The Total Cost of Security Patch Management

A Comparison of Microsoft Windows and Open Source Software

Abstract

There is conflicting information in the IT community about whether security patch management in Microsoft Windows client and sever operating systems is more expensive than their open source software (OSS) counterparts. In 2004, the Product Strategy & Architecture Practice of Wipro Technologies conducted an independent study of 90 enterprises. The study compared security patch management costs of Windows and OSS systems. Based on the results of this study, Wipro concluded that:

- Costs of patching security vulnerabilities of individual Windows-based systems are roughly comparable to those of similar OSS systems.
- On a per-patching event basis, Windows-based systems require less effort to patch than similar OSS-based systems.
- OSS-based systems faced with high-level and critical vulnerabilities are at risk longer than comparable Windows-based systems, and the number of OSS vulnerabilities is underestimated.
- Using patch-related best practices can reduce patching costs significantly for both Windows and OSS systems.

Sponsored by Microsoft Corporation

Audited by the META Group

Authors

Theo Forbath	Theodore.forbath@wipro.com
Patrick Kalaher	Patrick.kalaher@wipro.com
Thomas O’Grady	Thomas.ogrady@wipro.com

WIPRO
Applying Thought

April 2005

Overview of Wipro Product Strategy and Architecture Practice

Wipro's Product Strategy & Architecture (PSA) Practice focuses on the strategic intersection of business, information technology, and globalization. Wipro's PSA Practice combines deep technology expertise in IT and embedded systems, broad strategic planning skills, proficiency in global sourcing strategies, and familiarity with high-growth emerging countries. Wipro's PSA Practice uses senior teams of technical architects and management consultants to help vendors, service providers, and large enterprises document the business value of technology and global sourcing and to develop product and market entry strategies.

For further information, contact Theodore.forbath@wipro.com or visit http://www.wipro.com/psa_practice.

Audited by META Group

META Group validated the approach and the comparison methodology utilized by Wipro to create this white paper. META Group did not validate or certify in any way the results derived by Wipro or the content/data collected by Wipro in support of this study.

For more information about the Meta Group, go to http://www.metagroup.com.

The information contained in this document represents the current view of Wipro Technologies Ltd. (Wipro) on the issues discussed as of the date of publication. Because Wipro must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Wipro, and Wipro or its respective suppliers cannot guarantee the accuracy of any information presented after the date of publication.

This white paper is for informational purposes only. WIPRO AND ITS RESPECTIVE SUPPLIERS MAKE NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Contents

Executive Summary

Many IT managers have experienced long nights of software patching, business disruption, and drains on their IT budgets when security vulnerabilities are left open on client PCs, non-database servers, and database servers. A viewpoint evangelized by the Linux community is that patching pain is a Microsoft phenomenon, and that the solution is to replace Microsoft Windows with open source software (OSS), most notably Linux. Analyst firms are more cautious on this issue and provide little guidance except to say that organizations should evaluate their options carefully. As a result, many IT managers are left with conflicting information and don't know who to believe or what to do.

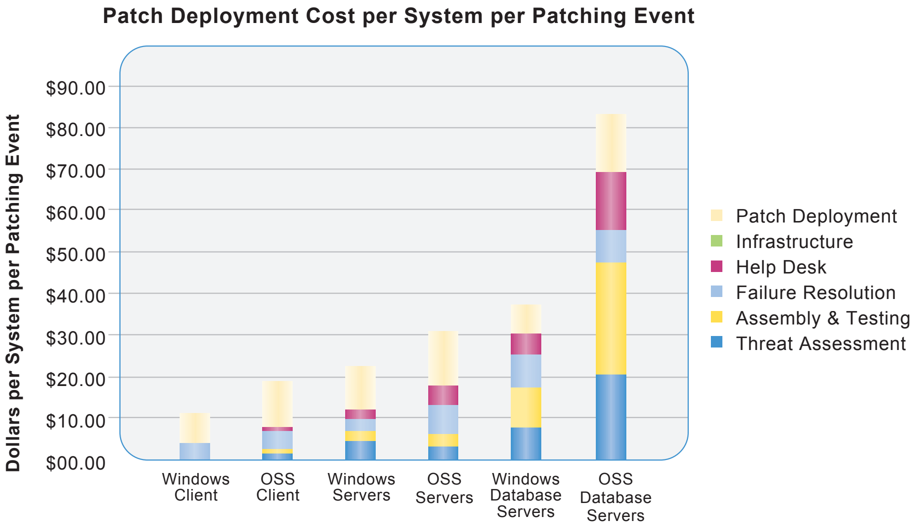

Figure 1: Windows per-system patching event costs are less than those in OSS

Wipro Technologies, a leader in the IT services and consulting industry, conducted a study in 2004 by surveying 90 organizations that use both Windows and OSS-based operating systems. The purpose of the study was to quantify the costs of security patch management of each operating system and determine if the viewpoints of the OSS community are supported by real-world experience and data. Key findings of the study include:

- **The annual costs of patching the security vulnerabilities of individual Windows-based and similar OSS-based systems are roughly comparable.**
  - Patching Windows clients costs an average of 14 percent less than patching OSS-based clients.
  - Windows non-database servers are 13 percent less costly than OSS-based servers to patch.
  - Windows database servers are 33 percent less costly than OSS-based database servers to patch.
- **On a per-patching event basis, Windows-based systems require less effort than similar OSS systems.**
  - Windows client patching events require 40 percent less IT labor than OSS-based client patching events.
  - Windows server patching events require 29 percent less IT labor than OSS-based server patching events.
  - Windows database server patching events require 56 percent less IT labor than OSS-based database server patching events.
- **Survey respondents assess the number of vulnerabilities that apply to their systems inaccurately.**

  Actual exposure to OSS-based system vulnerabilities is consistently underestimated, and exposure to Windows-based system vulnerabilities is consistently overestimated.
- **OSS-based systems faced with high-level and critical vulnerabilities are at risk longer than comparable Windows systems.**
- **Using patch-related best practices can reduce patching costs for both Windows and OSS systems.**
  - Centralizing IT operations can reduce patching costs by up to 55 percent.
  - Standardizing on one or two client-server operating systems can reduce costs by up to 41 percent.
  - Adopting an end-to-end patch management system can reduce costs by up to 44 percent.

This paper covers new ground in the Windows-OSS security patching debate not previously covered by other analyst firms. This research required Wipro to review the best available reports from other leading analyst firms and then fill in the gaps with new data by surveying IT managers at 90 enterprises. For a complete explanation of the research methodology, refer to the Survey Methodology section of Appendix A, "About This Report."

For a detailed discussion of patching events, refer to the Event-Driven Costs section of "Patch Management Costs" later in this report.

[1] Non-database servers refer to servers used for file and print, utility, networking, applications, messaging and groupware. Non-database servers for both Windows and OSS are referred to as 'servers' for the remainder of this report.

Introduction

With increasing focus on cost-effective management of IT infrastructure, IT managers must find more efficient ways to carry out the IT activities that support organizations and end users. Security patch management has long been recognized as a major contributor to the IT budget, but it has never been examined in detail to understand what drives costs, how to manage them effectively, and how to mitigate against security risks.

The Wipro Product Strategy & Architecture (PSA) Practice wanted to get a better understanding of the day-to-day experiences of enterprise IT managers when they manage security patches and patching events on Windows and OSS operating systems. In 2004, PSA analysts conducted a survey of 90 enterprises from different industry sectors and locations in the United States and western Europe. All of these organizations ran both Microsoft Windows and OSS operating systems on client PCs, non-database servers, and database servers.

