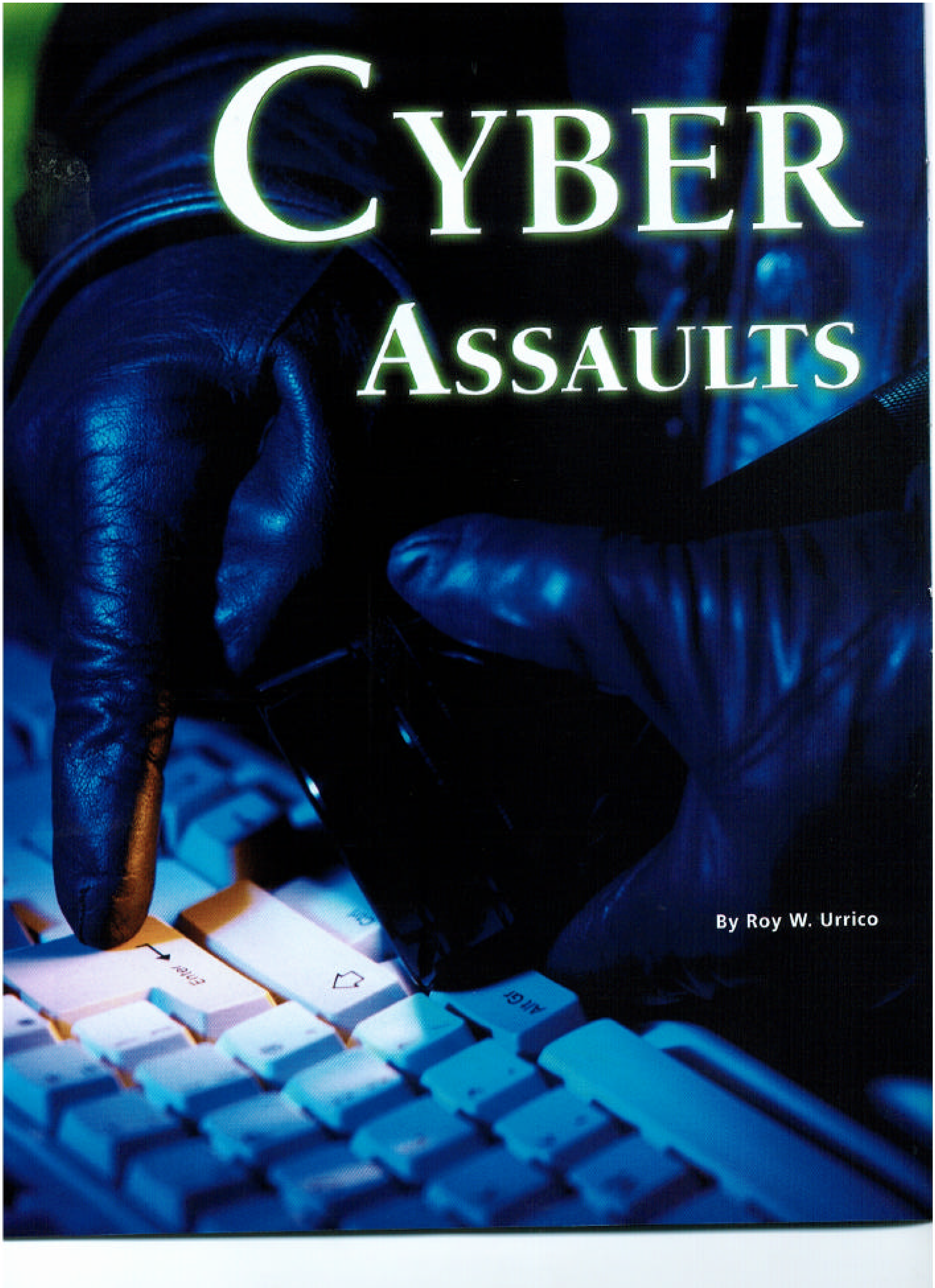
CYBER ASSAULTS



By Roy W. Urrico

Steps you can take to protect confidential information from hackers and other criminals.

The financial services industry, as well as the rest of American commerce, is under assault from cyber-terrorists intent on disrupting business. Despite greater protection and detection efforts, the number of security transgressions continues to rise dramatically.

