

Realtime
publishers

"Leading the Conversation"

The Definitive Guide™ To

Service-Oriented Systems Management

sponsored by



altiris®

Dan Sullivan

Chapter 11: Benefits of Mature Systems Management Processes.....	222
Controlling IT Costs	222
Labor Costs	223
Automation of Manual Processes	224
Cross-Functional Skills.....	230
Improved Support Services.....	232
Capital Expenditures.....	233
Improved Asset Management	233
Decision Support Reporting.....	235
Operating Costs.....	235
Improved Management Reporting	236
Improved Allocation of Resources	237
Improved Predictability of Operations.....	239
Improved License Management.....	240
Improved Security Posture.....	240
Cost of Not Controlling IT.....	242
Compliance	242
Loss of System Integrity and Availability	243
Loss of Confidential and Private Information	243
Business Disruption	244
Summary	244

Copyright Statement

© 2007 Realtimepublishers.com, Inc. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtimepublishers.com, Inc. (the “Materials”) and this site and any such Materials are protected by international copyright and trademark laws.

THE MATERIALS ARE PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of Realtimepublishers.com, Inc or its web site sponsors. In no event shall Realtimepublishers.com, Inc. or its web site sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

The Materials (including but not limited to the text, images, audio, and/or video) may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, in whole or in part, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

The Materials may contain trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of such third parties.

Realtimepublishers.com and the Realtimepublishers logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

If you have any questions about these terms, or if you would like information about licensing materials from Realtimepublishers.com, please contact us via e-mail at info@realtimepublishers.com.

[**Editor's Note:** This eBook was downloaded from Realtime Nexus—The Digital Library. All leading technology guides from Realtimepublishers can be found at <http://nexus.realtimepublishers.com>.]

Chapter 11: Benefits of Mature Systems Management Processes

The SOM model discussed throughout this guide touches on many aspects of IT infrastructure management, from risk analysis and asset management to patch management and service delivery. It has to; IT is a broad and varied discipline. Despite the variety of topics, a single theme links them all—process management. The information systems that run businesses, governments, and organizations long ago reached levels of complexity that could not be managed with ad hoc approaches. Formalized processes and procedures, aligned with organizational objectives, are the foundation upon which successful IT operations are built.

This chapter examines the benefits of mature systems management processes by examining two related questions:

- How can a mature systems management model help control IT costs?
- What are the costs of not controlling IT operations?

Not surprisingly, the answers to these questions are as diverse and varied as the field of IT itself. There is no simple answer to either of these questions, but the following pages will provide a high-level overview that spans the breadth of the costs and benefits of mature systems management processes.

Controlling IT Costs

“Do more with less” is something of a popular mantra in management circles, and less popularly, with IT operations staff. As unpopular as it is with some, that four-word sentence captures the driving business factors that are shaping how we implement and manage information services. Consider how it translates into day-to-day operations:

- As employees and contractors leave, the remaining staff is expected to assume their responsibilities
- Strategic plans—driven by market conditions, perceived opportunities, government regulation, and other factors—create new requirements for IT services but not additional funding for meeting those needs
- Internal customers’ expectations are increasing because they are exposed to rich applications in other external environments, such as the Web

The outcome of these pressures includes the need for IT managers to deftly reallocate resources, leverage technologies in innovative ways, and constantly plan for change. To succeed, managers need to focus on business fundamentals while adapting to the dynamics of information technologies.

The fundamentals of controlling costs are the same in IT as any other part of an organization; economics textbooks will tell you that there are labor costs and there are capital costs. What those textbooks do not always tell you is what to do with those costs. To fill this knowledge gap, let's first divide the world of IT costs slightly differently than the most basic branch and consider three types of costs:

- Labor
- Capital expenditure
- Operating costs

Let's examine how mature systems management processes benefits each of these.

Labor Costs

Labor costs can make up a significant portion of an organization's IT budget, and controlling those costs while maintaining quality service levels can be a challenge. Of course, any manager can cut staff and reduce bottom-line costs, but organizations need to maintain services, adapt to new opportunities, and expand the range of services offered. Blindly cutting staff is a short-term solution to a long-term problem. IT managers succeed when they consider the full range of issues in staffing their operations:

- Cutting costs can mean reducing quality if reductions are not based on reorganization that includes quality measures in decisions
- Restructuring often requires improved communications and reporting to support a geographically dispersed workforce
- Automation can reduce labor costs and maintain quality of service (QoS) if workflows are well understood and systems are implemented to accommodate those workflows

The SOM model described throughout this guide can help reduce labor costs by making systems management more efficient while maintaining and improving QoS. In particular, the SOM model can support

- Automation of manual processes
- Cross functional skills and reallocation of resources
- Improved support services

Automation of Manual Processes

Given the level of sophistication of businesses' IT infrastructure, it is surprising how many manual processes are still required in some organizations. Some common labor-intensive operations that can be automated include:

- Provisioning user access
- Patching and upgrading devices
- Inventorying devices
- Troubleshooting

Provisioning User Access

These tasks vary in the level of automation possible. Provisioning user accounts, for example, can be highly automated. New users can create requests for access, managers can approve requests, and then an automated process could create accounts, set authentication parameters, establish authorizations based on roles, and notify the new user when the process has completed. Figure 11.1 shows a typical workflow for this process.



With the exception of the initial request and the manager approval, the rest of the process is driven by an established and automated workflow that is controlled by policies for authentication and authorization.