This paper provides detailed evidence that shows where the costs, risks, and opportunities of patch management really lie in both Windows and OSS/Linux environments. This research delivered three key themes:

- **Annual patching costs for individual Windows and OSS-based systems are surprisingly similar.** Although respondents reported more patching events for their Windows systems, each patching event is less expensive to complete, and more patches are delivered at the same time. This essentially negates the impact of the higher patch volume for Windows systems.
- **After a patch is available, Windows clients are patched more quickly than their OSS counterparts.** For servers and database servers, there is no significant difference in risk between Windows and OSS systems.
- **Patching does not have to be painful.** Organizations that embrace solid best practices and automated tools can drive the costs out of patch management for both Windows and OSS systems.

This white paper compares patching and overall patch management costs for known and reported vulnerabilities on Windows and OSS/Linux systems. The paper also discusses the relative benefits of employing patch management best practices for both operating system and application software.

There are multiple security patch management costs that contribute to lost productivity and opportunity cost. These include the costs of unplanned downtime in the data center as well as unplanned downtime for end-users. This study focused on the direct costs of patch management for IT operations. While losses of end-user productivity or opportunity cost are significant in every organization, they are also very difficult to quantify because each organization assesses value differently. This survey discovered how respondents identified common challenges in security patch management and which management responses were most effective. The results clearly showed several areas of best practice that apply equally to Windows and OSS environments.

Security Patch Management From Two Points of View

To begin measuring the cost of security patch management (patch management) in the enterprise, it is important to define how enterprises and independent software vendors (ISVs) perform patch management and how these differences are reflected in the response and release processes used by each group.

This distinction is important because from an IT manager's perspective, one is about their own internal process for dealing with security threats, and the other is about how their software suppliers respond to the same threats. In terms of the speed with which ISVs respond to known threats and their response of issuing patches to address those threats, the gap between the two processes is critical to addressing security vulnerabilities in a timely manner. This important issue will appear again later in the paper in the discussion of deployment days of risk.

For the purposes of this study, Wipro adopted the high-level process model shown in Figure 2 to distinguish the ISV and enterprise responses to patching.

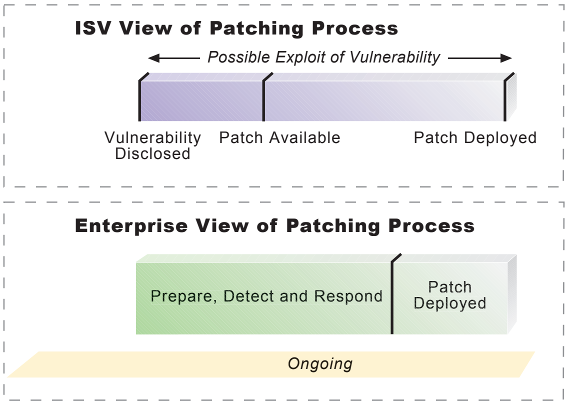
ISV View of Patching Process
Possible Exploit of Vulnerability
Vulnerability Disclosed
Patch Available
Patch Deployed
Enterprise View of Patching Process
Prepare, Detect and Respond
Patch Deployed
Ongoing

Figure 2: Comparison of enterprise and ISV patching processes

The second critical event occurs when the patch first becomes available, and the enterprise actually deploys the patch. Based on the enterprise view presented in Figure 2, the total annual patching costs for an enterprise can be calculated as:

*Total Annual Patching Cost = [(Cost of Patching Event) * (Number of Patching Events)] + [(Prepare and Detect Costs) * (Number of Reported Vulnerabilities)] + (Total Annual Ongoing Costs)*

But Figure 2 does not show the complete picture of how an enterprise looks at security patch management. Figure 3 provides a snapshot of the sub-categories used by most of the companies surveyed for the study. Ongoing measures are particularly important to contend with security threats that are measured as annual costs that include research and monitoring costs activities (measured per vulnerability) and actual patching activities (measured per patching event).

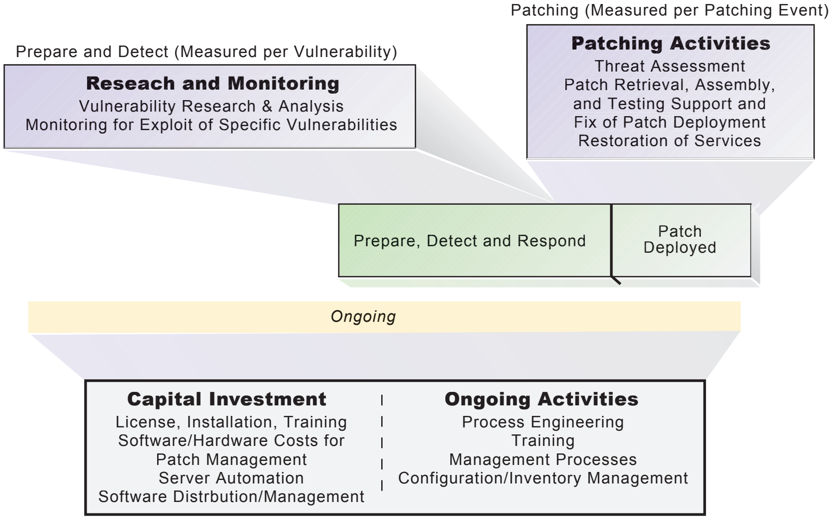
Patching (Measured per Patching Event)
Patching Activities
Threat Assessment
Patch Retrieval, Assembly,
and Testing Support and
Fix of Patch Deployment
Restoration of Services
Prepare and Detect (Measured per Vulnerability)
Reseach and Monitoring
Vulnerability Research & Analysis
Monitoring for Exploit of Specific Vulnerabilities
Prepare, Detect and Respond
Patch Deployed
Ongoing
Capital Investment
License, Installation, Training
Software/Hardware Costs for
Patch Management
Server Automation
Software Distrbution/Management
Ongoing Activities
Process Engineering
Training
Management Processes
Configuration/Inventory Management

Figure 3: Patching processes in the enterprise

Although ISVs can lose credibility by not responding to security threats quickly, the enterprise stands to lose something more valuable: data, which can take months and huge costs to retrieve and reconfigure.

For purposes of this study, all costs illustrated in Figure 3 are calculated as:

*Cost = (Fully Burdened Hourly Rate) * (Hourly Effort)*

Patch Management Costs

This part of the analysis covers the reported patching costs for organizations that participated in the Wipro study. To build a complete picture of patching costs, this section reflects the structure presented in Figure 3. These costs include:

- Event-driven costs (per-system, per-event patching effort and annual patching effort per system)
- Prepare and detect costs
- Ongoing patching costs, including capital costs and the costs of ongoing activities

Event-Driven Costs

Wipro measured how the organizations in this study conducted patching events from two related perspectives. The first approach measured the elapsed time that it takes an organization to successfully complete a patching event. The second approach measured the cost to organizations in terms of IT effort.

Event-driven costs are incurred by an organization every time it mobilizes around an available security patch and begins a patching event. Activities that generate these costs include:

- Patch-specific threat assessment
- Patch retrieval, assembly, and testing
- Patch deployment
- Support and fix of patch deployment
- Restoration of services to compromised systems

Patching events. Patching events occur when organizations deploy updates to executables, data, or system configurations that reduce or eliminate known vulnerabilities or bugs.

- Patches, which are generally applied to systems after a period of testing, often require a restart of systems or services.
- Typically, more than one software patch is applied, and more than one vulnerability is closed during a single patching event.
- Successful completion of a patching event occurs when an organization deploys the patches to a pre-determined percentage of systems. For the companies in this study, the average pre-determined percentage of systems patched during a patching event was 77 percent.

By convention, patching events do not include patches that are deployed as part of routine maintenance. This is because routine maintenance is usually a sunk cost—costs that have already been incurred—with fixed IT labor and system downtime.

For each patching event, the IT staff must spend time engaged in tasks specific to patching. Even with sophisticated tools at their disposal, staff members must complete some or all of the steps in Figure 4, each of which contributes to event-driven costs.

