White Paper

The Patch Impasse: Front-line Perspectives From Enterprise IT

Research conducted by: COMPUTERWORLD
The Voice of IT Management

April 2006

Sponsored by: BlueLane

Contents

The Patch Impasse: Front-line Perspectives From Enterprise IT

Methodology overview

In March 2006, Computerworld invited IT influencers to participate in a survey on server patching. The goal of the survey was to better understand the issues managers face related to patching, such as costs, slow deployment and downtime. The survey was commissioned by Blue Lane Technologies Inc., but data was gathered and tabulated independently by Computerworld Research. The following report represents top-line results of that survey and is meant to serve as a brief benchmarking tool for IT managers seeking information about how their peers are addressing patching challenges.

Profile of respondents

The survey included over IT influencers from companies of varying sizes. The focus of this paper will be to show how larger organizations (those with over 500 employees) are addressing server patching. This will be illustrated by comparing responses from larger organizations to those from smaller organizations (those with fewer than 500 employees). Below is a breakdown of respondents based on company size:

Overall respondents: 361

Large organizations (500+ Employees):	252 respondents
Small organizations (fewer than 500 employees):	86 respondents

Percentage Breakdown by Company Size

Large organizations (more than 500 employees)

20,000+ employees:	28%
5,000-19,999 employees:	19%
500-4,999 employees:	23%

Small organizations (fewer than 500 employees)

100-499 employees:	11%
Fewer than 100 employees:	13%

Don't know:	6%

The demands of patching

Computerworld Research surveyed large and small enterprises similarly challenged by the demands of patching. A majority of respondents indicated high levels of concern with the following:

- The overall cost of patching.
- Delays in deploying critical patches.
- Rolling back problematic patches.
- Unpatchable applications.

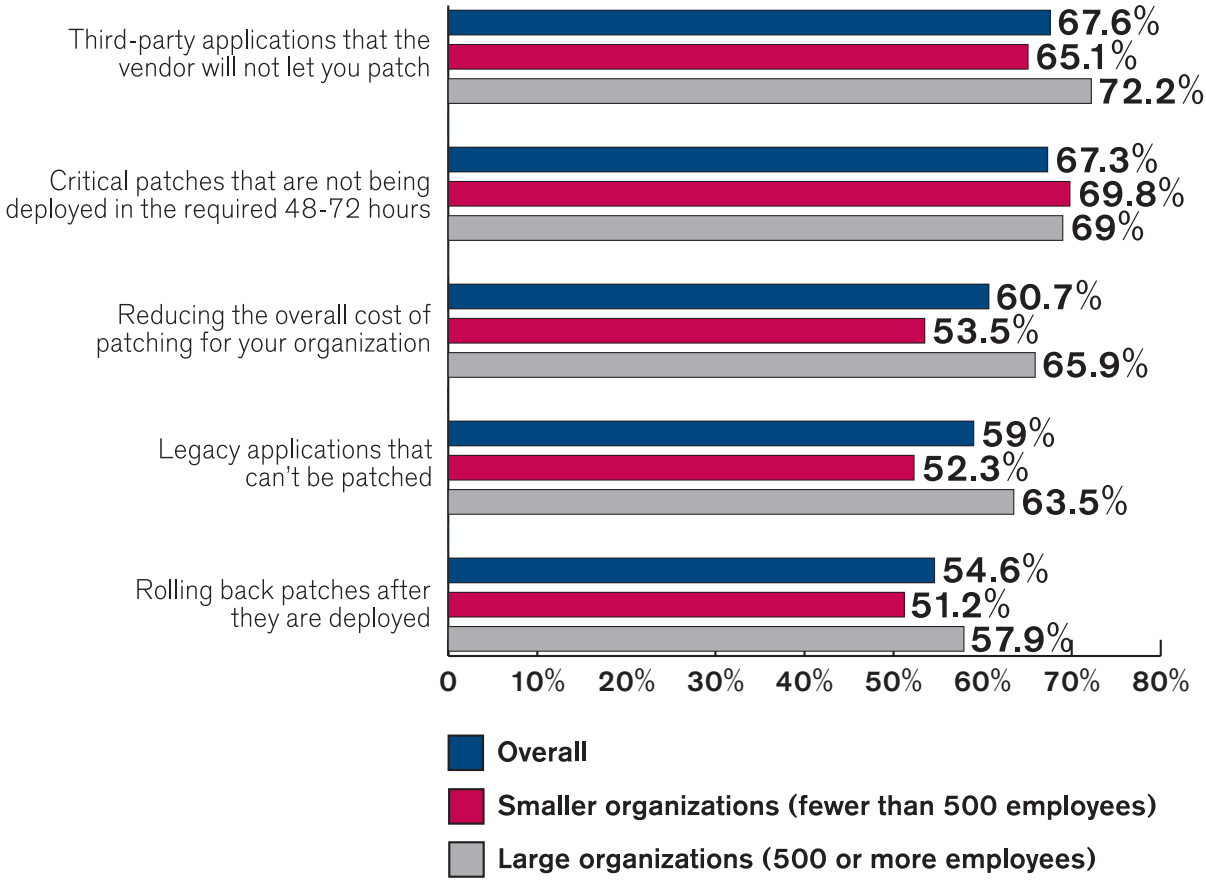
While smaller organizations scored lower on most concerns, a majority of small organizations still reported substantial concern. Most organizations were also concerned with server downtime (83% of large organizations) and boosting business application availability (89% of large organizations).