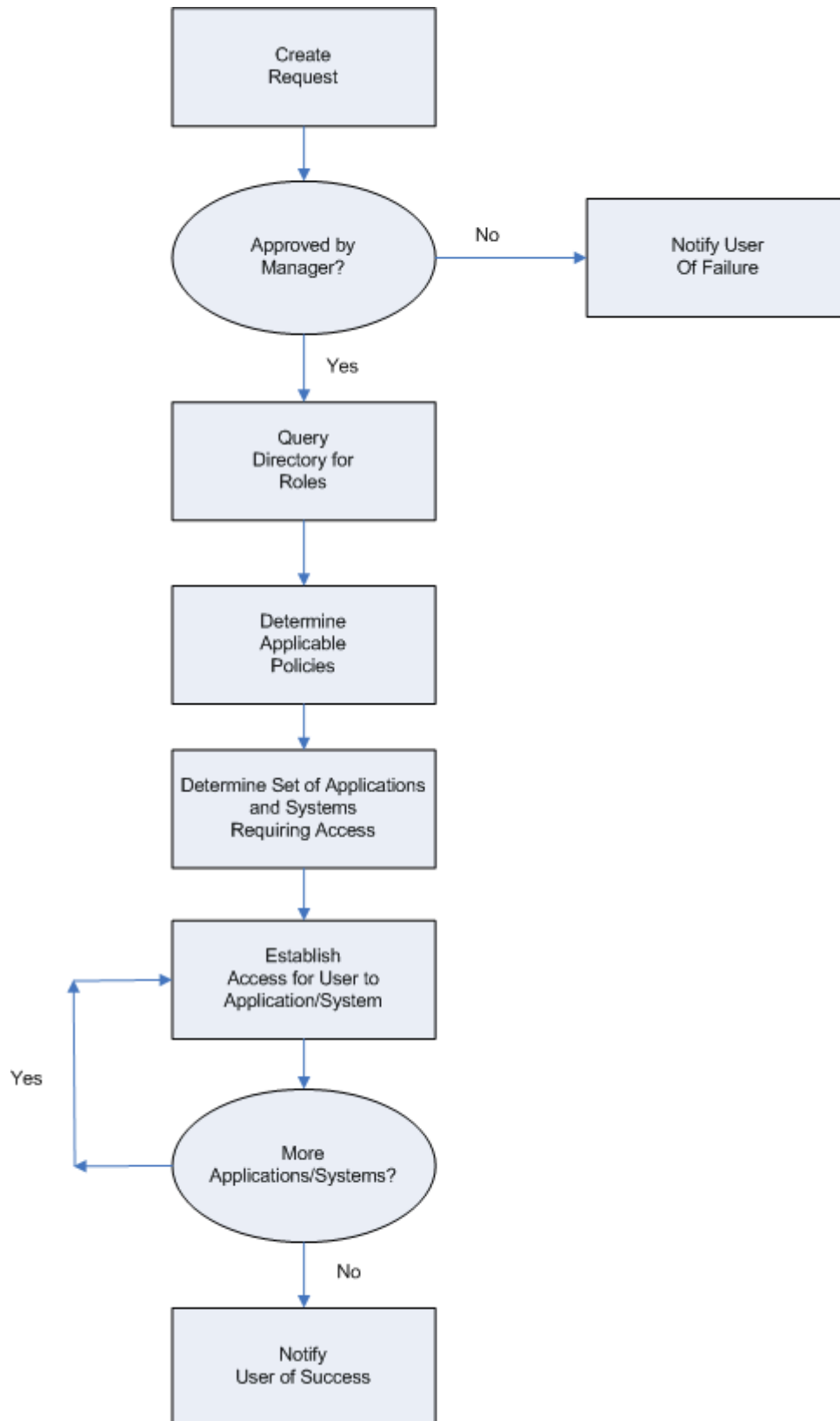


Figure 11.1: An example of user access provisioning workflow.

Automation in this process provides several advantages. First, although the time required to create user accounts may be relatively small, a large volume of transactions can result in significant costs over time. With support for password resets, a provisioning system can further reduce the cost of user access management.

A second benefit is improved quality control. The business rules governing user authorizations can be lengthy and in some cases complex. For example, authorizations may be granted based on employees' department, roles in the organization, and the projects they work on. It is more efficient to have an automated process querying a directory for user attributes and applying a policy using those attributes than having a system administrator manually checking detailed request tickets for specific details about system access. Consider: If a user had to specify which systems he/she needed access to, the list might include:

- Local PC
- Shared network drives
- An email account
- Group calendar
- Employee self-service portal
- Department-specific applications
- Project-specific applications
- Position-specific applications

Each of these may have different authorizations. For example, employees in IT may be given administrator or power user privileges for their workstations but others are not. Managers may have access to a project management application but other staff does not. By defining policies that specify authorization rules and applying them consistently with a workflow process, you reduce the likelihood of errors.

Patching and Upgrading Devices

In spite of efforts to standardize platforms, there will always be variations that must be supported. An organization may standardize on Windows and run Windows XP on most desktops. There are always exceptions though. Some are outside the scope of the normal device management process. For example, an IT lab may have devices running beta versions of Windows Vista. The IT staff working with these versions assumes responsibility for their management. But there are cases in which operational devices have to run a non-standard configuration:

- A legacy client-server application that will not run on an operating system (OS) later than Windows 2000 (Win2K)
- A rich Internet application that requires a different version of the Java runtime environment than the supported version
- A department application that is supported on Linux but not the distribution supported by IT

There are also variations among categories of devices. For example, mobile devices may require a virtual private network (VPN) client that is not needed on desktop devices.

Automation can reduce labor costs related to patching and upgrading by determining the current patch level of devices, allowing administrators to install software to specific devices based on current configurations, and, in general, reducing the average staff time required to perform patching and upgrade operations.

Again, as with user provisioning, quality can be improved. An automated process can detect failures in upgrades, roll back to previous configurations, and report the problem to a systems administrator. This process allows administrators to quickly detect common patterns in failures and revise the upgrade or patch scripts as necessary.

