Breaching Your Walls of Defense
Strategize the plan to ensure real security of electronic data
By Daryl L. Thompson

As vital, confidential documents containing sensitive data are converted to an electronic format, its accessibility and mobility are primary concerns of security. With many risk factors, including hackers, third-party partners and employees, organizations need to collaboratively strategize their security measures to safeguard all vital information.

Your business data is at risk. In fact, the electronic data records that document an organization's transactions, clients and proprietary information are very much at risk of being breached. These data breaches are unauthorized disclosures that compromise the security, confidentiality and integrity of proprietary information. Moreover, the high volume of reported security breaches this year at businesses, government institutions, college campuses and other organizations indicates that risk exists for every establishment, regardless of its size or mission.

Such data breaches can be caused by hackers, business employees and third-party partners, located halfway around the world or sitting in the very next office cubicle. These perpetrators may or may not have criminal intentions, but their motivations are largely irrelevant. Data breaches, ultimately, harm an organization's capacity to effectively deliver quality services. As a matter of survival, businesses must take proactive action to ensure that their critical records are private and secure.

Record Security and Privacy

Most organizations define the life cycle of electronic records, including how records are created, retained and, ultimately, discarded. Electronic records are typically stored within an organization's computer network on a file or application server and in an off-site archival storage. Many businesses also determine how these electronic records are accessed. Records can be accessed by employees, third-party partners, clients and even other computers. Prior to accessing a record, users must present unique identifying credentials such as a password, a token, certificate authority or even a fingerprint. Once credentials are accepted, users are authorized to access records, but only for specific actions such as to review, modify, copy or print. Ideally, users should only be permitted to access the minimum set of records required for them to complete their work. Such authorizations should be updated as records progress through their life cycle as users change work assignments, third-party partner's contracts terminate and when clients are no longer receiving service from the organization. Record privacy, therefore, is achieved when an organization has knowledge and control over the users who are authorized to access records and their associated actions. In regards to privacy, records are considered confidential, only available to authorized and valid users. When record privacy is violated, security breaches occur.

Threats to Record Privacy

Record privacy threats originate from billions of sources with just as many distinguishing characteristics.

Hackers attempt to gain unauthorized access to an organization's computer network. Their attempts are motivated by a desire to control computer resources for entertainment purposes or for criminal activity. Hackers can be anyone from children, executing scripts downloaded from a hacking website, to organized criminal gangs. For example, in January, 2006, the state of Rhode Island was forced to take down its online vehicle registration system after hackers stole user information, including credit card numbers.

An organization's third-party partners, typically, have temporary restricted access to their partner's computer network. Malicious partners can manipulate their user credentials to gain access to confidential records and other sensitive information, such as when a Blue Cross and Blue Shield contractor, during the first quarter of 2006, sent names and the Social Security numbers of employees and vendors to his/her home computer.

Business employees either accidentally or consciously misuse confidential records that are in violation of their organization's security policy. Employees have the most knowledge regarding their organization's computer operations and, therefore, pose the biggest threat. In fact, in May, 2006, a burglar stole a laptop and external hard drive from a United States Department of Veterans Affairs analyst's home. The laptop and hard drive contained the personal data records of 27 million veterans and their families, including names, birth dates and Social Security numbers. Over a period of three years, the analyst had been downloading records in order to work, out of hours, at home. However, the analyst's actions were in direct violation of VA security policies. Moreover, both the laptop and hard drive were unprotected by passwords or encryption.

Hacker Tools and Methods

A hacker's objective is to obtain access and control of an organization's computer network and resources. Hackers accomplish these goals by utilizing a variety of methods and tools to gather information, impersonate valid users and damage the network. Furthermore, hackers perform information gathering activities to document computer network configurations, operating systems and software applications. Network analysis tools are used to map out an organization's computer usage patterns. Such proprietary information is gathered through traditional corporate espionage activities such as searching an organization's dumpsters, eavesdropping on lunchtime conversations and surreptitiously looking over an employee's shoulder as he or she works. However, access to an organization's computer network is often achieved through password cracking. Hackers utilize password cracking software to generate valid passwords and then, break in to the computer network.

Computer software applications and operating systems have vulnerabilities that hackers exploit with malware, which is software that is designed to infiltrate and damage computer systems and includes computer viruses, worms and spyware. These flaws are typically programming errors that vendors attempt to regularly identify and patch. Effectively, there is a race between vendors and hackers in fixing and exploiting these vulnerabilities. Hackers also spread malware through seemingly legitimate emails and instant messages. These messages, typically, originate from valid email addresses. But opening the message attachments or web links enable the loading of malware onto the computer. From this initial contact, a whole office network can become infected. Thus, everyone is a target of hackers. Small businesses are as likely to be attacked as large enterprises. There is no one-size-fixes-all solution that protects an organization 100%. Achieving record privacy requires an ongoing security management process.

Security Management

An organization's computer network should only be used for business purposes. Security management documents organizational policies and procedures for authorized usage of computer resources. Thus, a security policy establishes organizational standards for managing, protecting and distributing sensitive information, while access controls implement the security policy. These access controls can be administrative, technical and physical.

Administrative controls are procedures put in place supporting authorized usage of computers. This includes the employee's roles and responsibilities for record access, Internet surfing and the handling of proprietary information. Each employee and third-party partner must be trained to comply with the organization's administrative controls.

Technical controls are software tools used to restrict access to organizational resources.

- Access lists are sets of data associated with a file, directory or other network resource that defines the permission that users, groups, processes or devices have for accessing it.
- Email filtering software prevents confidential information from being sent outside the organization.
- Encryption is a process of obscuring file contents to make it unreadable without special knowledge.
- Antivirus software attempts to identify, thwart and eliminate malware.
- Firewalls are software and hardware barriers designed to prevent unauthorized or unwanted communications between computer networks.
- Physical controls are locks, guards, alarms and any other controls that restrict individual access into and within a facility.

Security Management Process

The security management process consists of the following ongoing steps:

Risk assessments identify critical business records, discover threats to record privacy and estimate costs to the organization if the threat occurs. Risks are ranked by cost and probability. The highest ranking risks are addressed through the identification and implementation of access controls. Risk assessment, specifically, targets “gaps” between an organization’s security policies and real life organizational practices. These gaps represent avenues through which unauthorized record access can occur. When conducting risk assessment, there should be representation from the entire organization. The IT department may understand the best methods for implementing technical controls, but the business operations and record management personnel actually define the circumstances under which users are authorized to access records. Organizations should walk through record usage scenarios that take into account employee work habits, changes in work assignments and record life cycles.

Security control implementation involves selecting combinations of administrative, physical and technical controls to reduce risk. Employees are the most powerful security management asset. Proper employee training can go a long way towards ensuring record security.

Monitoring and testing focuses on ensuring that the implemented controls reduce risk as expected. Monitoring and testing are also good practices for evaluating the quality of technical controls.

Auditing and improvement: the organization should regularly meet to discuss security standing, actively identify new security risks and update the organization’s security policy.

Daryl L. Thompson is founder of Thompson Network Consulting, LLC. He has 15 years of experience in the data networking industry, implementing secure networking solutions for businesses of all sizes. For more info, please visit www.thompsnet.com or email darylthompson@thompsnet.com.