

▶ Financial Fitness ▶ Self-Service ▶ Branch Capture

SEPTEMBER 2006

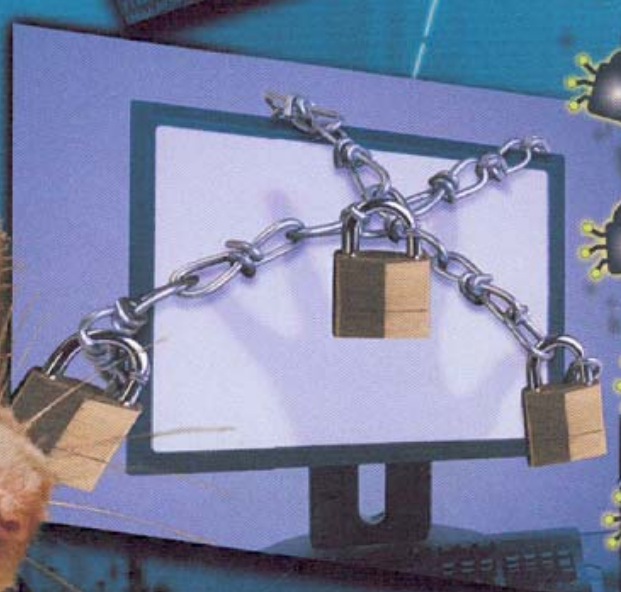
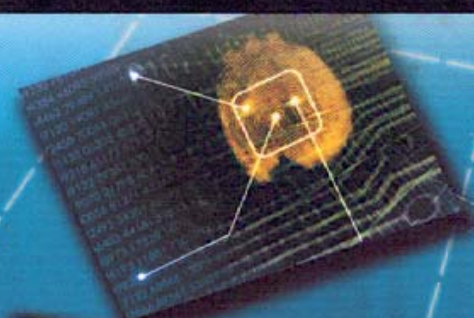
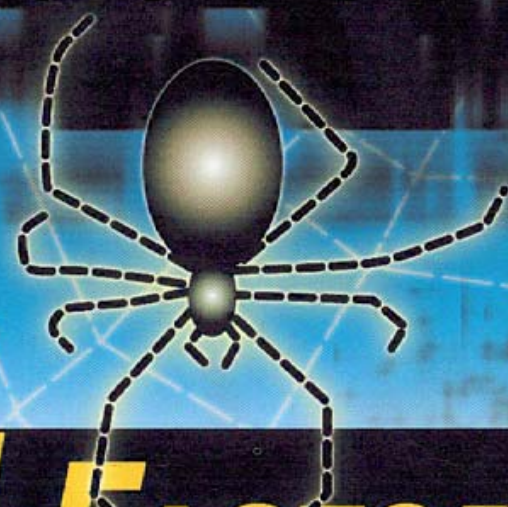
CUNA.ORG

CREDIT UNION

M A G A Z I N E

IT ~~FEAR~~ FACTOR

CUs thwart security threats



Limited resources force CUs into a perilous decision: How much security is enough and at what cost?

ROY URRICO

With modest resources and internal technical expertise, credit unions with high-tech systems and services must determine whether additional security measures are justified—or just a fear-fueled response to an over-publicized problem.

"While we'd like to buy every cool new product that comes out, we can't afford to do so. There's a tendency to play the 'fear factor' with some of this stuff and make credit unions believe they're in severe danger if they don't buy the product," says Cameron Piercefield, assistant vice president of technology at Indianapolis-based Forum Credit Union, with \$970 million in assets.

Yet underspending can be costly, too. "How much is reputation worth to your credit union?" asks Brian Warfel, senior vice president of sales and service at Pembroke Pines, Fla.-based Power 1 Credit Union, with \$375 million in assets. Warfel, CUNA Technology Council chair, reveals that Power 1 builds security enhancements into everything it does. Close to 15% of its information technology (IT) budget goes toward security.

Most of the IT security expenditures are the result of Federal Financial Institutions Examination Council (FFIEC) and

National Credit Union Administration (NCUA) guidance concerning multifactor authentication and information security compliance (CU Mag 4/06, p. 38).

Multifactor authentication is a major focus at Power 1. "That's the major project in the online space," says Warfel. It isn't the only focal point. There are continuing security expenses, such as for penetration testing—protecting systems from computer network attacks. "We went as far as hiring a security specialist for our IT department," he notes.

Some additional costs address membership concerns.

"Consumer education is an increasing expense for us," adds Warfel.