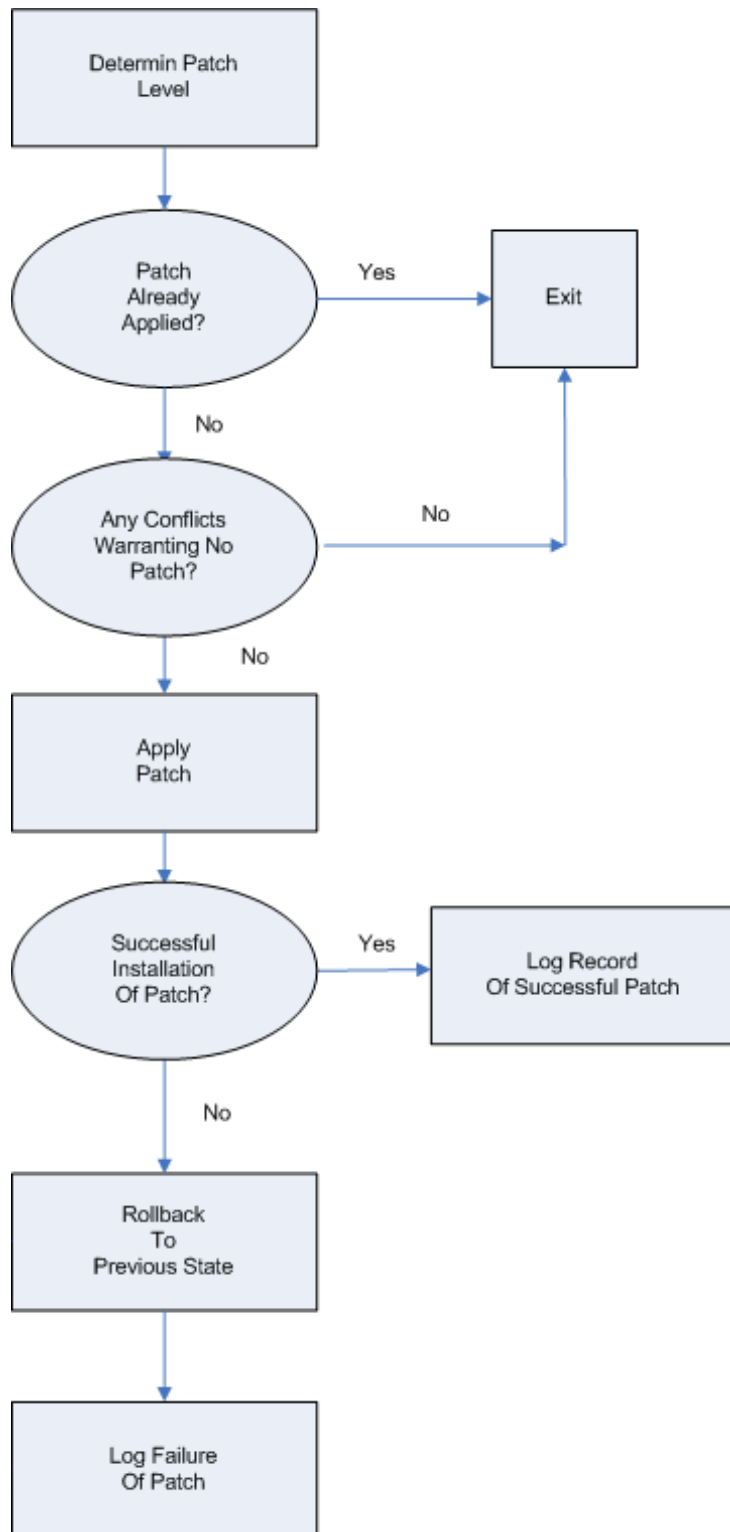


Figure 11.2: Patching and upgrading workflow.

Inventorying Assets

Tracking which devices are online is a fundamental operation; without accurate inventory data, other operations, such as patch management, lease management, license allocation, and security management, will produce suboptimal results, at best, and fail, at worst. In fact, inventory management is the foundation of asset management and begins with discovery of both software and hardware assets to populate the inventory.

As the number of devices in an inventory grows, the problem of tracking them obviously becomes more difficult. But quantity is not the only problem.

Configurations can change quickly. New software may be installed on client devices, OS configurations may change, and peripheral devices may be added to PCs and workstations. In addition, reorganizations, mergers, and divestitures can create an inventory management challenge because of the short time and large number of changes that can occur. Updating inventory with a large number of changes in a short period of time while maintaining sufficient quality controls is a task that can place a significant burden on IT staff. Again, automation can result in significant cost savings by reducing the number of staff required to manage inventory.

Troubleshooting

Troubleshooting is more difficult to operate than other operations, but supporting services can be automated resulting in reduced labor costs. Some troubleshooting problems are isolated to a single device. For example, a user may notice an increase in the time required to open local files, start desktop applications, and perform routine tasks. A review of the current configuration may determine that the recently added applications are taxing the device resource and additional memory is required. A Service desk technician may also notice differences in the configuration from the standard configuration, which leads the technician to investigate the possibility of a spyware or botnet infection. Having hardware and software configuration information from a configuration management database (CMDB) can reduce troubleshooting times in such cases.

Other situations are more difficult to diagnose. For example, users of an enterprise application may report slow performance. The application is a multi-layered system that includes:

- A Web client application
- A Web server
- A J2EE application server
- A messaging service
- A relational database

The slowdown could be caused by a problem in one of these components or in a combination. Troubleshooting multi-layered applications requires coordination of developers, database administrators, application administrators, and network support staff. This coordination is facilitated if a configuration database is available that tracks information across platforms.

Consider a potential problem with a critical system, such as a financial services application. What if a single configuration item fails, what is the impact on system availability? Will an essential business operation complete on time? Since the CMDB tracks configuration item relationships that define the service, technicians can quickly evaluate the impact of a potential failure and assess alternative solutions to work around the failure.

The potentially labor-intensive tasks—provisioning user access, patching and upgrading devices, inventorying devices and troubleshooting—are examples of common IT operations that can realize reduced costs if automated processes are in place. Another way the SOM model, coupled with automation, can reduce labor costs is through the facilitation of the development of cross-functional skills.

Cross-Functional Skills

IT professionals have come to expect frequent reallocation of staff as a strategic initiative change. Along with reallocations come the understanding that more and more tasks are being aggregated into fewer staff positions. This is part of the logic of improved productivity that is so important to remaining competitive. An important corollary to the idea of consolidating responsibilities is the need for cross-functional training.

Consider a systems administrator who had been responsible for managing a number of Linux servers that supported Web servers and application servers. The administrator is then assigned responsibility for a set of Windows XP servers used for network file shares. If this person is out sick, on vacation, or quits, who will run these servers? It is not practical to have another person on staff as backup. It is practical to cross-train others for the job.

