How Risky is Your IT?

A Report on What Organizations are Doing to Manage Risk and Vulnerabilities

EVALUESERVE
Your Global Knowledge Partner

Table of Contents

Executive Summary

This global study by Evalueserve shows how IT decision-makers assess the current state of risk management with a focus on challenges of implementing and sustaining an effective program from a risk, vulnerability and patch perspective.

Perhaps the single most important element of a sound risk management program is to know which IT assets – the applications, data stores and systems that make the business go – are critical to the continued health and success of the enterprise.

Businesses operate in a hostile, globally connected environment of cyber criminals who are constantly probing and penetrating their networks with the intent of doing harm. But security is expensive and time consuming. Diligent risk management enables organizations to allocate resources where they will provide the greatest benefit to protect the business.

Accurate information about the importance of IT assets to the business, the severity of vulnerabilities in those assets, and the likelihood of exploitation enable corporations to make intelligent, informed, risk-based decisions on where and when to commit mitigation and remediation resources. A sustainable, continuous program of asset identification and classification, threat evaluation, risk assessment, monitoring and validation will significantly improve the organization's security posture and enable compliance with regulatory mandates, as well as facilitate business productivity.

In their responses to this survey, enterprise IT leaders and managers demonstrate the value of risk management programs that reflect an intimate understanding of and visibility into their operations that enables them to:

- Assess their vulnerability
- Prioritizing the threats against them
- Take effective remediation steps

This survey provides insight into how tools such as risk analysis, vulnerability scanning and patch management products can help, and what organizations should expect and demand when making purchase decisions.

Specifically, the survey showed:

- Organizations are keenly aware of the importance of high visibility into their risk posture, but few feel they have achieved that level of insight.
- Users of risk management products generally feel more confident about their knowledge of what assets are at risk, the threats against them and their ability to protect their business against those security threats.
- Most enterprises expect timely ROI on their risk management investments, and cite ***Cost*** most frequently among the factors in product selection.
- Patching, especially out of cycle, eats up heavy corporate resources. Organizations that use risk management products are particularly interested in reducing patching frequency.
- Companies expect their risk management processes and products to produce detailed reports that provide specific information about their current risk posture and the effectiveness of their remediation efforts. Most of them look to their vendors for regular threat notifications.

Understanding Current Risk Posture

Organizations expend inordinate numbers of man-hours trying to understand the impact of threats on their environment. Nevertheless, they still have generally poor visibility into their network, system, application and database vulnerabilities, a somewhat deficient overall security posture and incomplete risk assessment. This section of the survey shows how greater visibility improves security and saves resources, and how risk management products enhance this ability and instill user confidence.

Insight into Enterprise Risk

Enterprises cannot efficiently address risk unless they understand what they are up against and can apply the appropriate controls. Without this knowledge, security efforts are likely to be dispersed and diluted or misdirected, putting resources into low-priority areas. The majority of companies surveyed appreciate this critical point. More than 50 percent of them believe that it is *very important* to know the risk they currently face, when and where to deploy a security product, and be aware of the threat levels of their IT infrastructure.

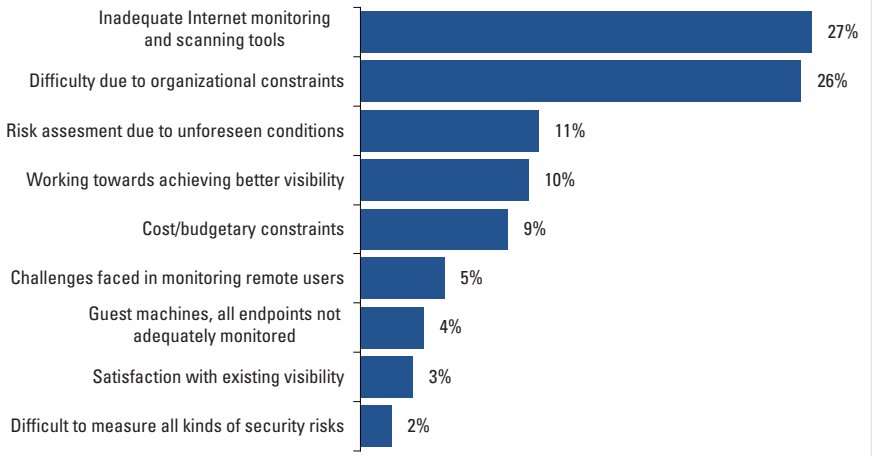
> "Only 10 percent of the companies surveyed said that they have a high visibility into the risk posture of their IT environment."

