

November 15, 2000

Lack of e-mail security imperils assets

Holes in messaging systems open doors to internal and external threats

The whirlwind pace of modern business has made electronic mail the preferred method of communication. Analysts report that corporate usage of the Internet is currently doubling each year, and companies are predicted to send more than 200 billion e-mails in 2004. While many organizations have embraced the productivity gains afforded by this instant communication medium, a smaller percentage has done so with a focus on security issues.

The media regularly publish stories on security flaws uncovered in popular messaging software, yet consumers pay little heed. Despite privacy concerns raised over Carnivore, the Federal Bureau of Investigation's electronic surveillance software, less than one percent of e-mail messages is encrypted. Sending e-mail in plain text exposes the information within to far greater threats than the legitimate monitoring performed by the federal government for law enforcement purposes. Several companies offer encryption software free of charge on the Internet, but the added step is more than most users are willing to take, even with messages of a confidential nature, such as legal correspondence.

This edition of The Lipman Report examines the current state of e-mail security. What threats do organizations face, and what are the ramifications of such breaches? What steps can companies take to protect their information assets and their reputations? A thorough understanding of the issues involved can safeguard companies from the dangers that lurk—internally and externally—in the world of electronic communication.

In terms of privacy, e-mail users have long been cautioned to regard their messages as the electronic equivalent of postcards. This standard, however, does not always prove practical in corporate communication; the potential efficiency gains are far too tempting. As a result, companies need to invest in security measures to protect their proprietary information.

A typical e-mail message passes through several different servers during the course of transmission, possibly leaving a copy of itself behind on each system. Any one of these copies can be retrieved, either by a system administrator or by a hacker. In addition, a tool known as a "packet sniffer"

has the capability of capturing e-mail while in transit, acting as the software equivalent of a wiretap. This type of utility is legitimately used to enable administrators to analyze and read electrical signals for diagnostic purposes, although hackers and industrial spies can also employ them for malicious purposes. This threat decreases significantly for e-mail messages confined to a secure corporate network. An increasing number of workers, however, are using other avenues of communication for greater convenience and perceived privacy.

Perils of electronic communication

Unregulated e-mail usage presents a wide array of risks to organizations, ranging from loss of confidential information and productivity declines to litigation costs from the transmission of inappropriate content through the corporate messaging system.

Trade secret theft ranks as a primary information security concern—and rightly so. Studies indicate that economic espionage costs the U.S. economy \$2 billion per month, with e-mail playing a prominent role in several lawsuits involving theft of proprietary data. The new technology makes it all too easy for an employee to send a sensitive document to someone outside the organization—as one information systems manager discovered when he received a message containing proprietary information intended for an outside recipient. Sometimes, information breaches occur by accident. Such was the case earlier this year, when a teenager in England received approximately 250 messages meant for the British Ministry of Defense, one of which carried the warning: "This is intended for the addressee only and may contain privileged information."

A 1999 study revealed that 31 percent of Internet e-mail presents a potential threat to proprietary data, employee productivity and corporate messaging networks. The analysis, which involved

(continued on next page)

Lack of e-mail security imperils assets

Holes in messaging systems open doors to internal and external threats

(continued from preceding page)

surveillance of numerous corporate e-mail systems for a minimum of one week, uncovered the following data:

- 10 percent of all e-mail surveyed constituted spam, or electronic junk mail;
- 9 percent disclosed proprietary data or violated the company's communication policies;
- 4 percent contained bulk mail;
- 4 percent contained profanities;
- 2 percent contained jokes; and
- 2 percent contained viruses.

These numbers translate into quantifiable losses for companies. According to one analysis, for instance, an organization that employs 5,000 people can suffer productivity losses of more than \$12,000 a day from employees wading through spam and other types of bulk e-mail.

Earlier this year, the now-infamous "Love Bug" virus ravaged corporate messaging servers around the globe, serving as a painful reminder of the need for e-mail and virus security. Various sources estimated the total costs in damage and downtime between \$700 million and \$15 billion, with copycat viruses producing billions more in damages during the weeks that followed. Just last month, a computer security software group reported finding more than 2.8 million files infected with the "Love Bug" virus on its North American customers' systems in the previous 30-day period.

Information security experts predict that such e-mail-borne viruses will only become more virulent in the future. These increasingly dangerous payloads may lie dormant on infected systems, waiting for certain conditions before they strike. In a worst-case scenario, these viruses may be programmed to search systems for specific files and then mail them to a predetermined address. Already, reports have emerged of hackers infil-

trating corporations with Trojan horses—viruses disguised in seemingly benign attachments, such as text or graphics files.

Yet another threat comes from spoofing, in which one party assumes the identity of another without consent. The dangers of e-mail spoofing are exacerbated by the ease with which it can be executed; for instance, an employee can simply walk up to an unattended computer and send e-mail under the user identity of the active account. Even more alarming, research has shown that nearly three-quarters of corporate e-mail users would respond to an executive's request for confidential information without verifying the authenticity of the demand.

A global electronics corporation experienced a shutdown of its e-mail network from a massive spoof/spam attack. An irate customer, claiming to represent attorneys for the electronics organization, sent thousands of e-mails that accused the company of engaging in illegal activities, including hacking. The firm was subsequently assaulted with a flood of angry e-mail responses, which peaked at 10,000 messages per day. Although the organization was innocent, the attack produced losses through business interruption, if not also from reputation damage.

Security strategies for e-mail

Companies cannot eliminate the vulnerabilities inherent in electronic communication, but they can drastically reduce their risk exposure by implementing the following strategies:

Establish a corporate e-mail policy. To help protect against common e-mail abuses, organizations need to develop a written code of conduct addressing the use of electronic mail. Such a code needs to be brief, yet detailed—clearly spelling out what types of e-mail activity are acceptable, as well as which are prohibited. Employees are more likely to adhere to a simple code consisting of several straightforward bullet points, rather than a 10-page booklet.