At the \$400 million asset Purdue Employees Federal Credit Union in West Lafayette, Ind., about 10% of its IT budget goes toward security, explains Gail Koehler, senior vice president of technology. Another \$100,000 goes to physical security and ways to prevent social engineering.

"We have a whole division



'People mix up vulnerability testing with penetration tests, which aren't nearly as thorough.'

Jim Stickley

FOCUS

- ▶ **Increased IT security expenses** are tied to recent regulatory guidance and compliance.
- ▶ **Integrate security** with internal processes.
- ▶ **Vendors must implement** proper security programs to safeguard and securely dispose of member data.



'The best vendors can accomplish a set of goals within a defined budget. In other words, sell me a solution, not the product of the month.'

Cameron Piercefield

focus that is risk management," says Koehler, who adds that five years ago about 3% of the total Purdue Employees Federal IT budget went toward security. "As soon as you opened systems to the outside world, you had to take steps to make sure you were secure," she adds.

Palo Alto, Calif.-based Stanford Federal Credit Union, with \$600 million in assets, spends one-third of its \$500,000 IT budget

on security initiatives, explains Sam Tuohy, vice president of e-commerce and technology, and chief technology officer. "In a given year, [security spending] might be 17% or it might be 67%. It changes from year to year. If you upgrade your firewalls, for instance, you easily could blow 40 grand, but you might do that only once every four or five years."

He adds that risk-management costs (as a percentage of his total budget) have doubled during the past five years.

Xerox Federal Credit Union, El Segundo, Calif., with \$799 million in assets, also spends almost one-third of its total \$480,000 IT budget on security, says Dave Price, director of IT. That's quite a transformation from five years ago, Price notes, when "we didn't spend much at all."

► INFO SECURITY SPENDING = BIG BUCKS

Financial institutions' IT expenditures worldwide will reach \$375 billion in 2006, representing about 15% of noninterest expense, estimates TowerGroup, Needham, Mass. Information security accounts for more than 4% of total budget allocations across the industry.

Overall, the credit union industry is expected to spend between \$1.8 billion and \$2.2 billion on 2006 technology needs, including installation, maintenance, staffing and support, according to the 2006 Credit Union Technology Survey by Callahan & Associates, Washington, D.C. Two-thirds of survey participants reported that their 2006 technology budget increased, with technology spending falling between 8% and 10% of operating expenses.

"The proportion of the budget allocated to information security has been growing steadily," explains Guillermo Kopp, vice president, cross-industry at TowerGroup. "Given their leaner IT budgets, in smaller institutions this proportion has been growing much higher."

The security-spending increase has occurred across many businesses during the past five years, points out Khalid Kark, senior analyst, Forrester Research, Cambridge, Mass. That steady increase is primarily because of regulatory constraints and anxiety over protecting the corporate image.

Credit unions are focusing their 2006 technology spending on multifactor authentication of identity, the survey says. Multifactor authentication was the most frequently mentioned item in the technology budget and was considered a priority by 82% of respondents. Survey respondents had average assets of \$679 million.

The good news, explains Kark, is that financial institutions are ahead of other industries. In a survey of chief information officers, Forrester found organizations across industry lines spent 6.6% to 7.3% of their IT budgets on risk management. Financial institutions allocated 8.75% of the 2005 IT budget toward security.

Surprising to Kark is a slight dip—to 8.5%—in projected 2006 financial institution security spending. While security still is a top concern, financial institutions "want to show more value and be more efficient on what is spent," suggests Kark, adding they're moving toward better manageability instead of best-of-breed technology.

The right tools

Simply throwing money at the security problem doesn't solve it, suggests Guillermo Kopp, vice president, cross-industry, TowerGroup, Needham, Mass. The challenge is to have the right balance of security integrated with internal processes. People also need to be proactive, understand risks, and take action.

"The best vendors can accomplish a set of goals within a defined budget. In other words, sell me a solution, not the product of the month," explains Piercefield.

Make sure you're investing in the right tools. Jim Stickley, chief technology officer at TraceSecurity, Baton Rouge, La., a Credit Union National Association (CUNA) strategic alliance provider, believes all credit unions should have:

► **Firewalls;**

► **Intrusion detection** systems for external and internal vigilance;

- ▶ Antivirus software on every desktop; and
- ▶ Secured and/or monitored remote connections, for example, via a virtual private network server.

The FFIEC guidance recommends all financial institutions provide multifactor authentication. "What the government agencies are saying is, 'When we come in, we'd better find something better than ID and password,'" says Kopp.

Not all security threats are external. "Almost half of all intrusions involve some internal oversight or security breach," emphasizes Kopp, who suggests credit unions automatically monitor transactions and flag those that look irregular.