While 90 percent of organizations that use risk management products rate it very important to have visibility into risk posture of the company's IT infrastructure, among non-users, 13 percent fewer rate this as important. A similar gap is observed in importance of accurately knowing when and where to deploy security products for protection from possible threats.

However, while enterprises clearly recognize the importance of visibility into their risk posture as critical to knowing where and how to commit their security controls, few of them feel they have that visibility. Consequently, a substantial number are not satisfied with their risk management and security efforts. Only 10 percent of the companies surveyed said that they have a high (90 percent or higher) visibility into the risk posture of their IT environment. A significant 42 percent of organizations feel they are either "*inadequately protected*" against information security risks or are "*not fully aware*" of the risk posture of their IT environment.

CIOs and their peers cite multiple reasons (*see Figure 1*) for this inability. More than a quarter of the respondents cite inadequacy of Internet monitoring and scanning tools. Another fourth cite organizational constraints, such as large employee base and fragmented security operations, for low visibility into their IT risk posture.

Figure 1: Reasons for Low Visibility into Enterprise Risk Posture



Risk Management Products Make a Difference

Despite these obstacles to visibility into risk posture, enterprises using risk management products feel a lot better about their security. The survey revealed that 62 percent of these organizations have greater confidence about their protection against and awareness of IT security risks. Only 44 percent of those who do not use risk management products have that level of confidence.

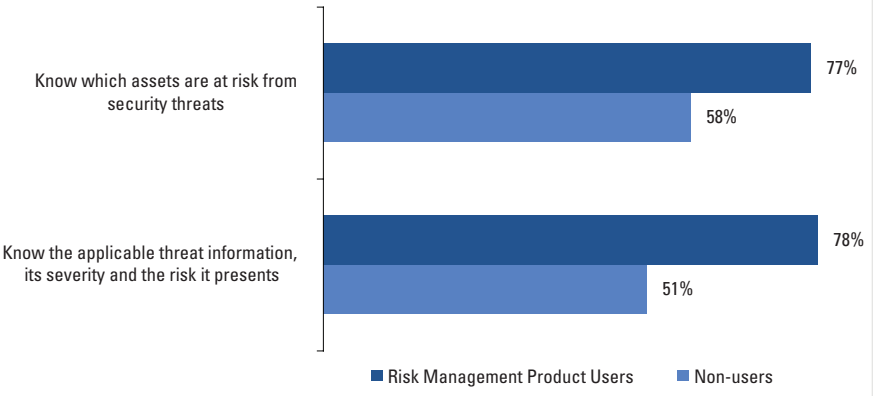
In addition, more than three-quarters of enterprises that use risk management products are confident of not only having specific knowledge on the assets at risk, but also detailed information about applicable security threats, their severity and the risks they present (*see Figure 2*).

"Eight out of 10 CIOs and their peers believe increased visibility into the IT risk posture can save their team up to 10 man-hours a week."

In contrast to this, enterprises that do not use risk management products are far less likely to understand the security threats and the risks they pose.

> "Eight out of 10 CIOs and their peers believe increased visibility into the IT risk posture can save their team up to 10 man-hours a week."

Figure 2: Knowledge of Threats and Risks



Source: Evalueserve Primary Research, 2009

This pays off in lower cost as well as better security and risk management.

Enterprises agree that identifying threats is difficult and labor-intensive, and therefore greater visibility into the threats across their networks can save valuable man-hours spent in managing IT operations. Eight out of 10 CIOs and their peers believe increased visibility into the IT risk posture can save their team up to 10 man hours a week.

Consider, then, that tools such as vulnerability scanners and patch management products provide detailed information on current vulnerabilities and remediation, providing critical insight and automating time-consuming risk management tasks. It's not surprising that users of risk management products have greater clarity around such savings. A quarter of them say greater visibility will save man-hours, double the number of non-users who hold the same opinion.