The U.S. Department of Homeland Security reports that malicious code incidents, for example, have grown significantly, going from none reported in all of 1999 to 880,167 in just one month (June 2004). Meanwhile, the number of computer reconnaissance activities—hackers probing for chinks in security systems—climbed from just 222 in 1999 to an astonishing 54,290,346 reported in June 2004 alone.

The extreme rise in reconnaissance activity "demonstrates the need for intrusion detection and prevention systems," says Joe Lima of IS Audits in Macon, Ga., which specializes in information service management.

Security weaknesses

This is especially true at financial institutions. "Electronic vaults have their doors open to breakdowns in business processes and also to information security exposures," explains Guillermo Kopp, director of financial services strategies and IT investments for the TowerGroup in Needham, Mass., in his report "FSI Information Security: Can Customers Take Their Data To The Bank?"

These vulnerabilities surface because of a complex assortment of financial business operations and information technology that has complicated the security situation. "The major challenges financial institutions have are that their information infrastructures have grown more complex…the increase in sophistication has come at the cost of controlling information access," observes Andrew Greenawalt, chief technology officer for Perimeter Internetworking in Trumbull, Conn., which concentrates on the network defense needs of community financial institutions.

A 2003 CSI/FBI study points out that the highest number of attacks (82 percent) come from independent hackers and disgruntled employees (77 percent). Eighty percent of the threat is from the Internet.

"Directors are often shocked when they learn how vulnerable their systems are, and how they assist hackers in propagating their crimes against privacy," points out Jack Malinowski, chief technology officer and chief operating officer of Benchmark Technology Group in Alpharetta, Ga., which provides branch technology solutions for financial services institutions. He adds that these attacks are varied and include such nuisances as:

■ Denial of service: Web sites, e-mail, Internet applications and other services become unavailable to customers when financial institutions are too busy handling requests from malicious users or programs. "To the customer it looks as if your server is down."

■ Trojans and spyware: Web sites compromised by "malware" could endanger customers since access to applications, forms, files and even just keystrokes can be easily copied and sent to a hacker when customers access these services.

■ Network security: Misconfigured, outdated or compromised firewalls can let attackers jump from an external Web site to your production network.

"The greatest and most costly security threats faced by financial institutions on a daily basis are attacks on electronic services," says Malinowski. He says that these attacks cost the industry mega-millions every year in terms of stolen bandwidth, storage capacity, computing power, system performance and staffing.

In addition, because flaws in internal security and controls cause operational losses, financial services institutions are writing off billions of dollars annually due to failed transactions, defalcations and operational errors, reports the TowerGroup.

Greenawalt points out that many financial institutions that have a level of sophistication regarding traditional lines, such as protecting what is in the vault and cash drawers, are naive when in comes to electronic hazards. "Very few have visible intrusion detections measures in place," he explains. "Institutions need to be looking at this problem with the same critical eye that they look at traditional threats."

Sometimes organizations unwittingly expose their customers, observes Mark DeBellis, president of the Financial Services Division for PSB-The Marketing Supersource, an end-to-end marketing service provider. On at least one occasion, PSB has received mailing lists for a financial institution's market-

fyi…

Some common security weaknesses:

- Lack of awareness
- Employee apathy
- Weak workstation access controls
- Always-on Internet access
- Internet downloads
- Little or no incident reporting
- Inadequate detection responses planning and testing
- Wireless networking
- Unrestricted third-party vendor access

—list by Joe Lima of IS Audits

ing campaign complete with the names, addresses and Social Security numbers of that institution's customers.

That is an extreme example, but he suggests that those dealing with confidential information, such as marketing directors, should "create a mental firewall" and strip out unnecessary data when outsourcing services or engaging a third party. He also suggests encrypting and password protecting transmitted data.

Also, do not send the password in an e-mail with the encrypted information; send it separately.

Customer awareness

The TowerGroup reports that threats to information security are a primary factor that undermines customer trust in online channels for financial services. According to the Internet Crime Complaint Center, there were 120,000 complaints in 2003 (up from 48,252 in 2002), and Federal Trade Commission statistics show that there were 166,617 consumer fraud reports in 2003 (up from 110,288 in 2002).

"Even though we are employing more antivirus software, we are not discouraging [hackers] from trying," says Lima.

However, the Web is not the only threat. Although 42 percent of all fraud is identity theft, only 3 percent comes from the Internet, explains Lima. ID theft primarily occurs from lifted wallets and purses, stolen mail, dumpster diving, or from information obtained from business or personal records, information brokers or through pretext calling.