The policy should also address the use of Internet-based e-mail. The convenience of such e-mail services can tempt executives to direct their electronic correspondence to these easily accessible accounts, enabling them to bypass network security measures viewed as cumbersome. While Internet-based e-mail services can serve legitimate business purposes, a comprehensive policy should address appropriate uses for such accounts to head off a potential security breach.

In addition, the code of conduct needs to establish guidelines regarding unattended computers. Studies have shown that the majority of security breaches result from insider abuse. While a hacker or industrial spy might attempt to retrieve sensitive e-mails from a shared server, a more likely scenario involves a co-worker walking up to an unattended computer and simply reading the absent user's mail. Lax controls in this area can also contribute to spoofing.

Simply having an e-mail policy is inadequate. As part of the information security program, organizations need to educate employees on the electronic code of conduct, ensuring that they understand their responsibilities when using the company's electronic assets. Many organizations incorporate such policies in the employee handbook or in the firm's code of ethics. This policy can also appear as part of the corporate log-in screen; it can be posted on a card near the computer terminal, or framed and displayed in a conspicuous area. Companies can use any one or a combination of these options to communicate such a policy. Doing so makes the policy an integral, visible component of daily operations and sets the tone that security is part of the corporate culture. This message, however, is only conveyed when the policy includes enforceable consequences for violations.

Employ encryption technology. Encryption provides the greatest protection against an unintended party intercepting sensitive information. Even

if an unauthorized user opened the message, he or she would be unable to decipher the contents without the appropriate key. The market offers several good, relatively inexpensive encryption programs, making this security measure highly affordable. In implementing encryption, organizations and individuals need to keep in mind that encryption simply shields e-mail messages from prying eyes. Encryption does not guarantee the identity of the sender, a process known as authentication, nor does it guarantee the safety of the contents.

Some popular encryption programs use digital signatures, which provide some level of authentication, but they require a certain degree of trust between the involved parties. Companies that transmit ultra-sensitive data should invest in more sophisticated means of user authentication, such as biometric devices or smart cards; they can also use a third-party certification authority to verify the identity of the correspondence participants.

At the same time, encrypted e-mail still needs to pass through a virus scanner to make sure a known virus does not lurk within the secured message. Even if the sender is a trusted contact, recipients need to sequester decrypted attachments and analyze them with an up-to-date anti-virus utility before executing any program files or opening a document that may contain macros. Virus scanning can also be accomplished at the firewall in organizations that use corporate signing keys. These master keys enable networks to open encrypted e-mail for filtering and scanning purposes, allowing the identification of potential viruses before they reach internal systems.

Monitor e-mail content. To ensure compliance with the corporate e-mail policy, experts recommend the use of content filters. Network administrators can customize these tools to monitor or block messages containing key words identifying confidential data. Organizations also use

(continued on next page)

Lack of e-mail security imperils assets

Holes in messaging systems open doors to internal and external threats

(continued from preceding page)

such programs to prevent the transmission of offensive material, spam and large video or graphics files. These filters can be programmed to respond to questionable message content in different ways: they can notify network administrators upon encountering messages with suspicious contents, or they can return suspect messages to the senders, accompanied by a notice of non-compliance with the corporate e-mail policy. Content filtering software protects both the interests of the employer and the privacy of the employees, within the boundaries of the organization's e-mail usage guidelines. These programs can also be used to monitor employee Internet usage, denying access to sites that may contain questionable material that violates the corporate ethics policy or general business guidelines.

In addition, filtering software can identify and block spam, freeing network resources and contributing to increased productivity. This capability also makes such software an important defense against viruses and Trojan horses, which pose one of the greatest dangers to computer networks. According to a recent survey of information security professionals, 80 percent of the almost 2,000 respondents report experiencing virus infections during the previous 12 months. Anti-virus programs can often detect even unknown viruses by identifying the self-replicating feature of the code, but unknown Trojan horses may slip through virus scanners by virtue of their disguise. Network filters, however, can bar their entry because of shared characteristics with spam.

Recent litigation has provided companies with even more compelling reasons to monitor employee e-mail. An energy company paid \$2.2 million to settle a lawsuit filed by a female employee who received a sexist e-mail message through the corporate messaging system. Last year, a British organization paid dam-

ages of more than £100,000, or \$150,000, after the High Court ruled that a 1997 e-mail contained libelous charges about a competitor. Messages sent through the corporate e-mail system are tantamount to letters on company letterhead, a fact that should make employees think twice about the content of their e-mail even as it drives many employers to practice e-mail surveillance.

Like so many other advances in the Information Age, electronic messaging systems present a double-edged sword in the world of corporate communication. Organizations must weigh the opportunity for instant, convenient communication against such potential risks as loss of proprietary information, virus introduction and decreased productivity, to name a few. Willingness to embrace this new technology without committing appropriate resources to information security has already cost companies countless millions, if not billions, of dollars worldwide, and the stakes continue to rise in today's ultra-competitive marketplace.

Effective e-mail security begins with a firm commitment from management, detailed in a written policy that is communicated to all employees. Educating employees on the principles within the policy will help make information security an accepted element of the corporate culture and encourage adherence to the established guidelines. At the same time, companies must have a means of monitoring compliance and enforcing the policy on a fair, consistent basis. Inadequate e-mail security can impact the bottom line through decreased performance at the very least; at its worst, it can destroy shareholder and customer confidence. Few businesses can afford the risk.



The Lipman Report Editors