While organizations of all sizes recognize the critical importance of applying available vendor security patches, they are also reporting substantial levels of concern with the burden of patching. Based on this exclusive research project, we have identified a deep, fundamental problem faced by organizations of all sizes: Given the criticality of patching server vulnerabilities, what are enterprises to do about costs, delays, rollbacks and dealing with unpatchable applications?

Top concerns related to patching

When respondents were asked how concerned they are about a number of issues related to patching, we saw some differences along company size lines. Large organizations are most concerned about the third-party applications they have that the vendor will not let them patch. This is not quite so high a concern for smaller organizations, most likely because they generally have fewer applications to deal with. Organizations of all sizes agree that the time of deployment (within the required 48-72 hours) is a top concern. Additionally, large organizations are far more concerned with the cost of patching.

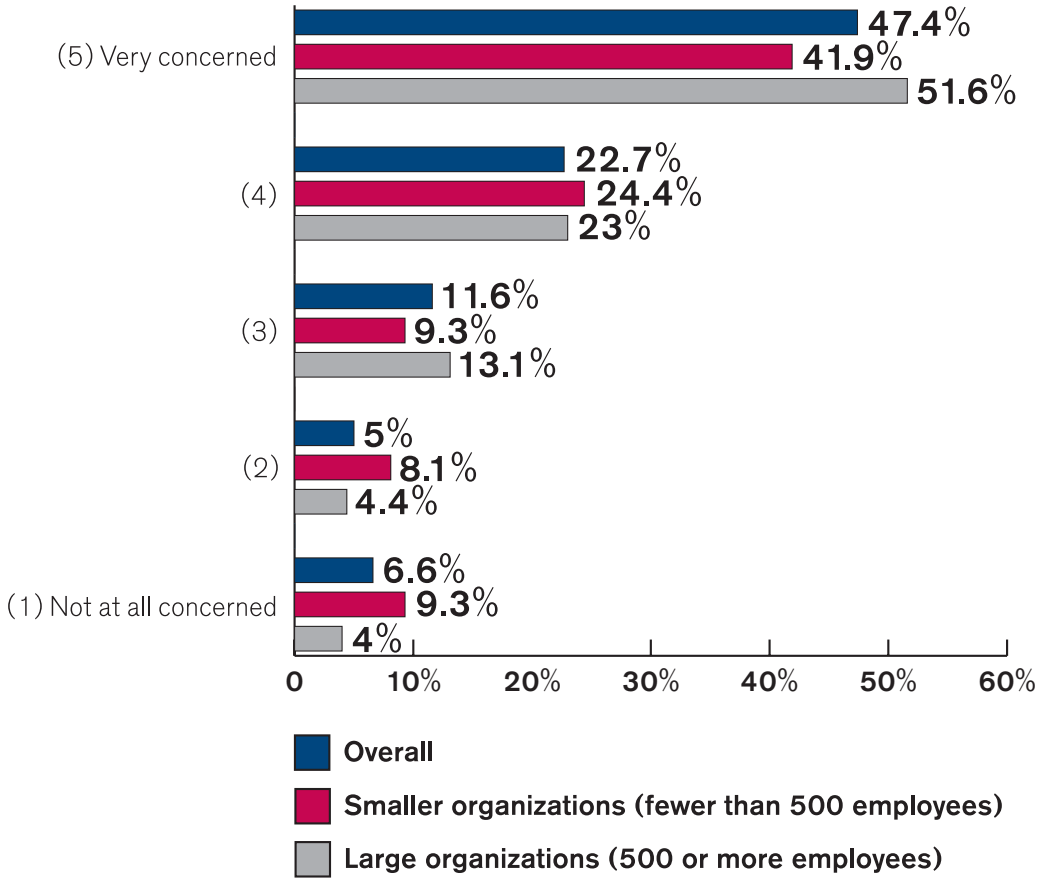
On a scale of 1 to 5, with 1 being not at all concerned and 5 being very concerned, rate how concerned you are about the following: (respondents answering 4 or 5)



