

## Protecting Our Information Systems

*Many of the biggest risks facing the Federal Reserve Bank of Philadelphia come from cyberspace. Threats to the security of the Bank's information networks—for example, from the Internet or e-mail—are almost constant. The Information Technology Services Department has primary responsibility for managing the risk posed by these threats.*

Fending off attacks from cyberspace may have a “Star Wars” sound to it, but it’s a task that the Bank’s Information Technology Services (ITS) Department deals with every day. According to Pat Regan, vice president, ITS, “The Federal Reserve System takes very seriously the establishment of information security standards for all of the Fed’s technology.”

To protect computer systems from intruders, the Federal Reserve uses intrusion detection technology. According to Regan, the technology “senses” certain types of unauthorized activity and reports it to a group that analyzes the information and, if necessary, takes action.

The Philadelphia Fed also uses technology to look for vulnerabilities in its computing systems. Keith Morales, information security manager, notes that assessing vulnerability is one of the first steps in learning how to protect ourselves.

Regan points out that the security industry has noted a dramatic increase in the number of exposures and the number of computer hacking attempts. He describes the Bank’s information security situation as a “punch/counter-punch” problem. “When we learn of a



Pat Regan, Vice President, ITS, and Keith Morales, Information Security Manager

vulnerability,” he says, “our goal is to fix it before the bad guys can exploit it. But it doesn’t take long before the bad guys have another virus or worm to spread.”

The Philadelphia Fed is also the site for the Federal Reserve System’s Groupware Leadership Center (GLC). The GLC provides e-mail, desktop con-

ferencing, instant messaging, document management, and self-service team website capabilities for almost 20,000 customers across all 12 Reserve Banks. To protect the System's computers, the GLC employs rigorous security safeguards that act as a layer of defense against numerous threats from a variety of sources. Such safeguards include filtering spam, which actually exceeds the total volume of delivered e-mail.

### System Architecture

Morales says many of the Bank's information security measures are designed to fit the System's security architecture, which focuses on finding solutions to information security risks. This architecture sets security standards from the standpoint of risk management rather than risk avoidance. "Because we're such a large organization," Morales observes, "we have multiple layers of defenses in place. However, no layer is perfect. So the System's security architecture helps us look at the solutions we have in place and figure out if they're the right ones. The Fed's computer network is so interconnected that a weakness in one area may create weaknesses elsewhere."

Another ITS effort involves the containment of malicious software, or "malware"—for example, spyware or adware that websites download onto computers that connect to them. This effort also encompasses potentially harmful elements distributed through e-mail attachments and embedded links to "bad" websites.

A final factor that helps ITS staff keep computer systems safe is the Bank's own internal audit procedures.

As Regan notes, "We have a high level of security awareness at the Bank. But an important element in protecting the Bank's—and the System's—computer network is training our employees and relying on them to follow security procedures." Internal audits help to ensure that employees develop and use good security habits.

In addition to the endeavors listed above, Philadelphia's ITS Department is involved with many other ongoing projects related to information security. For example, the Bank is leading an initiative to look at how the Fed handles compliance with legislation such as the Federal Information Security Management Act (FISMA). FISMA defines what actions federal agencies need to take to be deemed appropriately secure. Morales says, "It's the government's version of the Federal Reserve's security architecture and risk management." So although the Reserve Banks are not federal agencies, the Board of Governors and the U.S. Treasury are; so any systems developed for use by the Board or the Treasury need to comply with FISMA. Mike Ram, senior information security consultant, is playing a leadership role supporting some of the Fed's initiatives with FISMA.

Ultimately, Morales summarizes the Bank's security position this way: "The Fed wants security at an appropriate level. We're not trying to build 80-foot walls around *all* of our computer systems. But it may be appropriate to have 300-foot walls around Fedwire, which is a significant part of our nation's payment system."

To protect the Fed's computers, the GLC employs rigorous security safeguards that act as a layer of defense against numerous threats from a variety of sources.