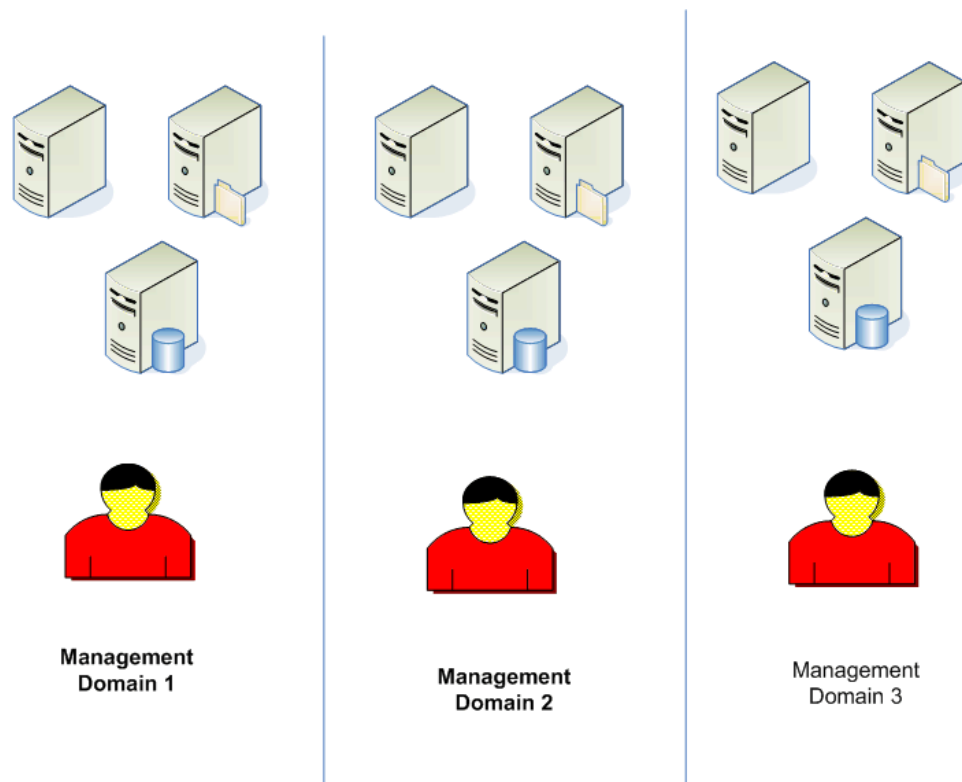


Figure 11.3: Without cross-functional skills, dependencies develop on single individuals or small groups.

The idea behind cross-training is that there is no dependency on a single individual to provide an essential service. If one systems administrator is away, another should be able to fill in. The problem is that the complexity of systems management makes it difficult to understand the depth and breadth of a wide array of systems. A Linux administrator may be able to pick up UNIX administrators' duties pretty quickly, but the same might not be said for a Windows administrator. Similarly, a Windows administrator familiar with supporting desktop devices may not be familiar with the intricacies of managing Windows servers running SQL Server or Microsoft Exchange.

The problem of maintaining adequate skill levels across multiple employees is reduced if low-level, tedious, platform-specific tasks are automated, leaving the higher-level analysis and management tasks to staff. For example, monitoring disk usage requires different commands under Windows than under UNIX and, depending on the reporting requirements, can require knowledge about specific parameters to command-line utilities. Rather than spending time scanning UNIX manual pages for the right parameter, a systems administrator's time is better spent addressing the core tasks and ensuring adequate disk space. Both Windows and UNIX administrators could perform basic monitoring tasks using a centralized management console with information about the status of various servers.

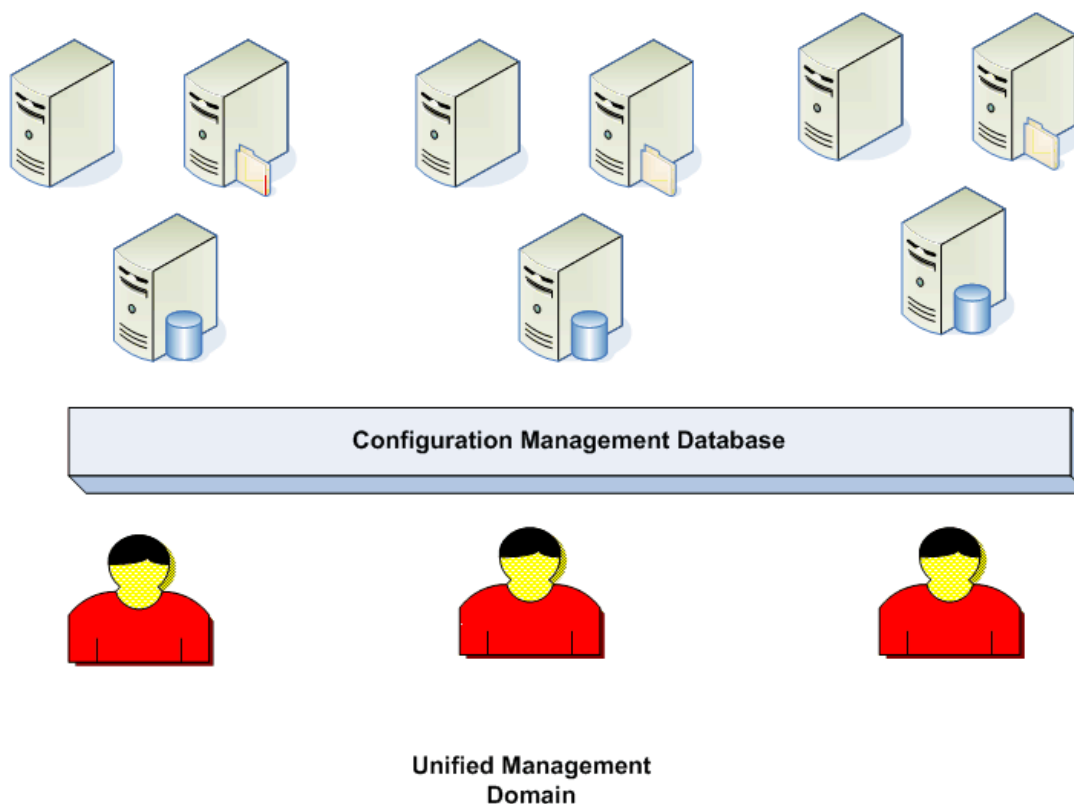


Figure 11.4: Using asset and configuration management tools can facilitate cross-training by alleviating the need to learn low-level, platform-specific details.

Using tools to perform low-level information gathering tasks is just one example of how systems management support tools can facilitate cross-training, which, in turn, can improve the overall quality of systems management and allow for consolidation of tasks across a smaller workforce.

Improved Support Services

The responsibility of IT staff does not end in the server room or at the workstation. Even if problems are addressed and systems are operating, if support customers are not satisfied, IT management will hear about it.

Support services are a critical component of IT operations and timeliness and quality are important elements of those services. This reality is evident in a number of ways:

- Response time to problem tickets
- Wait times when calling the Service desk
- The time required to troubleshoot and resolve problems
- System downtime
- Service provisioning

Often users will not care how a problem is resolved. What is important is that the problem is solved. If a user's workstation is unavailable because it has been infected with a botnet and a rootkit, how long will it take to service it? The user probably does not care about the details and challenges of detecting and removing rootkits, the user just wants the workstation back up and running with all of the previously available applications and data.

One way to clean the computer is to run anti-malware software to detect and remove as many rogue pieces of software as possible. Next, a systems administrator would have to review registry settings and manually check for hidden rootkit components—a time-consuming process that requires specialized skills. Alternatively, the systems administrator could format the OS drive, re-install the OS, and restore data files. This is a preferable option, assuming an automated backup process is in place to make copies of data files and a ghost image of the clean version of the OS and device-specific software is available.