Security Solutions Deployed

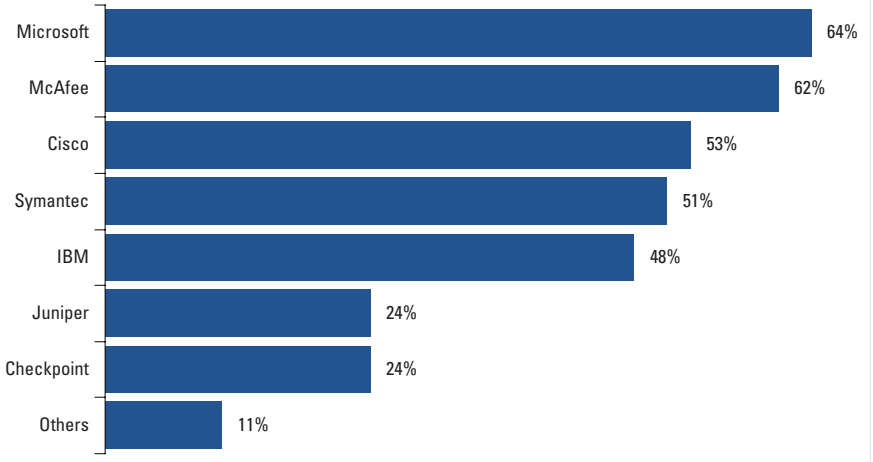
Enterprises have deployed multiple products from a wide range of vendors to counter security threats.

Almost all companies use anti-virus software. Network and Web application firewalls rank second in adoption, as 84 percent of the companies surveyed are using these products.

Around 80 percent of the companies say they use some sort of products that help address governance, risk and regulatory compliance. About half use patch management (49 percent) and risk management (51 percent) tools. Another one-third said that they are planning to install at least one of these over next six months.

Almost two-thirds of the respondents (*see Figure 3*) use Microsoft and McAfee security products. About half the companies use security products from Cisco, Symantec or IBM.*

Figure 3: Security Providers Used by Organizations



Source: Evalueserve Primary Research, 2009
** Multiple selections of products by a respondent was permitted*

> 80 percent of the respondents believe the payback period for IT security products should be less than 12 months.

Measuring ROI on Security Products

Although ROI on security products has often been considered difficult (some have compared it to buying insurance), IT professionals not only demand the products pay for themselves, but an overwhelming majority (80 percent) believe the payback period should be less than 12 months.

Users of risk management products rate ROI as very important - 89 percent compared to 66 percent of those who do not use risk management products.

Companies surveyed measure their returns on security products on analysis of three broad parameters – benefit, loss and incidence:

Benefit analysis: The products are measured on their performance against security threats/attacks, savings achieved in operational costs, and capital expenses. Measurements should also include reduced downtime and increased productivity.

Loss analysis: This is the "insurance" part of the equation, as companies study the impact on their business of security incidents that could be averted or more quickly detected and remediated by having particular security products. Loss factors include reputational risk indicators (brand damage, etc.), cost of lost productivity and loss of business (sales, contracts).

Cost of incident analysis: Companies should measure the mean time between security incidents and full recovery. This analysis includes the number of employees affected by the incident: How many employees will lose use of applications and data that are essential to performing their jobs, and for how long?

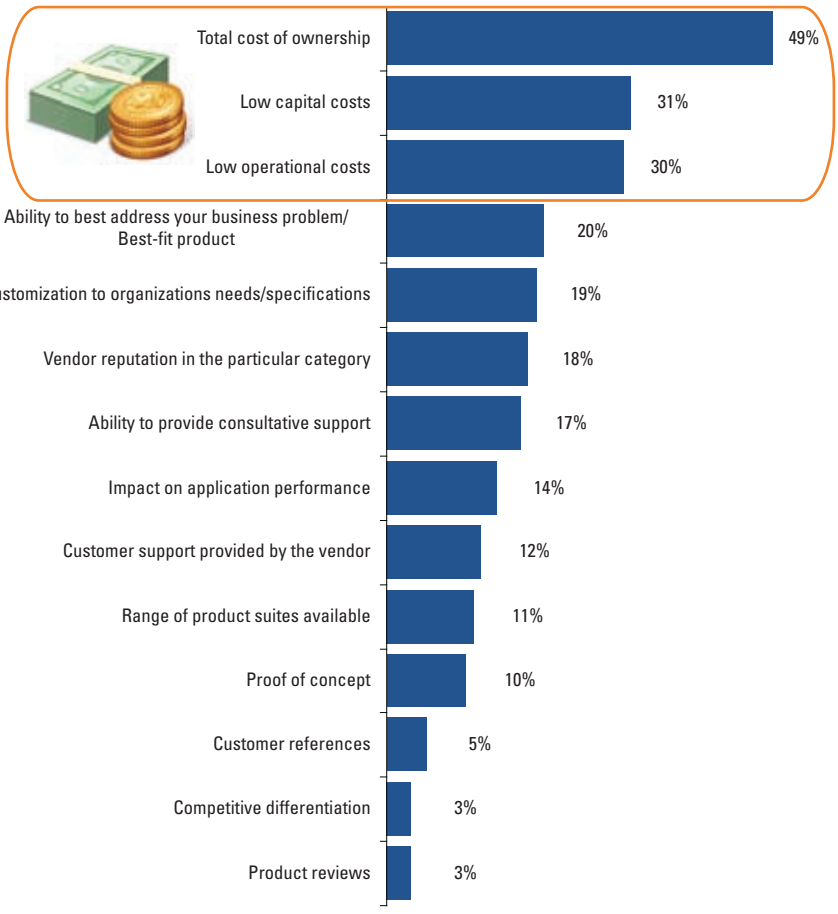
> “Half of those surveyed cite total cost of ownership as the top factor in selecting a risk and vulnerability management solution.”