Process Step		Description
1	Threat assessment	Includes risk analysis, impact assessment, and response planning.
2	Patch assembly and testing	The average amount of time spent includes these activities: ▪ Assembling the resources needed to deploy the patch ▪ Testing and qualifying the patches
3	Patch deployment	Support and resolution of patch deployment.
4	Failure resolution	The time it takes to resolve patch distribution failures (average effort to resolve each failure)
5	Help desk	End-user support costs associated with patches and patching
6	Infrastructure reconfiguration	Reconfiguration of network or system infrastructure related to patches or mitigating vulnerabilities

Figure 4: Patching process steps

Effort. Effort represents the total number of hours IT professionals work when they respond to a security threat and successfully complete an effective patching event. Figure 5 shows the amount of effort devoted to various types of patching activities. These effort values are roughly similar for the installed base of both Windows and OSS systems at participating organizations. These numbers are surprising, because the average installed base of Windows-based clients is approximately 10 times larger than the OSS client installation. Intuitively, one would think that the discrepancy would be much large given the relative installed base of Windows-based clients.

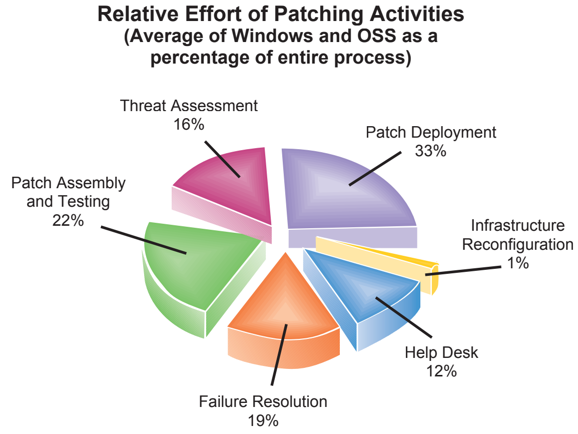

Figure 5: Relative effort of patching activities for Windows and OSS systems

The amount of time required to deploy a security patch per system is a vital component of estimating annual IT operations costs. Varying costs resulting from differences in IT expertise in Windows and OSS-based systems is offset by the overall number of systems. However the speed with which patches can be deployed and the overall volume of patches required based on known vulnerabilities and as-yet unknown threats is more important.

Per-System, Per-Event Patching Effort

Wipro estimated the average effort to complete a typical patching event by using the effort data supplied by study participants. To compare similar values, the analysis is presented on a per-system basis.

In every instance, the effort to patch each individual Windows-based system—clients, servers, and database servers—in each patching event was significantly less than for equivalent OSS systems. These effort values correlate directly to the labor expended on each activity. Applying labor costs to the hours spent patching each system shows a similarly striking picture:

- Windows clients took approximately 40 percent less effort per patching event than OSS clients.
- Windows servers took approximately 29 percent less effort per patching event than comparable OSS servers.
- Windows database servers took approximately 56 percent less effort per patching event than comparable OSS database servers.

Figure 6 shows relative values of the deployment effort per system per patching event for Windows and OSS systems.

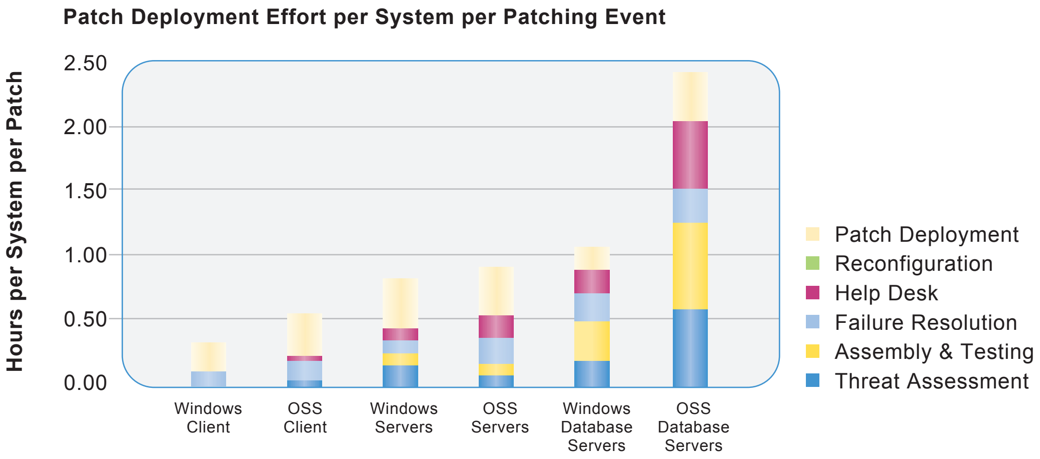

Figure 6: Comparison of Windows and OSS patching effort per system per patching event

Figure 7 shows the data presented in Figure 6 by looking at the patch deployment effort per system per patching event.

	Windows Clients	OSS Clients	Windows Servers	OSS Servers	Windows Database Servers	OSS Database Servers
Threat assessment	0.0025	0.0231	0.0569	0.0966	0.1962	0.5513
Assembly & testing	0.0033	0.0262	0.0848	0.1048	0.2803	0.7446
Patch deployment	0.2133	0.3074	0.2891	0.3535	0.1986	0.3880
Failure resolution	0.0958	0.1497	0.1326	0.1745	0.2271	0.2028
Help desk	0.0051	0.0269	0.0622	0.1532	0.1766	0.5499
Total	**0.3200**	**0.5333**	**0.6256**	**0.8825**	**1.0788**	**2.4365**
Percentage Difference	**40%**		**29%**		**56%**	

Figure 7: Effort measured as person-hours per patching event per system

Annual Patching Effort per System

Another way to view the effort of patching is to look at the annual effort of patching a single system rather than a single event. Wipro did this by multiplying the average reported number of patching events for each firm by workload with the per-patching event cost.

This analysis is based on activity reported by respondents for the calendar year 2003 rather than the absolute number of vulnerabilities and patches observed for Windows and OSS systems. This distinction is made because the goal of this research study is to understand actual costs incurred by organizations when they patch systems rather than to calculate a theoretical maximum number of patching events or vulnerabilities. Study results indicate that on an annualized basis:

- Windows client patches require 14 percent less IT effort than comparable OSS-based client patches.
- Windows server patches require 15 percent less IT effort than comparable OSS-based patches.
- Windows database server patches require 33 percent less IT effort than comparable OSS-base-patches.

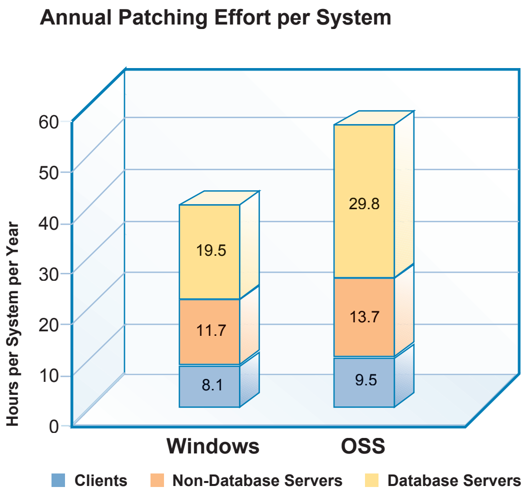

Figure 8: Comparison of total annual patching effort

Figure 8 presents the annualized average patching effort of Windows-based systems compared to OSS-based systems for respondent companies. The figure shows that a Windows-based system requires an average 26 percent less effort per year to deploy patches to than comparable OSS-based systems.

Prepare and Detect Costs

Prepare and detect costs are calculated by measuring the specific investments in vulnerability research and monitoring on a per-vulnerability basis and analysis in monitoring for exploit of specific vulnerabilities.

