus (virus): a computer program that can copy itself and infect a computer without permission or knowledge of the user. Viruses usually corrupt or modify files on a targeted computer.

Trojan horse (Trojan): malware that appears to perform a desirable function but, in fact, performs undisclosed malicious functions. A worm or a virus may be a Trojan horse.

Computer worm (worm): a self-replicating computer program that uses a network to send copies of itself to other computers on the network, possible without user intervention. A worm does not need to attach itself to an existing program and usually causes harm to the network, if only by consuming bandwidth.

Antivirus software: tracks and quarantines harmful objects based upon blacklisting and active scanning for known threats and suspicious behavior.

Blacklisting: an IT security approach where a "black list" identifies banned applications and other executable programs.

Whitelisting: an IT security approach where a "white list" identifies safe applications and executables.