Factors Determining Selection of Risk and Vulnerability Management Solutions

Beyond these general factors in determining ROI for security products, CIOs and their peers consider a number of factors before they zero in, in particular, on a risk and vulnerability management solution for their company. Consistent with the demand for timely ROI, companies place a premium on cost.

About half of those surveyed (*see Figure 4*) cite total cost of ownership as one of the top two factors. Capital and operational costs are the next two critical factors that companies look for when evaluating these products. Apart from these, respondents considered how well the product addresses their organization's requirements and environment and flexibility around customization to its specific needs as critical factors influencing their purchase.

Figure 4: Factors determining risk and vulnerability management solutions



Source: Evalueserve Primary Research, 2009

The decision factors that go into selection of risk and vulnerability management products and assessing their ROI are similar to the criteria for many other products. Organizations will not allow FUD (fear, uncertainty and doubt) to rush them into purchasing security products, and they demand measurable and timely ROI.

Patch Management

Patching is an integral component of the risk management lifecycle. It is not a simple operational procedure. It involves a lot of sub-activities such as reading the bulletin, downloading the patch, and deploying it across corporate networks. Patch management is a necessary evil – an ongoing and draining exercise – requiring testing of patches to avoid "breaking" critical applications and systems, and verifying that the patch has been successfully installed on each system. If the operation fails, administrators have to spend hours in determining the cause, rectifying the problem, reapplying the patch and verifying (again).

Therefore, organizations are obliged to prioritize patches based on risk: Which systems are actually vulnerable? Of these vulnerable systems, which are critical to the business? Which of these are most likely to be exposed to exploit?

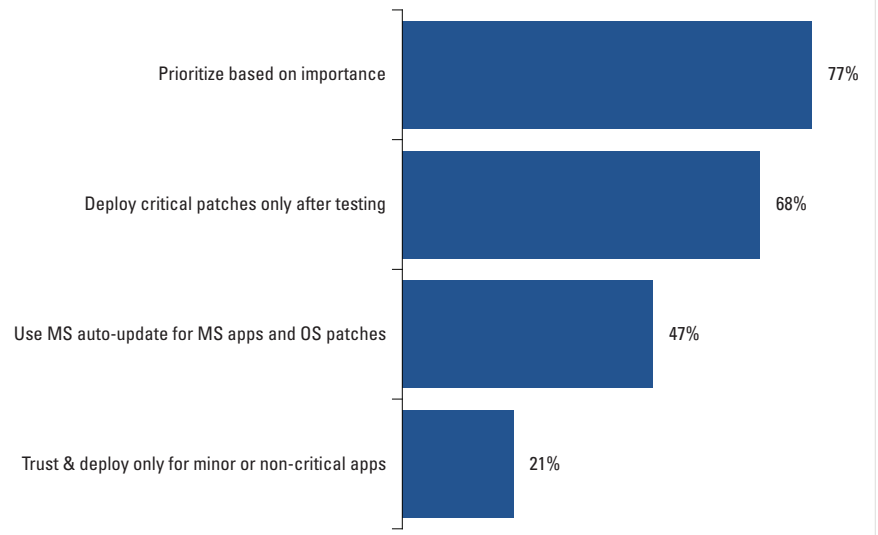
> "Enterprises are divided on how they treat patches and prioritize what to patch and when."

Which Patches – and When?

Enterprises are equally divided when it comes to how they determine criteria for prioritizing and deploying patches. Half of those surveyed treat all different classes of patches alike, while the others use a more discriminating approach. Companies that use risk management products are more likely to classify and prioritize patches than those who do not.