Figure 9 shows all the activities in the prepare and detect patching process for the surveyed organizations.

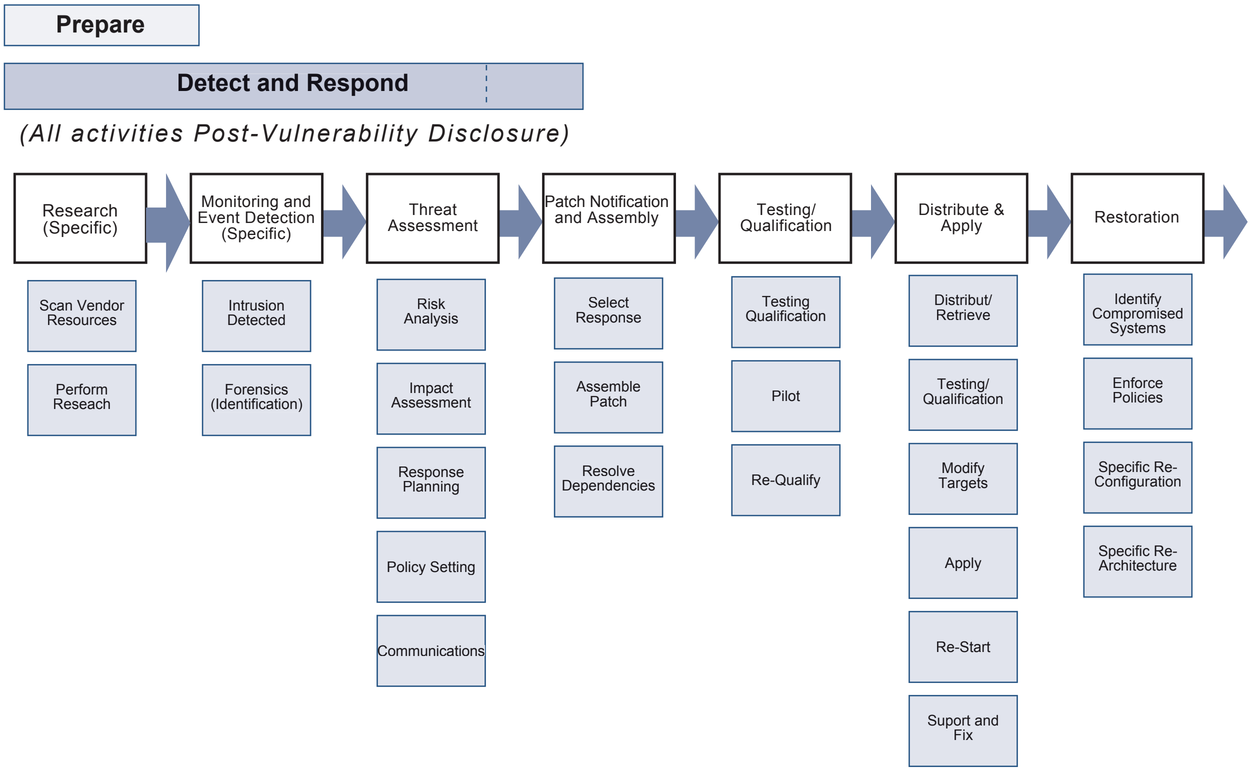

Figure 9 – Prepare and detect patching process

Figure 10 shows the relative number of vulnerabilities and cost per vulnerability for Windows and OSS systems.

	Prepare & Detect Cost per Vulnerability	Average Number of Vulnerabilities	Total Cost
Windows	$892	251	$223,892
OSS	$792	116	$91,872
Percentage Difference	**+13%**	**+116%**	**+144%**

Figure 10: Participant prepare and detect costs for 2003

For each vulnerability that is addressed, Windows-based systems experienced slightly higher prepare and detect costs than comparable OSS systems. Windows systems also experienced more than twice the average number of OSS vulnerabilities. However, when these numbers are evaluated on a per-system basis, the cost picture changes drastically. Figure 11 shows the differences of Windows and OSS installed bases of study participants.

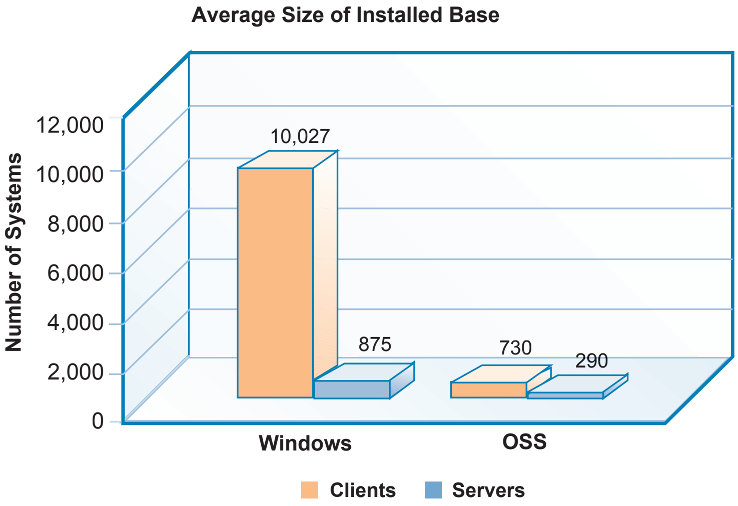

Figure 11: Average installed base for Windows and OSS environments

Taken on a per-system basis, the number of vulnerabilities of Windows-based systems is actually less than that of OSS-based systems. On average, the prepare and detect cost per vulnerability per system is 75 percent less for Windows-based systems than OSS-based systems.

There was no noticeable correlation between the amount of money spent on prepare and detect activities and patching event costs. This is not surprising, as prepare and detect activities have a measurable effect on containing the cost of actual breaches or exploits of vulnerabilities, rather than on the application of patches themselves.

Ongoing Costs

Event-driven and prepare and detect costs are only part of the story. Organizations also have ongoing costs that support the IT group's patching operations.

Figure 12 shows the activities involved in ongoing patch management activities.