"The whole information lifecycle needs to be protected, including documents to be shredded," remarks Lima. (How often is the box containing paper to be recycled spilling over or left unattended overnight at your credit union?)

This elevated attention to security and personal privacy is triggering tighter provisions for curbing fraud, fending off terrorist threats and preventing an epidemic of identity theft. Compromised financial institutions, suggests the TowerGroup, may incur liabilities in terms of customers, prospects and other intangible costs arising from any fraudulent use of customer information, in addition to the direct financial exposure. Networked services environments necessitate dependable, end-to-end security integration and authentication based on sensitive personal data.

Credit unions, observes Lima, "have cornered the market on this idea of trust" but that trust could be dampened if information becomes compromised to the point that it ruins a credit union's standing with its members.

At the same time, government mandates call for safeguards to preserve the privacy of personal data that customers entrust to their financial institution. "The Gramm-Leach-Bliley Act requires financial institutions to have safeguards in place and to prove they are working," says Lima. "All of their records have to be protected."

Online Resources

Digital Defense Inc.
www.digitaldefense.net

Kryptec.net.
www.kryptec.net

Perimeter Internetworking
www.perimeterco.com

Xacta Corp.
www.xacta.com

How to protect systems

An ounce of prevention is worth a pound of cure goes the old adage, but for credit unions the key is utilizing both defense and discovery tools. Some financial institutions are utilizing better detection techniques for increased resiliency, states Kopp. These creative software and hardware tools operate within the confines of an institution's firewalls and address many aspects of the security spectrum. This includes monitoring, enforcing and auditing to capture online and internal transactions and zero in on significant events.

"If you already have detection systems in place and keep them updated, it makes it harder for intrusion," advises Lima.

Credit unions, recommends Lima, need to perform an in-depth risk assessment of all the information that needs protection. "You need to prevent people getting into the information at every level." This applies to security at workstations, internal networks, wide-area networks, Internet connectivity security, mainframe security, paper documents, third-party access and even modems/faxes.

Credit unions can better manage PC security exposure by adopting a widely publicized corporate computing policy and adhering to it, suggests Malinowski. Such a policy should have the following mission goals:

- protecting member/customer data,
- protecting employee data,
- describing usage policies on Internet in the workplace, and
- describing usage policies on e-mail in the workplace.

Protecting member/customer data should be at the top of any list. "It is not only your competitors who would like your mailing lists and customer files," states Malinowski.

A good beginning to protecting this information is enforcing password policy guidelines, such as requiring that passwords be a certain length, that they be changed frequently, and that they be complicated enough that it would be difficult for someone to guess what they are.

In addition, he recommends login and time restrictions for sensitive applications and servers, timely backups, off-site restorations and a secure hosted environment with the help of third-party reviewers.

"Other simple precautions mitigate the chance of system intrusions, such as using each system's built-in security controls, which are often underutilized or not used at all, and limiting internal access to information. "It is amazing that financial institutions think everyone should have access to everything," explains Lima.

(Continued on page 31)

Cyber Assaults

(Continued from page 14)

It's nothing personal

Malinowski says it's also important that employees not view their work PC the same as their home computer. "Most users forget that even though the PC on their desk is similar to theirs at home, the PC on their desk is for business needs. Downloading the screen-saver of the month, instant-messaging a friend, or visiting a site for a laugh or picture you've heard about opens the door for spyware, malware and viruses being brought into the corporate network," Malinowski says.

Companies should employ the use of anti-virus, anti-spyware and content filtering systems in their infrastructure, so that these hazards never enter the system through a PC. E-mail needs screening for viruses and spam as well, notes Malinowski. "Spam is of a great concern not only because of the time wasted by going through the e-mail and deleting it, but also [because] offensive content may open a liability to the company through sexual harassment laws. Employees should be careful of whom and what Web sites they give their e-mail addresses to."

In the end, protecting confidential information requires everyone's cooperation and knowledge. "A lot of credit unions don't have the manpower to keep desktops current," says Lima. In those cases, it becomes prudent to keep PC users aware of operating system patches, and urge them to regularly update their computers, as well as their anti-virus software, and scan their drives weekly for any virus infiltration.

"Protecting an institution is a daily and reiterative process," advises Malinowski, who adds, "Hackers don't stop for lunch breaks or vacations."

Roy W. Urrico is a freelance writer who covers the financial industry and technology issues.