Organizations use several approaches to patching policy and practices (*see Figure 5*). Three-fourths of the respondents prioritize patch deployments based on their importance; 68 percent test prior to deploying the patches.

Figure 5: Patch Differentiators



Source: Evalueserve Primary Research, 2009

Security Burden: Patching/Updating & Fixing Vulnerabilities

We asked enterprises about their programs to counter growing security threats. Here are a few points that stood out:

- Update overnight to ensure systems are current
- Patch every system on a monthly basis
- Patch immediately upon receiving a high-risk alert
- Ensure OS updates are current, along with latest DATs
- Issue automatic and regular updates

Patching helps enterprises keep their systems' security up to date: Eight of 10 CIOs and their peers felt confident of their systems' protection after patching. A miniscule percentage cited non-uniform and ineffective patching upgrades as a reason for not being confident after upgrading their systems with new patches. Companies that do not use risk management products are less confident of their systems after patching as compared with users of risk management products.

Though frequent patching is obviously a high priority, it is a significant drain on time and resources. Most organizations (70 percent) spend up to 15 hours on each round of patch deployment. Two-thirds run these at least twice a week.

It stands to reason that 58 percent of the organizations stated that they would prefer to reduce that frequency. That's more of a priority to users of risk management products, 66 percent of whom felt reducing patching frequency is important, compared to 40 percent of those that do not use risk management products.

In fact, risk management products can help organizations streamline their patch management programs by automating the discovery of vulnerable systems, remediation and verification of patch operations.

Out-of-Cycle Patches

Many companies are not up to speed on the threats that can be prevented with out-of-cycle patches. Half of the organizations said they are not fully aware of these risks to their IT assets. Not surprisingly, the proportion of companies that admitted to this low awareness is higher among those that do not use risk management products.

> "41 percent of respondents who said the out-of-cycle Conficker patch was disruptive reported serious impact to their business."

It is revealing that a third of those who initially claimed in the survey that they are well protected against IT risks admitted heir lack of awareness about the importance of out-of-cycle patches. As you would expect, the figure is much higher (69 percent) among those respondents who initially said that they are not fully informed about their IT security risks.

More than half of the organizations said they immediately deploy an out-of-cycle patch only if it is critical, while a third deploy it immediately regardless of its criticality.

This overall caution reflects the negative impact of these patches, even if they are of critical security importance. More than half of the organizations surveyed expressed concerns around costs and disruption associated with out-of-cycle patches.

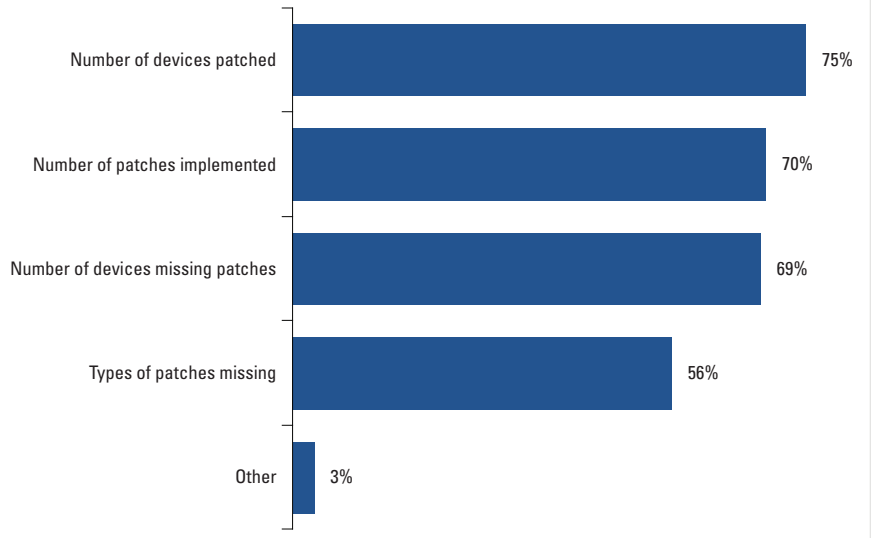
Last year's Conficker outbreak (MS08-067) is a prime example of the trouble out-of-cycle patches can cause if they do not fit into regular patching schedules, which generally allow organizations to patch during off-peak business/production hours and thoroughly test patches before deployment. Three-fifths of the organizations said the out-of-cycle Conficker patch deployment was disruptive; 41 percent of these reported serious impact on their business operations, including:

- Data loss
- System crashes
- Service interruptions
- Productivity loss
- Remote endpoints affected
- Disruption of planned activities
- Increase in IT management and security costs

Patch Management Reports

Accurate and detailed information is critical to the risk management process. Enterprises expect reports generated after patching to show their updated risk posture (*see Figure 6*). Most want to know the number of devices that have been patched; the number of patches implemented and the number of devices which are missing patches. In addition, more than half want to be told the types of patches missing.