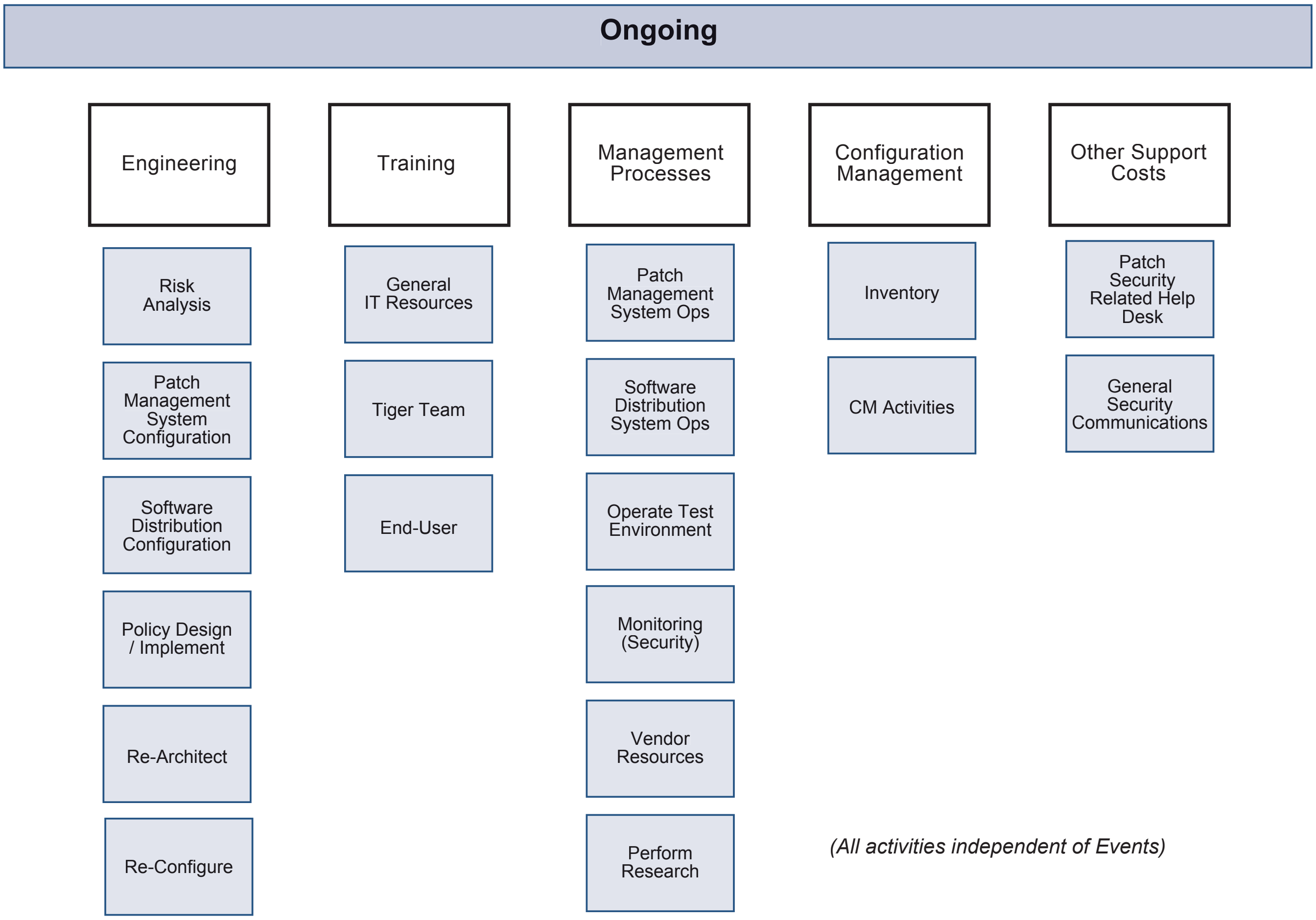

Figure 12: Ongoing patch management processes

Ongoing costs include capital costs and costs of ongoing activities. Wipro collected detailed ongoing cost data from participating organizations. Capital costs include:

- Software and hardware costs for systems that aid in patch management
- Installation, support, and training costs related to systems that aid in patch management

Ongoing activities include:

- Patching-related process engineering
- Patch management training
- Management oversight
- Configuration and inventory management

[2] Note: Investment costs are amortized over 3 years.

Figure 13 shows the average total cost and the average cost per system for using management tools in ongoing patch management processes.

Cost of Management Tools	Average Total Cost			Average Cost Per System		
	Windows	OSS	Percentage Difference	Windows	OSS	Percentage Difference
Patch management tools	$192,660	$107,500	+79%	$17.83	$107.19	-83%
Server automation tools	$79,400	$73,850	+8%	$7.35	$73.65	-90%
Software distribution tools	$242,000	$105,860	+129%	$22.39	$105.56	-79%
Total	**$514,060**	**$287,210**	**+79%**	**$47.57**	**$286.40**	**-83%**

Figure 13: Comparison of capital costs related to patching[2]

These calculations only include patch management, server automation, and software distribution packages that are used in patch management. The capital costs for OSS systems are noticeably lower than for Windows systems. However, given the approximate 10:1 ratio of Windows clients to OSS clients, the per-system capital costs for Windows systems are 83 percent lower than those of OSS systems.

Figure 14 shows which patch management-related tools are used most often by participating organizations.

Category	Windows	Open Source
Patch management	PatchLink Update Shavlik Technologies HFnetChkPro SecurityProfiling SysUpdate	PatchLink Update SecurityProfiling SysUpdate BigFix Patch Manager
Server automation	HP OpenView IBM Tivoli CA Unicenter	HP OpenView IBM Tivoli CA Unicenter
Electronic software distribution and management	Microsoft Systems Management Server HP OpenView Novell ZENWorks	HP OpenView Novell ZENWorks Custom developed by respondent

Figure 14: The most popular patch management-related tools used by participating organizations

Figure 15 shows detailed cost information for each ongoing cost category.

Cost	Overall Average			Per System Average		
	Windows	OSS	Percentage Difference	Windows	OSS	Percentage Difference
Patch-related Process Engineering: ▪ Adding patches to software images ▪ Patch management (software distribution and system configuration) ▪ Policy design and implementation ▪ Overall system re-architecture and re-configuration	$507,810	$219,560	+131%	$47	$160	-71%
Patch Management Training: ▪ System training ▪ Patch management process training ▪ Fire Drills (simulations and dry runs)	$375,200	$158,450	+137%	$34	$115	-70%
Management Oversight: ▪ Patch management (software distribution and system operations) ▪ Operation of test environment ▪ Researching or scanning vendor resources	$427,200	$152,900	+179%	$39	$111	-65%
Configuration and Inventory Management: ▪ System census and identification including tracking additions, moves, and changes ▪ Maintaining databases of system configurations and compliance with published configurations	$305,790	$154,650	+98%	$28	$112	-75%
Total	**$1,616,000**	**$685,560**	**+136%**	**$149**	**$499**	**-70%**

Figure 15: Comparison of ongoing Windows and OSS patching costs

Given the difference in total installed base of Windows and OSS systems at surveyed companies, the ongoing support costs are noticeably lower for OSS systems than for Windows systems. However, on a per-system basis, the costs for Windows systems are on average 70 percent lower.

Risk-Related Costs

Identifying risk and managing exposure is critical to the operations of all companies. Proactive organizations cannot rely solely on ISVs to monitor risk. Rather, they must actively develop processes to monitor and reduce exposure to security risks themselves. Reducing the number of vulnerabilities that affect operating systems will benefit organizations only if they patch operating systems to close high-level and critical vulnerabilities. The following section examines the risk exposure of companies with Windows and OSS systems.[3]

Potential Security Risk: Software Vulnerabilities

Respondents reported more patching activity for vulnerabilities on Windows systems than for OSS systems. To clarify the actual risk levels in both environments, Wipro researchers established a baseline of actual high-level and critical vulnerabilities reported in 2003 and compared them against the number of vulnerabilities addressed by participating organizations.

Wipro selected the Common Vulnerabilities and Exposures (CVE) dictionary maintained by MITRE.[4] Using CVE has many advantages, including comprehensive content, vendor-independence, and use of standardized names of vulnerabilities, which are often used as a key or cross-reference in vendor and analyst reports. These advantages enabled Wipro to learn more about specific vulnerabilities. The basic steps in this process involved:

1. Categorize the raw list of CVE-2003 vulnerabilities into the six system categories used throughout this study.
2. Match these vulnerabilities with the *overall inventory of software* reported by respondents. For example, if a participating organization uses Microsoft Exchange Server, Exchange Server-related vulnerabilities are included; if Debian is not installed, Debian-specific vulnerabilities are excluded.
3. Establish the number of possible patching events based on the total possible number of vulnerabilities applicable to each firm.
4. Compare the number of reported vulnerabilities to the number of actual vulnerabilities.

Wipro used a subset of the CVE research to estimate the number of vulnerabilities applicable to the respondent firms. Based on this subset of data, Wipro predicted the number of vulnerabilities for software and operating systems running on Windows and OSS servers and database servers.

[3] For information about reducing vulnerabilities in Windows-based systems, refer to an article published by Forrester, “Is Linux More Secure than Windows?” This article is available at: http://www.forrester.com/Research/Document/Excerpt/0,7211,33941,00.html.

