

COMPLIANCE WEEK

“Battling the Online Threat to SOX Compliance”

August 1, 2006

By Todd Neff

Once upon a time, compliance executives didn't need to worry about the big bad Internet all that much.

In the old days, protecting corporate data meant not losing floppy disks or reels of tape. And as corporate networks cropped up in the 1990s, IT security went medieval, erecting the digital equivalent of ramparts and moats around sensitive financial and other data.

Alas, those days are gone. Blame the Web application.

Today, those same applications that let executives work from anywhere—instant-messaging tools, online email, databases searchable by Web browser—pose dangerous new threats to sensitive financial information. And any time the integrity of financial information is at risk, SOX compliance enters the picture.

“There were lots of firewalls and network defenses to keep bad guys out, but on the inside, it could be soft and mushy,” says Michael Weider, chief technology officer of Watchfire Corp., which makes security software. “The Web application concept threw that to the wind. Insider programs were put on the Internet so anybody could access it, and hackers exploited it.”

SOX raises the stakes of Web-related IT security in three main ways. First, Web applications and networks must be hardened against unauthorized access of financial data. Second, employees, customers and partners must have clearly defined access rights to that data. Third, companies must make often hard decisions about the use of popular Web-based communication tools such as email and instant messaging.

The specific threats sound like a page from the IT department's list of worries: SQL injection, phishing, pharming and buffer-overflow exploitation to name just a few, plus procedural worries such as user access privileges to virtual private networks. All, however, stem from the same basic concept: an unauthorized person presenting bogus data to trick the recipient into revealing sensitive information.

One of the most common tactics is an SQL injection attack, where an online form can be tricked into sharing the contents of a nominally secure database, says Brian Cohen, chief executive of security software maker SPI Dynamics. Because such attacks look like normal traffic, firewalls are roughly as helpful as a guard cat.

Even within large public corporations, Cohen says, “We find that Web applications tend to be written insecurely. So to the extent that those applications can provide access to confidential or

financial data, it can provide early disclosure or access to information that shouldn't be disclosed at all."

Kevin Beaver, an Atlanta-based information security consultant and author of *Hacking for Dummies*, says one vital security measure is Web-application scanning software. Still, he and others say, the ideal is to train software developers to think like hackers.

"You've got to manually poke and prod around in Web applications to see how they're handling log-ins, transmitting data, storing sensitive information and so on," he says. "There's no replacement for human knowledge and experience."

Many software products can help detect such hacks, including programs that check server logs or monitor strange behavior on the network itself. Charles Kaplan, chief security strategist for Mazu Networks, which makes network behavior analysis software, says the software can spot an unexpected data transfer such as one caused by an SQL injection attack.

"Watching at the network layer, we get somewhat of an independent audit trail," Kaplan says.

More Fundamental Approaches

Others see the IT compliance problems caused by SOX as skewing more towards the design of IT systems themselves rather than ones caused by hackers. "Detective controls" such as firewalls, antivirus software, application-scanning and various monitoring software should be *de rigueur*, this view holds. That leaves the real SOX vulnerability on the inside.

"The key is really looking at an application and asking what roles and responsibilities are appropriate to the environments we're logging into and using," says Kevin Reardon, director of consulting services with IT security giant McAfee. "I've seen several very, very large financial and high-tech companies that have spent several million dollars on auditing roles and responsibilities of users as it relates to large back-end financial systems."

Likewise, Vivek Mehra, chief enterprise architect at the consulting firm Keane, says the primary SOX risks for Web applications come from the accuracy and validity of financial data recorded by managers. "Internal process is the elephant in the room," he says. "I'm seeing across clients a lot more reporting and cross-validation—a lot of risk-mitigation steps before data are presented to a Web-based dashboard."

Free, popular communications tools such as instant messaging and Web-based email programs offered by Google, Yahoo and Microsoft present a related corporate policy challenge. The problem here isn't system vulnerability, but rather data leakage and legal liability, says David Smith, a senior compliance analyst at IT security firm Symantec.

"How do you tell the difference between someone Hotmailing next quarter's financials and Hotmailing a home-loan application?" Smith says. "A lot of companies have drawn a line in the sand and said it's all bad."

Some companies—particularly those in the financial sector, which face stiff compliance obligations to archive practically every communication they make—have responded by offering remote email access and secure instant-messaging programs that leave audit trails. Akonix Systems, FaceTime Communications and IMLogic (recently acquired by Symantec) all make such software.

Still, some companies outside the financial industry are easing up, says Chrisan Herrod, formerly the chief security officer at the Securities and Exchange Commission and now a vice president at Scalable Software, which makes IT compliance software. “Companies originally took a very hard line against using anything outside of their approved email providers,” she says. “But companies I’ve talked to in the pharmaceutical and retail industries have backed off tremendously because they don’t see it as a primary threat.”

The key, Herrod says, is setting policy for what can and cannot be sent via third-party email. She also says that companies’ disclosure of SOX-related deficiencies show that access management problems—not hacking—are the weakest link in Web application security.

“Most companies still don’t get how critical to sound financial and technology controls that is,” she says.