Figure 6: Patch Differentiators



Source: Evalueserve Primary Research, 2009

Patch Management Preferences

Enterprises were divided about their preference for patch management solutions: 40 percent prefer hardware devices for this purpose, while 31 percent prefer software. Another 29 percent of the companies favor hosted services. Interestingly, just 12 percent non-users of risk management products expressed their preference for hosted solutions.

Organizations show considerable diligence in patch management and considerable distaste for the time and energy they devote to it. Organizations that use risk management products demonstrate their solid, process-based foundation by relying on testing and prioritizing patching, aided by the tools that gather relevant information and the automation that gives them time to follow ordered procedures.

Vulnerability Management

> “Eight out of 10 organizations feel it’s important to understand vulnerabilities in relation to critical assets.”

Vulnerability management is all about risk: What assets are at risk and how vulnerable are they? Are they mission critical? What is the business impact if the assets are down for any length of time? These considerations create the corporate security policies and compliance mandates that drive vulnerability management programs, specifically the use of vulnerability scanning tools.

Importance of Understanding Vulnerabilities and Their Management

The security risk of any particular vulnerability is based on the severity of the flaw, the likelihood of a successful exploit and, perhaps most important, the criticality of the asset that could be compromised. A browser flaw that endangers corporate intranet with company news is one thing; if the same flaw allows an attacker to exploit a critical online production Web application. It’s quite another.

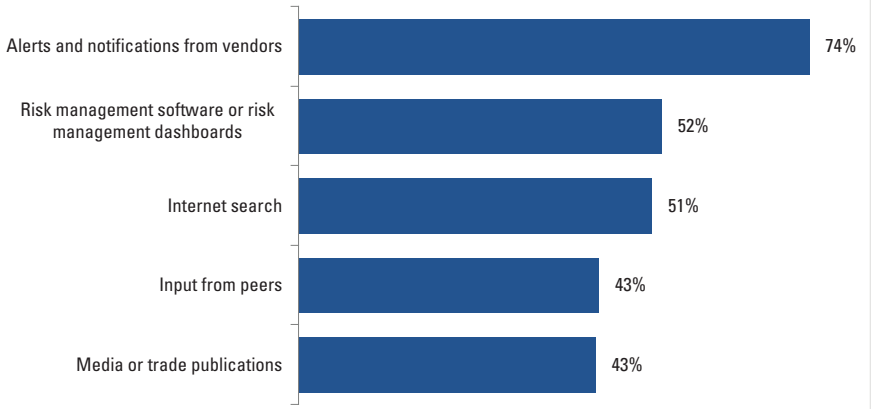
Seen in this light, it’s obvious why eight out of 10 organizations feel it’s important to understand vulnerabilities in relation to critical assets. While 85 percent of users of risk management products feel this is important, significantly fewer non-users (68 percent) perceive this to be important.

The top five vulnerabilities which resonate with organizations are:

- Operating system vulnerabilities
- Network vulnerabilities
- Database vulnerabilities
- Access control/authentication problems
- User data vulnerabilities

How do organizations manage vulnerabilities (*see Figure 7*)? Three-fourths of the enterprises surveyed receive alerts through their vendors, while just over half use risk management software and/or conduct Internet searches to stay informed about vulnerabilities.

Figure 7: Sources of Vulnerability Awareness



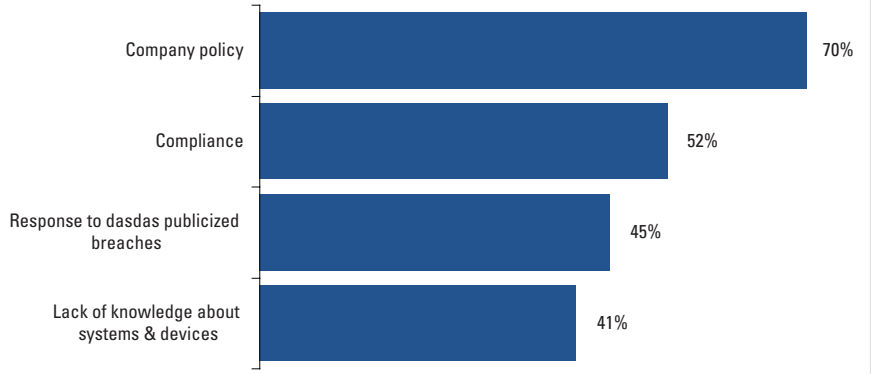
Source: Evalueserve Primary Research, 2009

> Seven out of 10 IT professionals cite corporate policy as a reason for vulnerability scanning.