The ability to roll back to a known-good configuration and restore users' data is just one example of how automated systems management processes can improve service support. Automating manual processes, supporting cross-functional training, and improving support services can reduce labor costs within IT departments. Improved support services can extend the reach of labor cost savings to user departments as well by reducing downtime and ensuring that operational systems are available when needed. Another area of potential savings is capital expenditures.

Capital Expenditures

Capital expenditures are expenses to acquire or improve long-term assets. These can include:

- Disk arrays
- High-end servers
- Enterprise applications
- Network devices

In budgeting, capital expenditures are often treated separately from operational expenses. Capital expenditures warrant detailed analysis because they are costly and commit the organization to a long-term investment. A formal, mature systems management model can help with capital expenditures in two ways:

- Improved asset management
- Decision support reporting

Improved Asset Management

After a capital asset has been acquired, management will expect that the asset is utilized as much as possible to realize the maximum return on the investment (ROI). IT capital assets are complex devices and how to get the most from them is not always obvious. Some capital assets, such as buildings and manufacturing equipment, are easy to assess. Is the building full? Is the manufacturing equipment producing its intended products? Measuring the utilization of IT equipment is not always so apparent:

- Is a firewall fully utilized if some features are not configured properly?
- Is a content filtering appliance fully utilized if it has only basic policies?
- Are software licenses fully utilized if some use the applications infrequently?

These questions demonstrate the problem of measuring the utilization of IT capital assets—the systems are so complex that there is not a single measure that can distill the relative value of an asset at some point in time. Rather a combination of measures is needed. An asset management system that includes information about both hardware and software utilization can help measure the utility of capital assets.

Hardware Asset Management

Capital expenditure management is not just about purchasing new equipment; it is also about managing existing assets. With the dynamics of today's organizations, it is likely that an asset will be reassigned to uses other than originally planned. Asset management systems can help with this process.

For example, a high-end server may have been allocated to a department with a large number of employees who used a custom application for its work. The department has since been restructured and the custom application replaced with an online service. Is the high-end server still required by that department? Could it be reallocated for another use, perhaps eliminating the need to purchase another server? Answering these questions requires information about the utilization of the server, the number of registered users, and planned projects in the department's pipeline that might make use of that server. Some of these questions can be answered with the right asset management and performance management data.

Sound hardware asset management practices are essential for organizations that lease hardware as well as those that purchase it. Leasing is a common method for reducing costs, but the practice introduces additional tasks, such as managing lease returns, which can be well served by centralized asset management procedures. Of course, not all capital assets are hardware.

Software Asset Management

Better software management is also an important aspect of capital expenditure management. Effective software management practices are important because software licenses are abstractions that do not take up room in a server rack or on a user's desktop. A single copy of an application may be installed multiple times, sometimes in compliance with license agreements and sometimes not. Tracking both licenses and software installations are important parts of asset management.

Automated tracking of software assets has several advantages:

- Better allocation of software licenses
- Providing information that can potentially lead to volume licensing discounts
- Decreased support costs due to better information for Service desk staff
- Improved security with the ability to rapidly identify instances of vulnerable applications
- Better license compliance
- Develop hardware refresh cycles to help predict purchasing needs
- Understand application usage—are there enterprise applications that only require read-only licenses?

Of course, a software asset management system can also provide information needed to justify additional software purchases when needed. This falls under the other broad benefit of capital expenditure management, improved decision support reporting.

Decision Support Reporting

When planning and budgeting for capital expenditures, you need accurate information about existing assets, how they are utilized, and expected changes in demand for services provided by those assets. A framework for systems management, such as SOM, can address these needs by answering questions such as:

- What hardware in the inventory meets the requirements of a proposed project?
- How is that hardware allocated?
- Is any of the hardware underutilized?
- If so, can it be replaced by lower-end hardware, freeing the higher-end hardware for the proposed project?
- If not and new hardware must be acquired, are ancillary resources, such as disk arrays, in place and do they have sufficient capacity to support the new project?

Many of the same details that can be used in operations management are also useful for long-term asset management; furthermore, many of the advantages found in capital asset management have parallels in operational aspects.

Operating Costs

The last type of cost in IT is operating costs, or the cost of running the IT department on a day-to-day basis. Labor costs are typically considered part of operating costs, but in this discussion, labor costs have been treated separately. This section deals primarily with the remaining types of operating costs. Specifically, this section examines how a mature systems management framework can improve cost controls by improving several areas:

- Management reporting
- Allocation of resources
- Predictability of operations
- License management
- Security posture

Improved Management Reporting

IT management reporting for systems management can be boiled down to three simple questions:

- What do we own?
- Where is it?
- How is it being used
- How much is it costing?

Everyone running an IT department needs to answer these questions, but how they are answered is, in part, a function of how IT operations are managed.

A common problem with management reporting is that silos of management form within organizations. Responsibility and control of operations need to be divided among managers, and how it is divided is somewhat arbitrary. For example, one business might divide along OSs with one group responsible for Windows systems, another for UNIX/Linux systems, and yet another for mainframe devices. In other cases, the division may be along functional lines with client devices managed by one group, Web servers and application servers managed by another, and database servers are under the control of a third group. There are good arguments for all of these arrangements and one is not necessarily better than the others; however, they all suffer from the same potential pitfall: silos of management.