[4] CVE stands for Common Vulnerabilities and Exposures, a list of standardized names of vulnerabilities and other information related to security risk exposure. CVE aims to standardize the names of all publicly known vulnerabilities and types of security exposure. For more information, go to http://www.cve.mitre.org/about.

Figure 16 illustrates the difference between the number of vulnerabilities that Wipro expected to see reported and the average actual number of vulnerabilities reported by respondents.[5] Across the board, respondents have overestimated the annual number of Windows vulnerabilities and underestimated the number of OSS vulnerabilities.

	Windows Platform			OSS Platform		
	Expected Vulnerabilities	Apparent Vulnerabilities Reported by Respondents	Percentage Difference	Expected Vulnerabilities	Apparent Vulnerabilities Reported by Respondents	Percentage Difference
Clients	64	110	-42%	60	48	+25%
Servers	51	81	-37%	73	37	+97%
Database Servers	39	60	-35%	50	30	+67%

Figure 16: Expected number versus reported number of vulnerabilities on Windows and OSS platforms

Based on the data in Figure 16, several themes emerge:

- OSS vulnerabilities are not reported as diligently as vulnerabilities on their Windows counterparts. This situation is especially true for servers. In Figure 16, the difference between the reported and the actual number of vulnerabilities for OSS-based systems is greater than 98 percent.
- In the case of client systems, the reported number of Windows platform vulnerabilities are consistently overestimated by as much as 42 percent. It is possible that some respondents running multiple versions of Windows counted the same vulnerabilities more than once, but that alone does not account for the disparity.
- A relatively lax attitude of IT managers towards OSS platform vulnerabilities is due to the assumption that OSS systems are more secure than analogous Windows systems.
- Immature OSS operational processes make vulnerabilities more difficult to notice and will likely result in less rigor in identifying patching events.

Overall, the difference in the frequencies of vulnerabilities between comparable system categories in 2003 was negligible. In fact, evidence points to significantly fewer vulnerabilities on Windows systems in 2004. The comparative slowing in discovery of new vulnerabilities was consistent with the introduction of new Microsoft products designed and built as part of the Microsoft Trustworthy Computing initiative.

If an organization ignores a specific vulnerability or patch, direct costs are not incurred. Similarly, if an organization bundles patches for several vulnerabilities into one patching event, their costs will probably be different than organizations that address only one vulnerability per patching event.

[5] "High risk" was externally assigned for each CVE entry by http://icat.nist.gov and self-assigned as "high" or "critical" by respondents.

Figure 17 summarizes reported patching events and reported vulnerabilities per patching event for Windows and OSS systems.

System	Average Number of Patching Events			Average Number of Vulnerabilities per Patching Event		
	Windows	OSS	Percentage Difference	Windows	OSS	Percentage Difference
Clients	25	18	+39%	3.5	2.0	+75%
Servers	19	16	+19%	3.5	1.8	+94%
Database Servers	18	12	+50%	2.6	1.8	+44%
Total	**62**	**46**	**+35%**	**N/A**	**N/A**	**N/A**

Figure 17: Summary of vulnerabilities, patching events and vulnerabilities per patching event

Figure 17 reveals some interesting insights. Windows system administrators perform 35 percent more patching events than OSS administrators. Deployment of multiple versions of Windows in most companies contributed to more patching events for Windows. However, in the overall patching process, Windows system administrators close between 31 and 49 percent more vulnerabilities per event than OSS administrators.

Using the average yearly number of patching events in Figure 17, the total annual cost to patch each kind of Windows-based system is actually slightly less than each of its OSS counterparts. Figure 18 compares annual risk-related patching costs per system per event.

Clients			Servers			Database Servers		
Windows	OSS	Percentage Difference	Windows	OSS	Percentage Difference	Windows	OSS	Percentage Difference
$297	$344	-14%	$416	$479	-13%	$682	$1,020	-33%

Figure 18: Comparison of annual risk-related patching costs ($ per system per event)

Deployment Days of Risk

One of the critical areas of risk management on which enterprises should focus is deployment days of risk, which measures the number of days between patch availability and completion of patch deployment.

Deployment days of risk, which were measured in this study, differ from distribution days of risk, which measure the time between development of patches and the time when they are available to organizations. Figure 19 compares distribution days of risk for Microsoft and selected OSS vendors.[6]

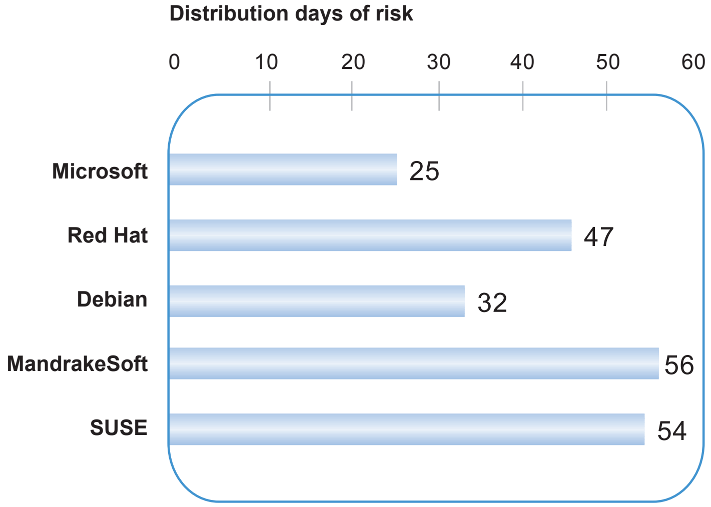

Figure 19: Comparison of distribution days of risk
(Source: "Is Linux More Secure than Windows?", Forrester Research, Inc., March 2004)[3]

The average completion times for all patching events for Windows and OSS installed bases were similar. The difference in Windows and OSS installed bases makes this similarity surprising. Figure 20 compares days of risk of Windows and OSS clients and servers at various levels of vulnerability.

Risk Type	Clients			Servers			Database Servers		
	Windows	OSS	Percentage Difference	Windows	OSS	Percentage Difference	Windows	OSS	Percentage Difference
Low	41.9	41.2	+2%	42.4	41.8	+1%	33.5	32.8	+2%
Medium	19.2	19.1	+1%	18.7	18.9	-1%	20.5	20.4	0%
High	5.9	11.8	-50%	10.9	11.4	-4%	13.2	13.6	-3%
Critical	4.4	9.9	-56%	4.3	4.3	0%	7.4	7.4	0%

Figure 20: Server patching times for different vulnerability levels

When the numbers are examined more closely, a significant scenario emerges. Organizations reported that it took them less time to complete patching events of high-level and critical vulnerabilities for their Windows client systems than for OSS client systems. In fact, critical vulnerability patches required less than half as much time to complete on Windows clients than on OSS clients. As a result, OSS clients encounter significantly more deployment days of risk on clients but few additional days of risk for servers and database servers.

[6] The number of actual vulnerabilities and patching events reported by OSS respondents as compared to the projected numbers of vulnerabilities that were compiled during the same time period by security-related organizations are widely divergent, adding the potential for significant business risk to enterprise systems.

Total Cost of Patching

The total annual cost of security patch management is a sum of these costs:

- Patching event costs
- Prepare and detect costs multiplied
- Total annual ongoing costs

Clients, servers, and database servers are included in this calculation. These system categories also appear in Figure 21, which summarizes the annual per-server patching costs for event-driven, detect and prepare, and ongoing costs.