Drivers of Vulnerability Scanning

Companies have standardized IT policy to remain informed about vulnerabilities; seven out of 10 IT professionals cite corporate policy as a reason for vulnerability scanning (*see Figure 8*). Three-fourths of users of risk management products cite company policy, while the number was significantly lower among non-users. Half the respondents said compliance is a driver. More than 40 percent cite response to publicized breaches and lack of knowledge about systems and devices as key drivers for vulnerability scanning.

Figure 8: Drivers of Vulnerability Scanning



Source: Evalueserve Primary Research, 2009

What's in Compliance? Knowing for Sure

Two-thirds of the responding companies are confident that they are aware of the systems that are non-compliant; almost as many, 62 percent, said they are similarly confident they know which systems are not vulnerable.

This is a prime area in which risk management products benefit organizations with their vulnerability management programs. Significant differences surface when we compared companies that use risk management products with those that do not: 71 percent of risk management product users are very confident of tracking non-compliant systems, as opposed to 47 percent of non-users. Similarly, two-thirds of risk management product users said they are able to identify systems which are not vulnerable, in contrast to just 39 percent of non-users of risk management products.

Preferred Vulnerability Scanning Options

One-third of the respondents said they require a combination of automated and hands-on approaches to vulnerability scanning, while 29 percent prefer a fully automated program.

The remaining are equally divided on their preference for strictly hands-on or fully automated reports to be provided through vulnerability scanning tools. A higher proportion of users of risk management products prefer a strictly hands-on approach, while a higher percentage of non-users prefer automated reports.

Automation extends to remediation for many organizations; 40 percent of the CIOs and their peers want vulnerabilities fixed automatically. Reflecting their expectation for the products they have purchased, a higher percentage of organizations that use risk management products expressed this need compared to non-users.

Vulnerability Reports: Users Set Expectations

A significant number of enterprises value post-vulnerability testing reports. About a third require list of vulnerabilities in order of severity. Also, about a quarter require post-fix assessment reports, for example, to validate that patches have been successfully applied or failed for some reason. Another 22 percent want to view a "scorecard" with details on vulnerability severity and status.

While most enterprises – two thirds of the respondents – expressed their satisfaction with the reports, they don't always get the level and type of details they feel their vendors should be providing. Among the reports they want to see:

- Details of the problem or error: Causes of the error, patch details, information about any unauthorized access.
- Details of risk involved: Severity, scale and type of risk; details of the potentially vulnerable assets, and additional details of the problem, such as its source. Detailed information would include:
  - Information on malware and attacks that can exploit the vulnerability.
  - Specific machines that require specific patches, breakdown by software titles and versions, etc.
  - Severity of the flaw and urgency to be repaired
- Remediation advice: Recommended options for addressing the vulnerabilities (patch, configuration change, IPS signature, firewall rule, etc.)
- Differential reports giving a detailed break up along with comparisons: Historical reference (when originally identified in wild and within our environment)

Organizations expect vulnerability scanners to conduct vulnerability management with a high degree of assurance as to what systems are in or out of compliance. They are looking for tools that give them that level of assurance, help them automate the process and deliver accurate and detailed reports that streamline and validate their activity.

Conclusion

Risk management programs are daunting in their scope and complexity. They are costly in time, money and man-hours—and still prone to error and misjudgment. Enterprises often invest enormous effort into assessing and managing risk without getting the results that reflect their level of commitment. Others are less diligent, conducting broad remedial security operations, such as patching, by rote, without a real notion of risk.

This survey reveals that there are enterprises that are on the right track; they understand that they can leverage risk management products to cut their task down to size. The findings clearly indicate a correlation between organizational maturity in terms of risk management and the effective use of supporting tools to sustain effective programs. These organizations are well-positioned and well-equipped to identify, prioritize and address the most pressing threats to their business while bringing cost and the draining commitment of time and manpower under control.

Conversely, the survey directs towards the conclusion that organizations which do not use risk management products tend, overall, to be less mature in their understanding and execution of programs to understand and mitigate risk.