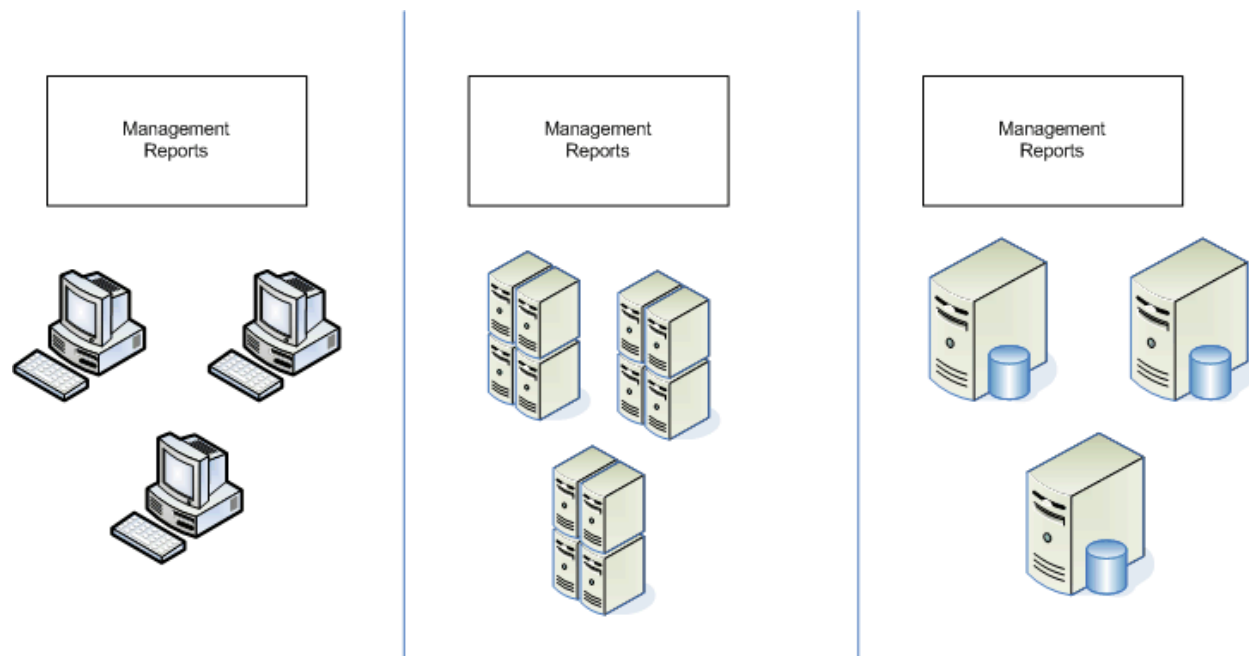


Figure 11.5: Silos of management have advantages but can make management reporting more difficult than it needs to be.

A restructuring is likely to lead to different silos without actually solving the management reporting problem (something of a “rearranging the deck chairs on the Titanic” solution). A better option is to use a centralized configuration database that can collect and manage information about assets across organizational boundaries. This option has several advantages:

- It is independent of organizational and management structure
- It allows for consolidated reporting
- Reports are consistent across management domains
- More in-depth analysis, such as dependencies between systems and resources, is possible

Figure 11.6 shows an example of the types of information that can be collected and managed within a consolidated centralized management database.

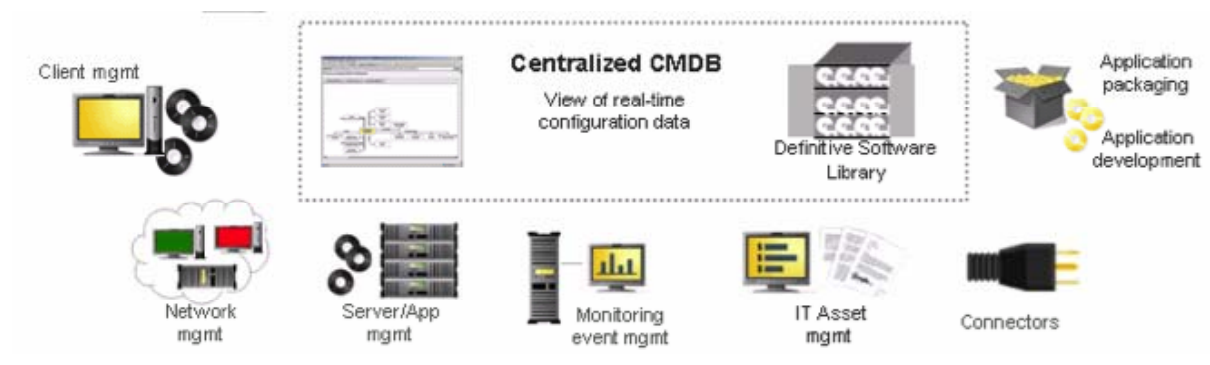


Figure 11.6: A centralized configuration management database can collect and maintain information about assets across organizational boundaries and support improved management reporting.

Improved Allocation of Resources

Allocating resources is fundamentally a problem of getting the right device to the right place at the right time. This, in turn, becomes a problem of understanding the

- Inventory of assets
- Needs of particular users, groups, and applications
- Total life cycle cost of assets
- Relative value of services rendered by allocating particular resources to particular needs