They also should encrypt sensitive data. "The exchange of electronic data can occur so easily [via online transmissions, iPods, flash drives]," explains Kopp. "Cyber thieves eventually may break into anything. But if sensitive information is encrypted, it isn't that easy."

Financial institutions usually "are well-versed with network and infrastructure security," points out Khalid Kark, senior analyst, Forrester Research, Cambridge, Mass. The focus now should be on:

▶ **Application security.** "Smaller financial institutions don't always pay a lot of attention to it. They need to be absolutely sure those Web interfaces and the overall infrastructure don't have vulnerabilities," notes Kark.

▶ **Risk assessment.** "Have systems in place that measure vulnerability, and make sure security training is built into the system from the beginning," including application development, Kark says.

▶ **A security strategy.** "Come up with a clear security strategy that measures progress," Kark adds.

Warfel also says credit unions must consider external and internal risk by assessing who has physical access to the computer room and to critical information. "Establish one or two super-users responsible for administering passwords," he suggests.

A lack of patch management also creates vulnerability, explains Warfel. This is because of the increase of invasive worms and malicious code targeting weaknesses on unpatched systems. More vulnerabilities arise due to increasingly interconnected partners, members, more broadband con-

nections, and remote workers.

"There are vendors that do nothing but patch management services," Warfel explains. "These services push patches out to every piece of equipment that needs them."

When evaluating risk, Tuohy advocates that credit unions audit their security with a professional risk assessment—and then "absolutely follow through on it."

"The best guidance NCUA and FFIEC give is to make sure your IT plans are starting from a risk assessment. It's what I strongly encourage other credit unions to do," he says.

Vendor interaction

The NCUA Security Compliance Guide also contains elements for overseeing, monitoring, and contracting with service providers specified "as any person or entity that maintains, processes, or otherwise is permitted access to member information through its provision of services directly to the credit union."

Credit unions must require vendors to implement proper security programs to safeguard the data and provide proper "data disposal" plans.

Requesting an SAS 70 is a good place to start. An SAS 70 signifies that a third-party service provider conducted an in-depth audit of its control activities, which usually include IT and related processes.

"We always write in [contracts] that they have to comply with all the privacy regulations," explains Warfel. "It's not only making sure you're protected from vendors but the information is used as intended."



'What the government agencies are saying is, "When we come in, we'd better find something better than ID and password."'

Guillermo Kopp





"When they don't do the SAS 70, we ask for their contingency plans," says Koehler.

Selecting a service provider to evaluate risk management also can help.

For example, TraceSecurity offers on-demand security compliance software and risk-assessment services.

The company examines vulnerabilities. "People mix up vulnerability testing with penetration tests, which aren't nearly as thorough," Stickle explains. As part of its assessment, TraceSecurity uses social engineering. "We send our engineers in posing as fire inspectors," he says. Once inside, they assess what systems and information are vulnerable.



'It's all about balance. There are going to be risks. What I'm mostly concerned about is our reputation.'

Sam Tuohey

union receives 170,000 e-mails every month; 165,000 of them either are spam or contain viruses, he explains.

Another example of a necessary security measure is blocking USB (universal serial bus) ports on employees' desktop computers. The combination of a flash drive (small, portable storage

device, sometimes called a thumb drive) and a rogue employee could equate to the loss of member information.

First, Tuohey had to block USB ports, and then buy additional software, validation tokens, and biometric thumbprint readers to authenticate users who have business reasons to use flash drives. The whole exercise set Stanford Federal back \$120 per call center workstation.

"It's all about balance. There are going to be risks. What I'm mostly concerned about is our reputation," Tuohey says. "What I don't want to see is an article in the newspaper that could be devastating" to the credit union.

Credit union boards and senior managers seem to understand the risks and costs. "They want us to be proactive," says Price. "If there are steps that need to be taken to protect security, most of the time the board approves it out of budget."

Purdue Employees Federal considers the need "to upgrade our security the cost of doing business," explains Koehler. "We made that commitment about four or five years ago."

Warfel believes the hype over security made credit unions aware of the issues. "Security is an enterprisewide initiation, not just part of the IT department," he says. More often than not, the board is "asking us whether we're doing enough. The most important thing for our board is that our membership is protected." ●

RESOURCES

► CUNA:

1. CUNA Technology Council: cunatechnologycouncil.org.
2. Security resources: buy.cuna.org, select "security."

► TraceSecurity Inc., Baton Rouge, La.: 225-612-2121 or tracesecurity.com.