Throughout the survey, companies that do not use risk management products repeatedly revealed they are less confident in their risk and vulnerability management programs and less likely to understand how these tools can help.

Consider that compared to companies that use risk management products, non-users:

- Are less inclined to recognize the importance of visibility into the risk posture of their IT infrastructure.
- Lack confidence about their protection against and awareness of IT security risks
- By a wide margin, are less confident about their ability to track non-compliant systems and identify those which are not vulnerable. Without this type of information, effective and efficient risk management is not possible.
- Are less likely to understand vulnerabilities in relation to critical assets. As a consequence, they are unable to prioritize remediation and focus on areas of greatest risk.
- Somewhat surprisingly, show far less interest in reducing patching frequency. This may reflect, in part, a failure to recognize how prioritization based on informed risk assessment, and automation can streamline patch management.

This is not simply a case of companies that are unwilling to invest in security technology, as organizations that use risk management products are at least as cost-conscious, and are, in fact, far more inclined to place heavy emphasis on a timely ROI for security purchases.

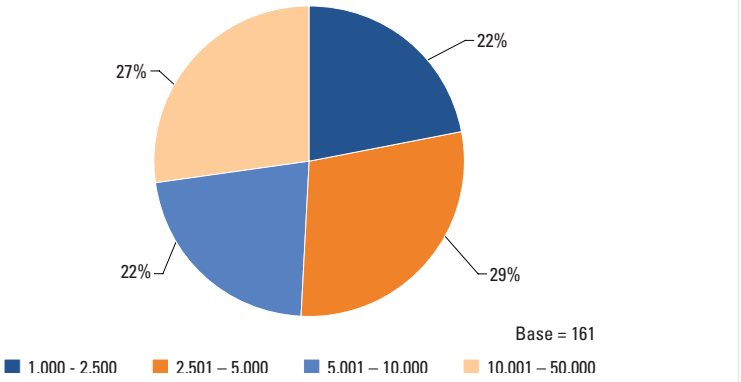
Risk and vulnerability management is not easy, and even best-in-class organizations have a tough row to hoe – after all, only 10 percent of all the companies surveyed feel they have high visibility into their risk posture.

But, it is clear that enterprises that implement policy-based procedures supported by risk management products are in the best position to sustain a continuous program of asset identification and classification, threat evaluation, risk assessment, monitoring and validation that will significantly improve the organization's security posture and enable compliance with regulatory mandates, as well as facilitate business productivity.

Research Approach

In November 2009, McAfee sponsored a survey with 273 IT decision makers, consultants and security analysts from large enterprises (1000+ employees) who are involved in evaluation, selection, day-to-day management and maintenance of security products.

Figure 9: Distribution of Companies by Number of Employees



Source: Evalueserve Primary Research

Of those surveyed, around half of the respondents are final decision makers for security software for their organizations. The remaining are either influenced decision making or managed the product.

The responses are gathered from different industries such as manufacturing, BFSI, software development, logistics, healthcare etc.

The survey was conducted across multiple regions and countries, including North America, the United Kingdom, Australia and Singapore.

The margin of error on a sample size of 273 is ± 5 percent with a confidence level of 90 percent-- i.e., at an overall level the findings have a 90 percent chance of lying between ± 5 percent. Interpretations by user/non-user of risk management products are at best directional. Percents on questions where respondents could select only one answer may not sum to 100 due to rounding. Not every respondent answered every question.

The sample size for some questions is lower as opposed to 273. This is because not all respondents qualified for answering these questions based on their response to previous question(s).

EVALUESERVE
Your Global Knowledge Partner

About Evalueserve

Evalueserve provides knowledge services to a global client base of Fortune 5000 companies, including Investment, Commercial and Retail Banks; Insurance Companies; Private Equity Firms; Corporates; Consulting and Research Firms; Law Firms and Intellectual Property Firms. Evalueserve's expertise covers areas such as Financial and Investment Research, Business Research, Market Research, Intellectual Property, Data Analytics and Knowledge Technology Services. Besides, we provide access to over 25,000 experts through our Circle of Experts.

We currently have more than 2,000 professionals in our research centers in India (Delhi-Gurgaon), China (Shanghai), Chile (Santiago-Valparaiso) and Romania (Cluj-Napoca). In addition, we have 60 client engagement managers located in all major business centers and regions around the world. We have sales offices in the Americas, Europe, Asia-Pacific and the Middle East.

For more details, please visit: www.evalueserve.com or write to ITResearch@evalueserve.com