Total Annual Cost of Patching Systems						
	Total			Per System		
	Windows	OSS	Percentage Difference	Windows	OSS	Percentage Difference
Event-driven costs Patching clients	$2,978,990	$350,610	+750%	$297	$343	-13%
Patching non-database servers	$303,821	$139,003	+119%	$416	$479	-13%
Patching database servers	$65,485	$66,325	-1%	$682	$1,020	-33%
Detect and prepare costs Vulnerability research & monitoring	$223,627	$91,667	+144%	$21	$91	-77%
Ongoing costs Ongoing patch management support	$1,706,000	$685,560	+149%	$158	$684	-77%
Investment in patch management tools	$514,060	$287,210	+79%	$48	$286	-83%
Total Annual Cost	**$5,791,983**	**$1,620,375**	**+257%**	N/A	N/A	N/A
Per-System Annual Cost	N/A	N/A	N/A	**$1,622**	**$2,903**	**-44%**

Figure 21: Average annual total cost of patching for 90 participating organizations

The significant cost differences shown in Figure 21 are due to the differences in the installed base of Windows and OSS systems. From this perspective, annual patch management costs are approximately $1,622 per system for Windows-based systems versus $2,903 for OSS-based systems. More importantly, individual Windows systems require roughly 14 hours per year of support effort versus 32 hours for OSS systems.

The comparative totals are not surprising. Even given the lower per-patching event cost of Windows systems, the sheer size of the average Windows installed base and the historically larger reported number of patching events means that there are many more Windows systems to patch.

The total cost of patch management was higher than most respondents expected. When asked to estimate the annual cost of patch management in terms of labor requirements measured in full-time equivalents (labor costs excluding capital expenses), firms consistently underestimated the effort required. It is unlikely that these unexpectedly high costs are well understood within organizations or properly budgeted and accounted for.

Figure 22 compares annual per-system patching costs for all 90 organizations participating in the Wipro study.

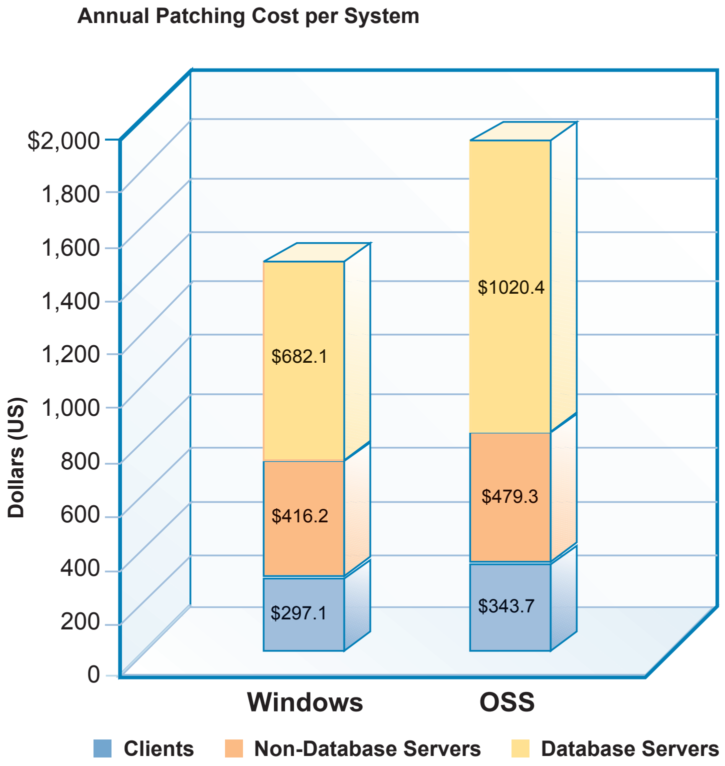

Figure 22: Total annual per-system patching costs

Conclusions and Recommendations

Security patch management activities are a major component of IT operating costs and must be managed more proactively to improve efficiency and lower total costs. This approach can be accomplished only by making patching activities more visible and by implementing security patch-related best practices. For IT managers, the key facts to keep in mind include:

- Costs of patching security vulnerabilities of individual Windows-based systems are roughly comparable to those of similar OSS systems.
- On a per-patching event basis, Windows-based systems require less effort than similar OSS-based systems.
- Actual exposure to OSS-based system vulnerabilities is consistently underestimated, and exposure to Windows-based system vulnerabilities is consistently overestimated.
- OSS-based systems faced with high-level and critical vulnerabilities are at risk longer than comparable Windows-based systems.
- Using security patch-related best practices can reduce patching costs significantly for both Windows and OSS systems.

Recommended Best Practices

In addition to the comparative analysis between the competing platforms, Wipro identified several best practices that can make the patch management process more efficient and help to lower the total patch management costs for both Windows and OSS systems. IT strategies that had a high correlation with lower patch management costs included:

- Centralize IT operations rather than use distributed operations.
- Use end-to-end solutions from one or more vendors rather than relying on a single vendor for all functionality.
- Standardize on two or fewer operating systems.
- Employ open standards versus proprietary architectures.
- Engage in heavy testing rather than little or no testing.
- Engage in strict policy enforcement rather than little or no enforcement.

Of the IT strategies analyzed, centralized operations, end-to-end solutions, and OS standardization resulting in a low number of operating systems were the most effective means of reducing patch management costs. These best practices were highly correlated with lower patching event costs and resulted in significant reductions in overall costs. Figure 23 shows the best practices that yielded the best results among survey respondents.

Best Practice	Description	Percentage Reduction in Total Patch Management Costs	
		Windows	OSS
Centralized IT Operations	Centralized IT operations are characterized by varying degrees of central control over IT policy and systems, consolidation of data centers and staffing.	55%	28%
End-to-end Solutions	Use end-to-end solutions from one or more vendors to provide business functionality as needed.	15%	44%
OS Standardization	Policy that tries to limit the number of operating systems in production on clients, non-database servers, and database server to two or fewer operating systems.	41%	N/A

Figure 23: Description of recommended best practices

There were no obvious structural or technical reasons for the differences in the effect of best practices in Windows and OSS-based systems. However, the Windows platform has both a larger installed base and more reported patching events per year relative to fixed costs. As a result, a greater cost reduction occurs when practices are improved.

Optimal results can be achieved by implementing best practices in the following manner:

- **Standardize client and server operating systems.** Operating system standardization should be introduced as part of a timed refresh of the client installed base. This type of standardization also provides substantial benefits beyond the patch management process.
- **Evaluate patch management systems.** Evaluate and implement patch management systems from a holistic, end-to-end perspective rather than relying on a single vendor for all functions.
- **Implement a program of continuous improvement.** As part of a program of continuous improvement, explore the costs and benefits of centralizing specific IT operations, such as system and staffing consolidation. This practice should be attempted incrementally rather than all at once, starting with the costs that can be improved the most. Firms should begin by centralizing policy and other up-front processes, which will provide a more stable base for further improvement in patching activities.
- **Establish processes and benchmarks.** Establish processes that will track patching effort and map process results against company and industry benchmarks. Create straightforward, high-level patching performance reports, distribute them widely, and show the patch management improvement through time.
- **Consolidate hardware configurations.** Reducing the number of hardware configurations from 50 to 25 can reduce the overall time to deploy patches and other minor updates by as much as 50 percent.[7]
- **Refresh client operating systems.** Removing clients that are three years old or older from the installed base can reduce the failure rate of minor updates and patches by up to a third.[8]

[7] See “New Insights on PC Management: Benefits of Controlled PC Hardware Diversity,” Wipro Technologies, 2004. For a copy of this report, visit http://www.intel.com/business/bss/products/client/stableplatform/wipro.pdf.

[8] See “Recommended Practices: Strategic Management of the PC Installed Base,” Wipro Technologies, Microsoft Corporation, and Intel Corporation, 2004. For a copy of this report, visit http://download.microsoft.com/download/b/7/e/b7eaa1d4-e67e-4b7c-92be-294bc42fc36f/MS_WP_303149-001USrv2.pdf.

Appendix A: About This Report

During 2004, the Product Strategy and Architecture (PSA) Practice of Wipro Technologies surveyed CIOs, IT directors, and senior IT managers at 90 enterprise organizations. Each interviewee managed the processes discussed in the survey for some or all of their organization's Windows and OSS systems. On average, the interviewees were directly responsible for 42 percent of their organization's total installed base.