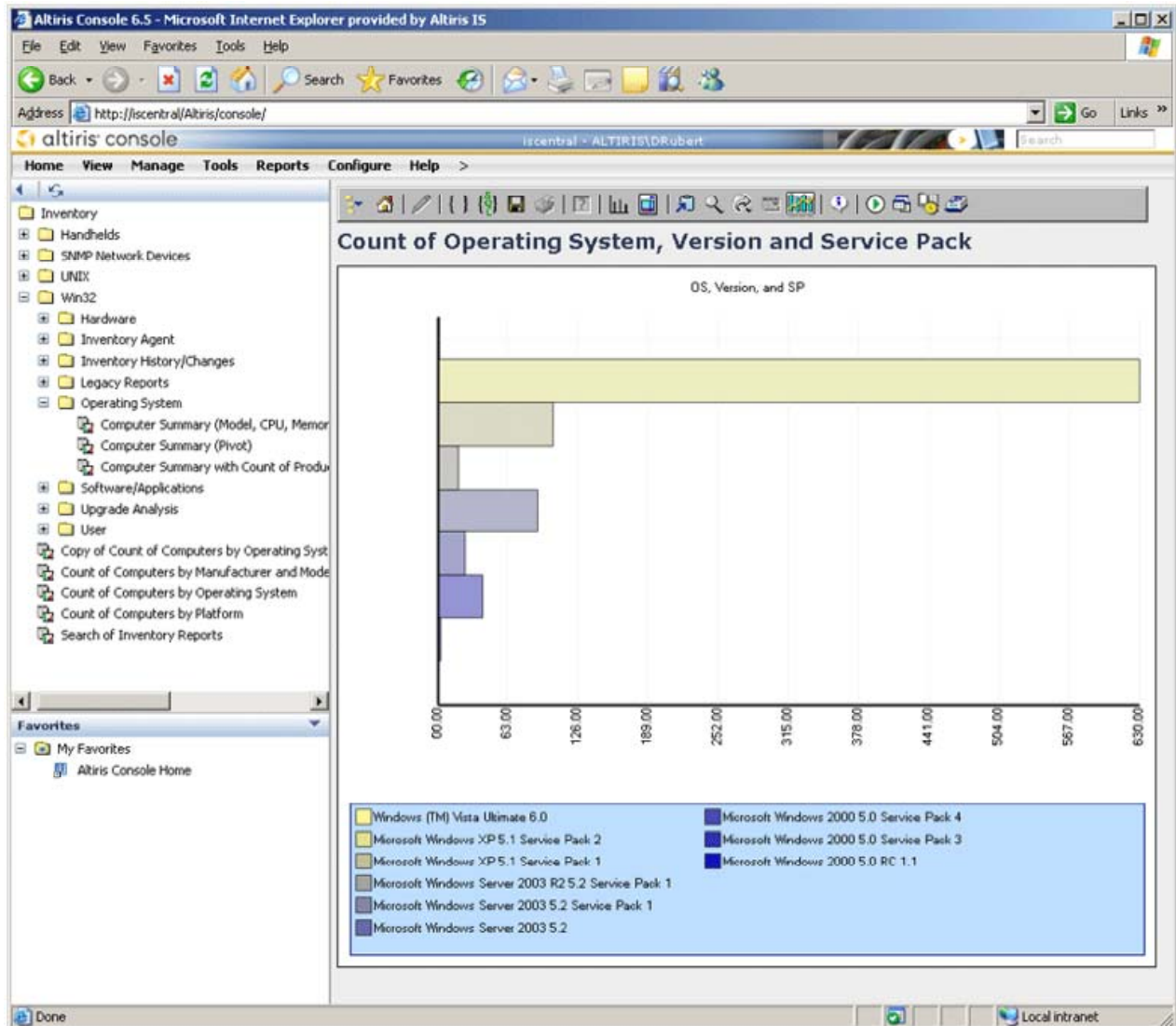


Figure 11.7: Knowledge of the types of assets in the inventory is the first step to optimizing the allocation of resources.

Understanding the value of particular operations, such as improving services in customer relations versus deploying additional servers to a database cluster in finance, is a business decision that expands beyond systems management. It does, however, require the kind of data that systems managers can provide:

- Cost of procuring the assets
- Cost of maintaining the assets
- Cost of end-user support for assets deployed to particular uses
- Cost of depreciation
- Cost of disposal

A centralized management model that includes inventory and cost information can greatly facilitate the financial analysis that must be done to optimally allocate resources. Much of the same data that is used for optimizing the allocation of resources is also useful for predicting time requirements and levels of effort required for systems management operations.

Improved Predictability of Operations

The saying “Those who do not remember the past are condemned to repeat it” has a corollary in the IT realm: “Those who do not measure the past are condemned to repeat it without guidance.” Consider some of the common and repetitive tasks that IT operations have to contend with:

- Patching applications
- Upgrading OSs
- Installing applications
- Resetting passwords
- Installing and configuring client devices
- Hardware refresh cycles

Managers are constantly planning for these kinds of operations. To do so successfully, they require raw data that can answer questions such as:

- What is the average time to push a Microsoft Office patch to remote users?
- What percentage of OS upgrades failed on notebooks?
- What is the average time required by Service desk staff to reset passwords?
- How many mobile devices still have to be patched with a security update?

Again, a centralized repository of asset and patch management information can provide the raw data needed to answer these questions. Although benchmarks and industry standards are good guides for planning and budgeting purposes, when it comes to day-to-day operations in which the margin between staying on budget and having an overrun is thin, having detailed information about past performance is essential. Another area in which detail management can directly impact the bottom line is with software license management.

Improved License Management

Managing licenses is a high-value proposition. It allows IT departments to show quick return on investment (ROI) and adeptly reallocate licenses as business needs change. At the same time, neglecting license management leaves an organization liable for violation of contracts if more copies of software are in use than are licensed.

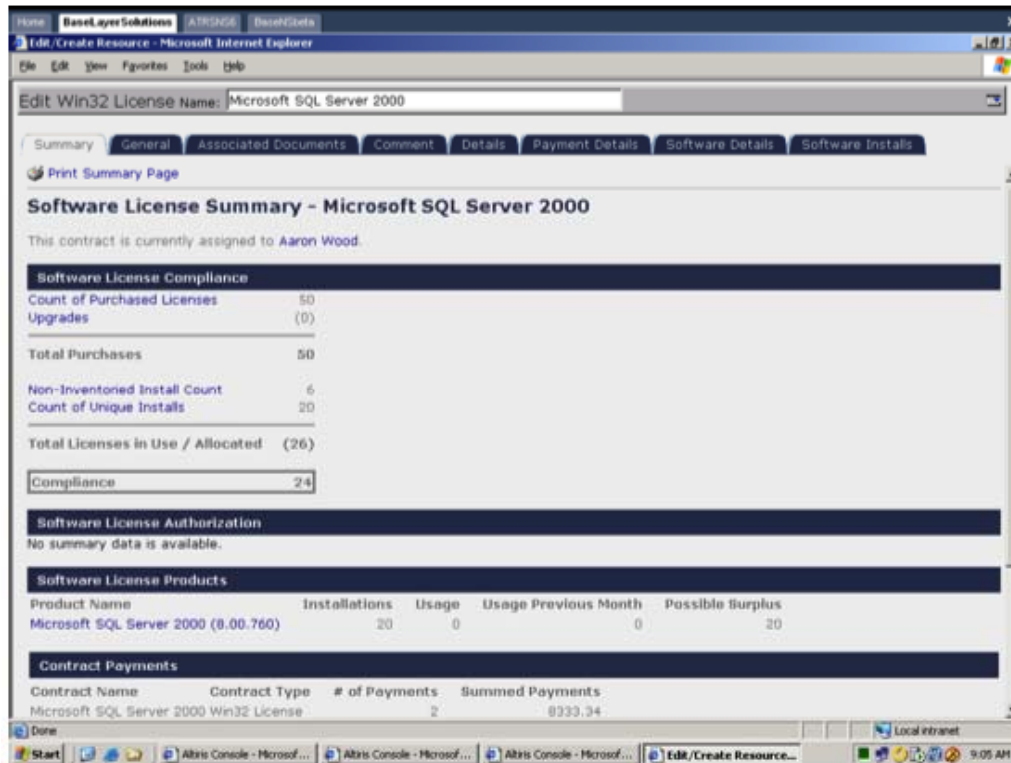


Figure 11.8: Software license management can track usage against licenses and help administrators remain in compliance with contractual agreements.