Organizational concern about unpatched servers

This survey showed that organizations in general are very highly concerned about unpatched servers. A full 75% of large organizations are concerned or very concerned about this – slightly higher than the 66% of small organizations. Meanwhile, only 4% of large and 9% of small organizations are not at all concerned. This shows just how critical server patching is in the eyes of IT influencers, particularly in larger organizations.

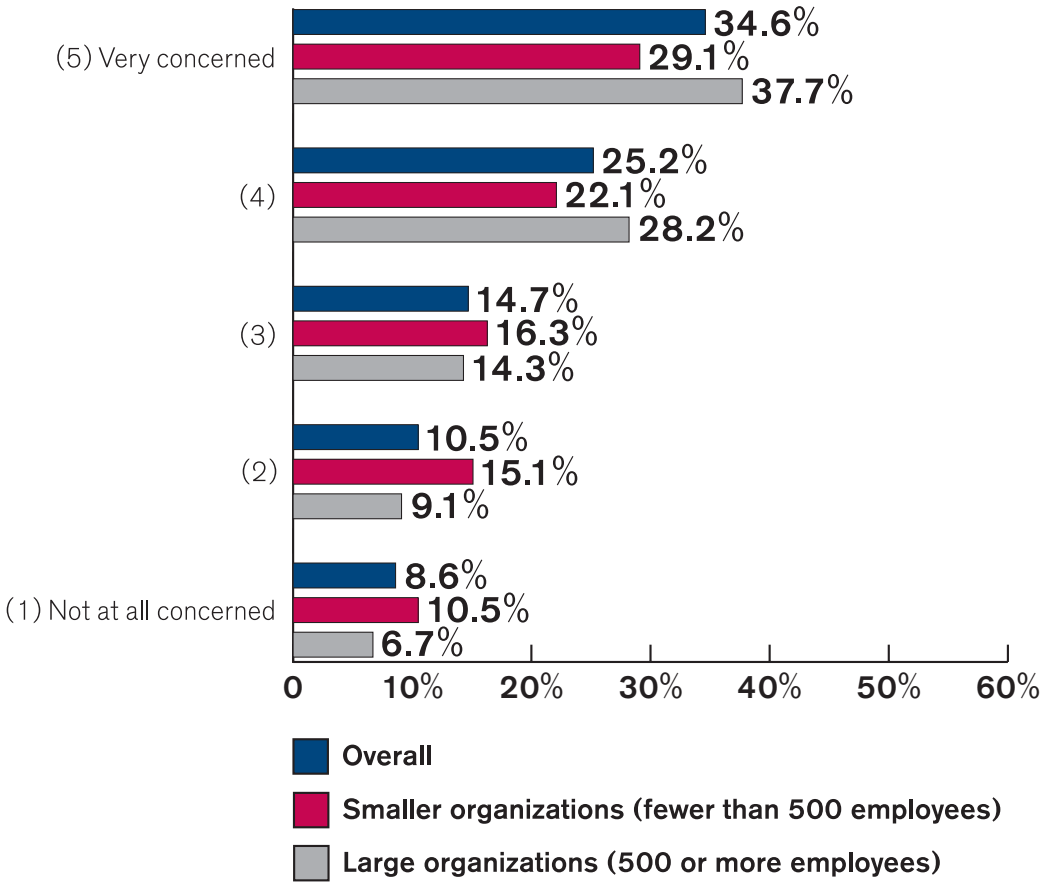
On a scale of 1 to 5, with 1 being not at all concerned and 5 being very concerned, rate how concerned your organization is about unpatched servers:



Records on patches for audits

To get at concern about records on patches for audits, we probed specifically about the respondents' teams' concerns. The question asked how concerned the respondent's team is about keeping up-to-date records on patches deployed for audit reasons. What we saw in the responses is again a high level of concern, much higher for large companies. A full 66% of large-company respondents said their team is concerned or very concerned about this, while just over half of small-company respondents cited this level of concern. This shows that in large organizations, it's not just crucial to have records on patches deployed for audits but to make sure a system is in place to keep them up to date.

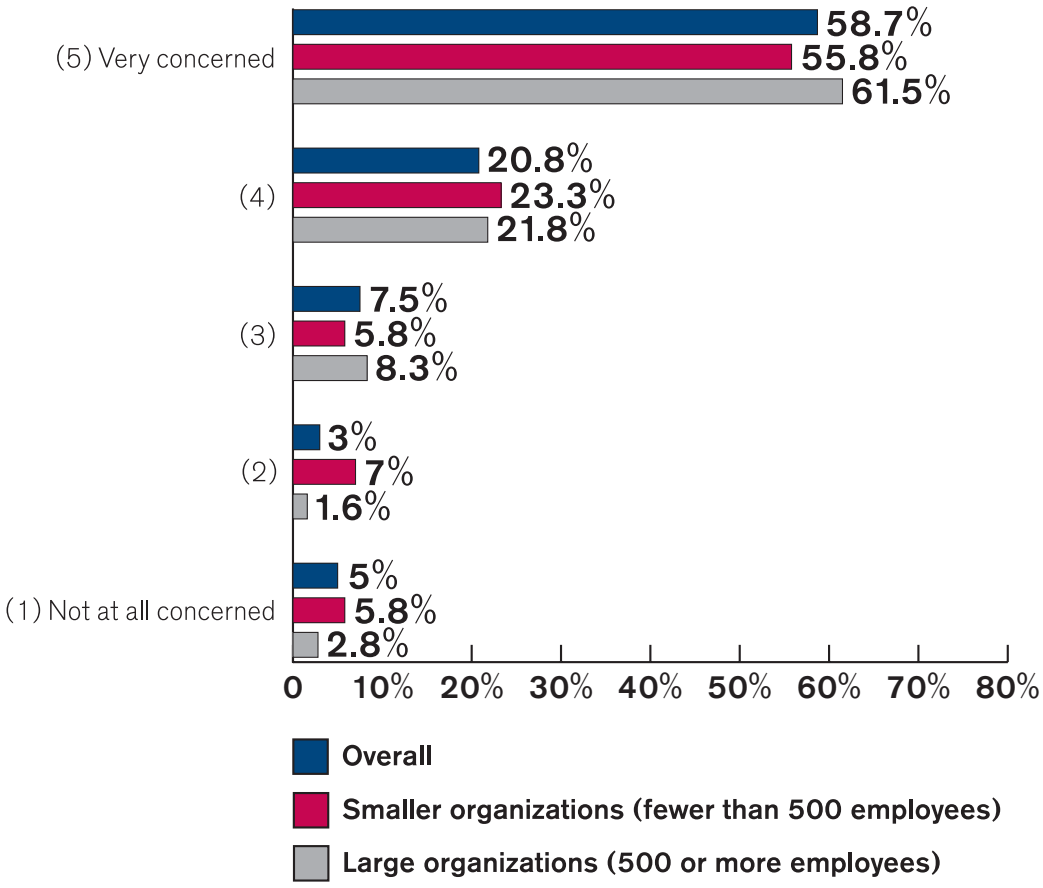
On a scale of 1 to 5, with 1 being not at all concerned and 5 being very concerned, rate how concerned your team is about keeping up to date records on patches deployed for audit reasons:



Downtime of critical servers when patching

Not surprisingly, elimination of downtime was shown to be a very important to influencers at companies of all sizes. Eighty-three percent of large-company respondents said it would be important or very important to eliminate downtime of critical servers when patching. Small-company respondents weren't far behind, with 79% saying this step would be important or very important.

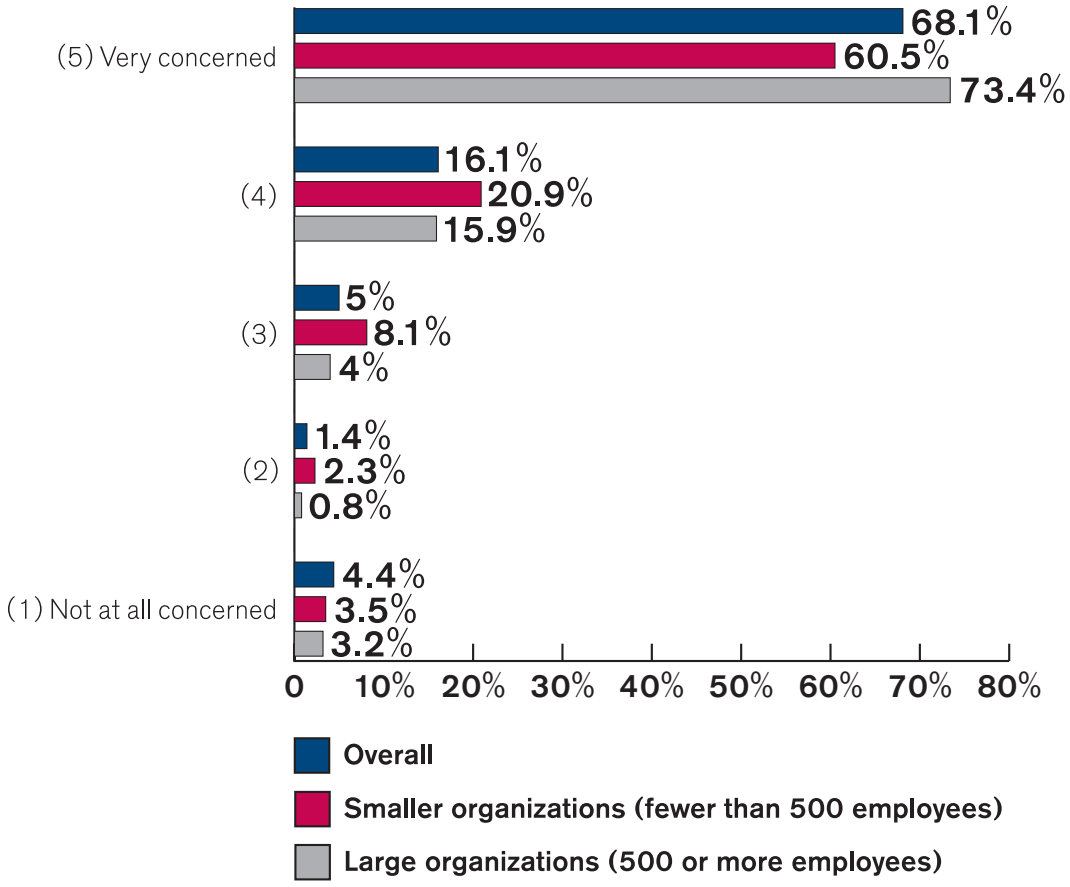
On a scale of 1 to 5, with 1 being not at all important and 5 being very important, rate how important it would be to eliminate downtime of critical servers when patching:



High availability of business applications that rely on servers

Most crucial business applications rely on servers. It's therefore no surprise that when asked how important it would be to have high availability of business applications that rely on servers, respondents saw this as just as important, if not more important, than eliminating downtime. Close to 90% of large-company respondents saw this as important or very important to their organization, with 81% of small organizations seeing this as important/very important. This illustrates a point that may seem obvious but is sometimes not fully grasped by the corporate management of a company: IT management and staff members often struggle to justify the effort and cost needed to maintain high availability of servers, whereas the minute a crucial business application is down, the corporate side of the house is up in arms. Server managers need to make sure the non-IT managers understand the link between high availability and their access to critical business applications.

On a scale of 1 to 5, with 1 being not at all important and 5 being very important, rate how important it would be to your organization to have high availability of its critical business applications that rely on servers:



Conclusion

This survey sheds some light on some very real concerns that IT influencers are facing related to patching. Organizations of all sizes are very concerned about third-party applications their vendor won't let them patch and the time it takes to deploy patches. Large organizations are also particularly concerned with the cost of patching. Across the board, large organizations are also more concerned than their smaller counterparts about unpatched servers, keeping up-to-date records on patches deployed for audit reasons, the downtime of critical servers when patching, and the availability of business applications. It's clear that these are not peripheral issues for these influencers and that a lot of their time is being spent trying to solve them. For those organizations investigating what type of patch strategy they'll take, this report can help serve as a guide to what types of issues peers are facing. It's clear, too, that the importance of each of these issues is amplified as you look to larger companies. It follows, therefore, that organizations looking for service providers to help them with their patch strategies should look to providers that have experience dealing with customers of a similar size so they'll understand the gravity of the issues they face.

Clearly, this survey data demonstrates an "across the board" concern with multiple aspects of the patch process for critical enterprise applications. The implications: 1) It is likely that we will see a rising tide of security and availability issues as enterprises move to more virtualized data center environments and open access to more users; 2) As long as leading application vendors are forced to bring installed, business-critical software up to code via patch releases, there will be a state of enhanced vulnerability and elevated front-line IT concerns. These concerns, indeed, signal an ominous trend as enterprises move to greater application and database interconnectivity. Patching problems and delays, combined with rising vulnerabilities and increasing hacker sophistication, ultimately mean that more data is at risk of malicious attack.

About Blue Lane Technologies

Installing patches on enterprise servers is painful. Vendor patches may close vulnerabilities but often require downtime and may disable application functionality or introduce system instability. Rigorous testing may reduce the risk of patching but also leaves servers in a vulnerable, unpatched state. Research firm Gartner, Inc. predicts that cyberattacks that exploit vulnerabilities where a patch has been available for less than 30 days will increase from 15% of total cyberattacks in 2003 to 30% in 2006.

Blue Lane Technologies is dedicated to easing the pain of patching while eliminating the risk of running unpatched servers. Blue Lane developed the PatchPoint System to fix server-bound traffic by emulating vendor patches inline, which enables servers behind PatchPoint to continue performing just as if the appropriate vendor patch had been installed. PatchPoint puts enterprise servers into a patched state without introducing the problems associated with patching. Once servers are in a patched state, there is ample time to thoroughly test vendor patches without having to worry about unpatched vulnerabilities. The ability to delay the installation of vendor patches provides an immediate return on investment by eliminating the reactionary need to hire additional IT staff or reallocate existing resources to deploy patches. PatchPoint enables administrators to fix now, patch later.

Contact Blue Lane Technologies

Blue Lane Technologies Inc.
10450 Bubb Road
Cupertino, CA 95014

866-492-6555 toll-free in U.S.
408-200-5200 U.S. direct
408-200-5299 fax

info@bluelane.com