Survey Methods

Study participants were selected from a pool of 100 enterprise organizations. Selection criteria included:

- Participant operations use both OSS and Windows systems.
- Participant operations use a total of at least 2,500 clients and all types of servers.
- Each participant operates:
    - At least 100 OSS or Windows clients or
    - 100 OSS combined non-database servers and database servers and/or
    - 50 Windows non-database or database servers.

For example, firms with a total of 45 OSS servers had their server costs excluded, though other costs may have been included.

Representatives from 100 firms were surveyed and interviewed for this study. Ten firms were excluded from the final analysis because they did not meet the criteria required for participation in the study. The most common reason for omitting a firm's responses was that they didn't meet the minimum requirements for OSS installations in more than one category.

Each study participant was given a 20-page, in-depth survey covering the full lifecycle of patching activities.[9] After the survey was completed and returned, Wipro reviewed the answers and conducted a 30-to-60-minute follow-up telephone interview with each respondent. This call helped participants finish any incomplete responses and enabled Wipro to clarify survey responses. The following conventions were used to keep the analysis accurate and straightforward:

- To allow direct comparison of all responses, respondents were asked to limit their comments to the activities and events of the calendar year 2003.
- Respondents were asked to include only computers running Windows or OSS operating systems.
- Whenever OSS software was run on a system with a Windows OS (Apache on Windows Server 2003, for example), or non-OSS software was run on an OSS system (such as Oracle on Red Hat Enterprise Linux AS), respondents were asked to consider all patching efforts as part of the operating system category. Therefore, Apache on Windows would be in the Windows category, and Oracle on Red Hat would be in the OSS category.

Then, Wipro developed an extensive financial model; the results of the model drive the analysis of this study. To confirm the integrity of the financial model, META Group validated the approach and the comparison methodology used to create this white paper.[10]

[9] The structure of the survey can be found in the "Survey Structure" later in this appendix.

[10] META Group did not validate or certify in any way the results derived by Wipro or the content/data collected by Wipro in support of this study.

For the purpose of this study, the PC and server operating systems are defined as follows:

- **Clients.** Desktop and mobile computers that operate on either desktop or laptop personal computers (PCs) and run Windows or OSS operating system and business software.
- **Non-database Servers.** Computers running a Windows or OSS operating system and a variety of server software that included:
  - File and print servers.
  - Security servers.
  - Networking servers.
  - Utility application servers (Microsoft.NET or J2EE application servers).
  - Line-of-business application servers (includes commercial, packaged applications).
  - Intranet Web servers.
  - E-business servers.
  - Messaging servers (e-mail servers).
  - System management servers.
  - Collaboration or groupware.
- **Database Servers.** Computers running a Windows or OSS operating system and a relational database management platform.

Survey Structure

The survey was structured in the following manner:

- Section 1, "Business and IT Profile," provided general background information about participating organizations. Data included the number of employees, number and type of OSS and Windows systems, IT staff hourly rates, and general IT management approach.
- Section 2, "Application Stack," provided detailed information about the OSS and Windows environments and gathered census information about the specific operating system and software packages in use.
- Section 3, "Security Patch Management Tools and Practices," asked questions about the security patch management tools, infrastructure, and best practices currently in place.
- Section 4, "Ongoing Security Patch Management Activities," focused on ongoing operating costs needed to run security patch management infrastructure and related activities.
- Section 5, "Vulnerability and Patching Event-Specific Security Patch Management Activities," asked questions about the total effort of dealing with different classifications of vulnerabilities as they are disclosed by software vendors or maintainers and about IT efforts of patching event activities.
- Section 6, "Event-Specific Security Patch Management Activities," asked about the total time and effort spent dealing with different classifications of vulnerabilities. Information related to vulnerabilities as they are disclosed by software vendors or administrators and answered detailed questions about IT labor used in patching event activities.
- Section 7, "Breaches and Downtime," asked questions about how IT departments and the organization as a whole respond to vulnerability-related security breaches and to planned and unplanned downtime.

Survey Participants

The 90 organizations that participated in the study operate in the United States (63) and Western Europe (27) and employ between 2,500 to 113,000 people. Figure 24 provides the organization size measured by employees.

Number of Employees	Participant Firms
2,500 to 5,000	58
5,001 to 9,999	10
10,000 to 39,999	15
>40,000	7
Total	**90**

Figure 24: Company profile by number of employees

Figure 25 demonstrates that participants came from a wide variety of industry sectors.

Industry	Participant Firms
Finance	26
Manufacturing	9
Media	7
Energy	3
Healthcare	14
Education	6
Retail	4
Other	21
Total	**90**

Figure 25: Company profile by industry

Figure 26 provides a frequency distribution of server types in Windows and OSS environments among the study's participating organizations.

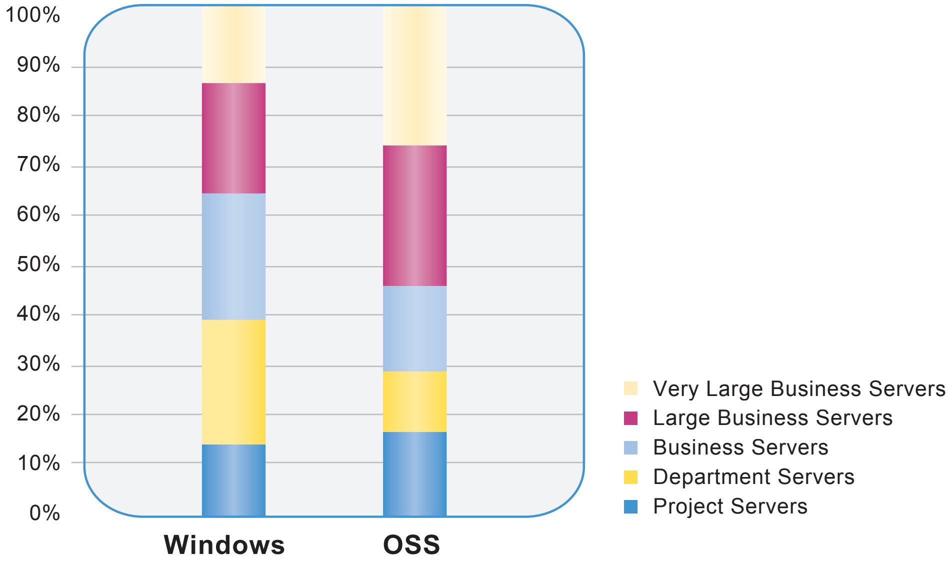

Figure 26: Types of servers in the study's Windows and OSS environments

Figure 26 groups servers into the following categories:

- **Project or workgroup server.** Supports up to 150 concurrent users.
- **Departmental server.** Supports up to 300 concurrent users.
- **Business server.** Supports up to 600 concurrent users. Typically a single or (in some rare cases) dual processor.
- **Large business server.** Supports between 600 and 1500 concurrent users. Typically limited to 2-, 4-, or 8- processor systems.
- **Very large business servers.** Supports more than 1500 concurrent users. Typically this type of server uses 8, 16, 32, or more processors.

About Wipro Product Strategy & Architecture Practice

The Wipro Product Strategy & Architecture (PSA) Practice is a division of Wipro Technologies, a global technology services division of Wipro Ltd. (NYSE-WIT). Wipro's PSA Practice has more than 10 years experience in researching, analyzing, and documenting the business value of technology solutions. In addition to consulting to technology vendors, practice consultants and technologists work with global enterprises and service providers in architecting and implementing large-scale systems. This practical hands-on experience gives Wipro's PSA Practice consultants and technical architects first-hand knowledge that informs their business analysis work.