REAL WORLD CASE 3

The Federal Reserve Bank: Creating a Sound Software Patch Management Strategy

No longer a grunt-level headache for systems administrators, keeping abreast of security patches has become an essential business practice for any company, large or small. Although an ad hoc patching policy might once have sufficed, the surge in updates during the past two years demands that IT managers be aware of security at every level. After all, if even one critical system is compromised, the entire network can be exposed.

Unfortunately, the sheer volume of updates has made securing an enterprise network more difficult than ever. Every platform is subject to security fixes, but Windows systems are typically the driving force behind most companies' decision to implement a patch management solution. Not only does the Windows platform account for the bulk of enterprise systems, it has also been the source of the greatest number of security vulnerabilities.

For a time it seemed that IT departments' calls for more secure software were falling on deaf ears, but Microsoft has since made security a top priority. In late 2003, the company initiated a full-force drive to revamp its patching strategy, beginning with the announcement that it would begin issuing patches each week. This action by Microsoft indicates their understanding that patch management requires a clear and sound strategy to be effective.

If there were ever a defining case for the need for a well-designed patch management strategy, the Federal Reserve Bank is it. In its New York location alone, the Fed maintains more that 10,000 discrete devices, including AS/400, HP-UX, Linux, Novell NetWare, and Sun Solaris servers, as well as a huge installed base of Microsoft Windows. The awesome responsibility of managing these assets falls on the shoulders of Sean Mahon, the New York Fed's vice president of system management.

"Our real problem is cross-platform," Mahon says. "Fortunately, our Unix-based platforms are more stable in regards to new security vulnerabilities. It's the Microsoft platforms that have become extremely resource-intensive."

Mahon's standard routine for non-Microsoft platforms begins by prioritizing each announced patch. "To us," he says, "these fall into only two categories: security-related, which we act upon immediately, and everything else, with which we can take more time for testing." After a patch is announced, Mahon's system administrators test it on a dedicated system and then deploy it using various tools that come bundled with Unix operating systems.

"Our response to Microsoft patch announcements is similar but with added granularity," Mahon says. Defending against an Internet worm, for instance, is a priority that far outweighs a functional problem in Microsoft Office.

Desktop workstations cause Mahon the most headaches. "'We have over 800 bank examiners, and we usually have no idea where they are," he says. "The challenge with keeping those guys patched is huge, but they have to be patched because if one is infected, he could disrupt everything."

After patches are discovered, Mahon requires that his staff also adhere to strict validation metrics, although he admits this can be problematic. "Ideally, we always do thorough validation and testing prior to deploying," he says. "But the fast-shrinking window of opportunity means we have to push them out faster to ensure we're not vulnerable, and sometimes that outweighs the potential disruption of business systems."

In the past, pushing patches to individual machines from a central location was the big problem, but most modern systems management products can handle that job with ease. Instead, today's headaches stem from the sheer volume of nodes that must be serviced, as well as the complexities of heterogeneous environments.

Even for those organizations with the ability to deploy a comprehensive patching solution, the path to a successful strategy is convoluted and highly individual. There are a number of different ways to attack the problem, each with its own strengths and weaknesses.

The one certainty is that no organization can afford to ignore the problem of patch management. Ignoring critical security fixes is not an option. Instead, the goal should be to apply the latest patches on a timely basis while minimizing the risk to the overall IT environment. To this end, each organization must identify its priorities, establish a policy, and implement the software tools that best suit its unique needs.

Case Study Questions

1. What types of security problems are typically addressed by a patch management strategy? Why do such problems arise in the first place?
2. What challenges does the process of applying software patches and updates pose for many businesses? What are the limitations of the patching process?
3. Does the business value of a comprehensive patch management strategy outweigh its costs, limitations, and the demands it places on the IT function? Why or why not?

Source: Adapted from Oliver Rist, "Applying Patch Management," and "A Network Secure Enough for a Bank," *Infoworld*, June 18, 2004. Copyright © 2004 Infoworld Media Group.