Improved Security Posture

Proper systems management practices can help to improve and then maintain a sufficiently secure environment. Systems management supports network and device security in several ways:

- Patching applications and OSs
- Maintaining proper configurations
- Monitoring activities and resource utilization
- Establishing and enforcing policies for network and system access
- Ensuring business continuity through backup and recovery procedures

These management areas are important to security because, as is well known, information security requires multiple layers of defense to mitigate the potential for a “weakest link” problem. For example, if a network worm is exploiting a known OS vulnerability and the only defense is the antivirus software running on desktops, any problems with that antivirus program could result in infection. It is not difficult to imagine, for example, a notebook without updated antivirus signatures that would miss detecting the worm and leave the notebook vulnerable. A comprehensive systems management program can mitigate this type of potential problem by


- Ensuring OS patches are up to date
- Allowing systems administrators to quickly identify devices that do not have up-to-date antivirus programs
- Providing better reporting on system accounts, increasing the chances of detecting unauthorized accounts
- Supporting the enforcement of least privileges, so if a system is compromised, the processes running on that device cannot do widespread damage

Let’s examine the problem of systemic vulnerabilities. Vulnerabilities are weaknesses in systems that can be exploited to compromise the integrity, confidentiality, or availability of a system. Vulnerabilities are created by

- Errors in applications
- Incorrect configurations
- Deficiencies in procedures

All these potential sources of vulnerabilities can be compensated for by proper systems management (at least to some degree). Patch management is especially important with the first problem, errors in applications. Applications today are increasingly complex, they are deployed on a variety of platforms, and they are often designed and developed under tight deadlines that leave too little time for comprehensive testing. The result is that serious flaws creep into the software and are eventually deployed across enterprise IT systems.

Vendors regularly patch software. Microsoft, for example, has regular monthly updates. Other large vendors, such as Oracle, use a quarterly schedule. Of course, high-risk vulnerabilities may be corrected outside of this schedule. These types of regular updates allow systems administrators to plan for updates so that patching does not have to be an ad hoc, disruptive process.

 Zero-day vulnerabilities are particularly problematic because they are unknown to vendors and customers until attackers or malware developers exploit them. By definition, there are no patches for zero-day vulnerabilities when they are exploited. This is one of the reasons that defense-in-depth security strategies are so important. No one security method, such as patching, is effective all the time against all threats. Only by combining multiple countermeasures can an organization achieve reasonable levels of security.

Security professionals often advocate defense-in-depth strategies. This advocacy should not be misconstrued as a call to simply implement more security applications, such as firewalls, antivirus solutions, content filters, intrusion prevention systems (IPSs), and a host of other tools. You certainly need those, no question—but you also need sound systems management.

A network fully loaded with the latest security countermeasures will not be secure if the network devices and servers are misconfigured, if client devices are not patched, if applications are not using authentication and authorization mechanisms, or if tested backup and recovery procedures are not in place.

The benefits of a methodical systems management approach touch numerous parts of IT management, from the allocation of resources and the predictability of operations to improved software license management and systems security. Just as any coin has two sides, so does the story of IT costs and systems management. The other side is the cost of not properly managing systems operations.

Cost of Not Controlling IT

The majority of this chapter has been dedicated to describing the benefits of a comprehensive approach to systems management, but a brief examination of the consequences of not following such a regimen can also be enlightening. There are at least four areas in which poor systems management can have a direct impact on the bottom line of an organization:

- Compliance
- Loss of system integrity and availability
- Loss of confidential and private information
- Loss of service and business disruption

The relative importance of each of these will vary by industry and market, but they can all have substantial impact on some groups of IT operations.

Compliance

Regulatory compliance is something we have all come to expect and live with. Some regulations are broadly applicable to a large number of organizations. The Sarbanes-Oxley Act, for example, requires adequate controls on IT operations to ensure the integrity of financial reporting of all companies publicly traded in the United States. Businesses are not the only ones subject to regulation: governments establish regulations for themselves as well. The Federal Information Security Act (FISMA) defines security requirements for U.S. federal agencies and departments. Some regulations targeting particular industries worth noting are:

- Health Insurance Portability and Accountability Act (HIPAA)—health care
- 21 CFR Part 11—pharmaceuticals
- FISMA—U. S. federal government
- Gramm-Leach-Bliley Act—financial services

When considering the impact of compliance, consider (at least) two parts: the initial fines and other costs of a violation and the cost of cascading violations. For example, a violation of HIPAA can result in stiff fines when protected health care information is disclosed. However, a violation of a state's privacy statute can result in fines and may trigger the violation of another federal regulation, such as the Gramm-Leach-Bliley Act, which results in additional fines. Effective systems management practices will not guarantee that an organization is in compliance but can provide the tools and management reporting necessary to get into compliance and demonstrate that compliance.

Loss of System Integrity and Availability

Another general downside of poor systems management is that information could be compromised or systems may be unavailable. System integrity is compromised in several ways, including when

- Data is tampered with and changed in unauthorized ways
- Applications and OSs do not function properly because dependencies are not understood, managed, and maintained
- Applications do not function properly because updates and patches are not applied properly

Closely related to system integrity is system availability. In this case, potential problems with availability stem from:

- System downtime due to virus, Denial of Service (DoS), or other attacks that may have been mitigated by proper systems management and security procedures
- Unstable applications that crash because of misconfiguration
- Insufficient performance because growth in use trends have not been monitored and insufficient resources are in place to accommodate demand

A well-managed systems administration program will not guarantee that systems never crash or that performance will degrade, but it does mitigate the possibility of those problems.

Loss of Confidential and Private Information

Losing confidential and proprietary information can be costly. In the case of confidential information, especially personally identifying data, the loss can lead to violations of regulations. Governments from the state to the national and transnational level are establishing privacy protections for their citizens. A combination of security measures and supporting systems management services can again, as with the loss of integrity and availability, mitigate the worst impacts of such a potential threat.

Business Disruption

Yet another factor to consider when determining the cost of systems management is the potential for business disruption. When information systems are down, the impact can be widespread, shutting down day-to-day operations as well as adversely impacting management operations. Often businesses will invest in backup solutions, offsite facilities, and other measures in case of disaster. The transition from primary to backup systems can be difficult in the best situations, but without proper planning and management, they may be impossible to implement without adverse consequences.

Clearly, there are costs associated with implementing comprehensive systems management models such as the SOM model. There are, however, even greater potential costs for not implementing such models.

Summary

The benefits of mature systems management practices are well known. Labor, capital expenditure, and operational costs all benefit from such practices. In the case of labor, the automation of manual tasks, improved cross-functional training, and improved service support follow. Capital expenditures benefit from better reporting and decision support. Day-to-day operations benefit in several ways ranging from better allocation of resources and license management to improved security and operational predictability. Finally, consider the cost of not leveraging systems management best practices, which, in addition to the lost opportunity for improvement, brings costs all its own.

Download Additional eBooks from Realtime Nexus!

Realtime Nexus—The Digital Library provides world-class expert resources that IT professionals depend on to learn about the newest technologies. If you found this eBook to be informative, we encourage you to download more of our industry-leading technology eBooks and video guides at Realtime Nexus. Please visit <http://nexus.realtimepublishers.com>.