



Vulnerability Management Survey

Executive Summary

November 1st, 2006

Conducted by Trusted Strategies
for
Shavlik Technologies LLC

Author: Bill Bosen



About Trusted Strategies LLC

Trusted Strategies is a research and advisory firm focused exclusively on IT security. We are information security market experts regarding industry trends, technologies, products, and vendors.

Our clients are product vendors who we help with market validation, positioning, competitive analysis, go-to-market strategies, business development, and the creation of marketing and sales tools for their IT security related products. We also assist companies who are buying, selling, or otherwise acquiring IT security technology or firms.

With over 20 years of experience in the field, and as successful IT security entrepreneurs ourselves, Trusted Strategies understands the information security industry and how to provide just what our clients need.

For additional information please contact:

Trusted Strategies, Inc.
239 Main Street Suite E
Pleasanton, CA 94566
925 461-1002

www.trustedstrategies.com

Vulnerability Management Survey

Executive Summary

While most organizations view integrated and automated vulnerability management as critical to their operations, fewer than 25% have it fully deployed, and growing numbers of mobile laptops are difficult to keep in compliance with company security policies and pose the greatest risk.

Survey Objective

Trusted Strategies, a research and advisory firm focused exclusively on information security recently conducted a survey regarding vulnerability management. This document presents an executive summary of the survey findings.

Vulnerability management, as used in this study, is the process of systematically locating and identifying security and other vulnerabilities within operating systems and applications, and applying patches, re-configuring machines, and removing unapproved software to mitigate these risks.

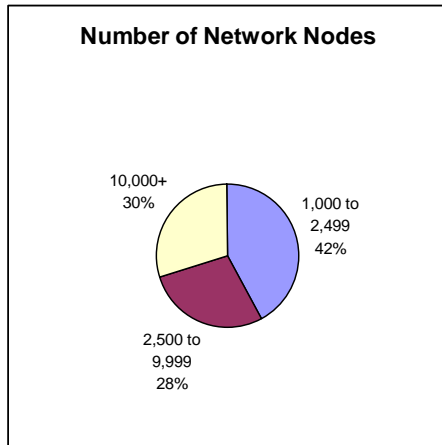
The goal of this survey was to determine how IT management and staff within mid to large sized organizations view the importance and success of their vulnerability management systems and its integration with related products and technologies.

Participants were asked 34 questions such as how effective their vulnerability management system is, how fast their systems are remediated, and their biggest areas of concern. Survey participants were also asked how integrated vulnerability management should be with other systems such as network access control (NAC) and regulatory compliance.

The survey also asked participants how much of the vulnerability management lifecycle they expected Microsoft Vista to solve.

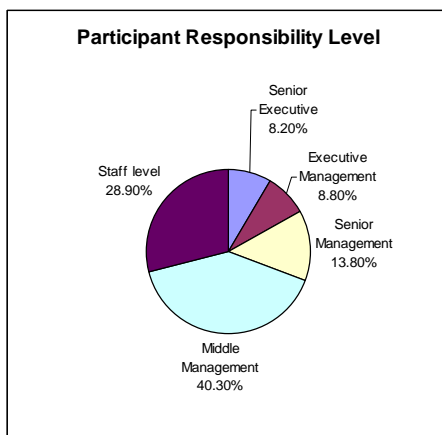
Survey Methodology & Participants

The methodology used for the study entailed surveying and screening 800 participants from mid to large sized organizations within the United States. Individuals selected to participate in the survey all belonged to organizations with at least 1,000 network nodes and either managed or were directly involved in the maintenance of their organization's computer networks, servers, desktops, and laptops. All participants were members of their organization's IT department.



Thirty percent (30%) of participants belonged to organizations with 10,000 or more network nodes (servers, PCs, laptops). Twenty eight percent (28%) were with organizations having between 2,500 and 9,999 network nodes, and the remaining participants had between 1,000 and 2,499 network nodes in their organizations.

The organizations involved belonged to a wide range of industries and government organizations including manufacturing, high tech, health care, banking and finance, education, communications, transportation, public utilities, and others.



Over thirty percent (30%) of the participants were in upper management with just over eight percent (8.20%) of those being senior executives and nearly nine percent (8.80%) in executive management roles while around fourteen percent (13.80%) were senior managers. Forty percent (40.30%) of the participants were mid-level managers, and twenty nine percent (28.90%) were staff level employees.

Key findings

The survey results provide a number of significant and enlightening conclusions.

- Most organizations view automated patch management as a critical and integral part of their operations, however less than a quarter have it fully in place.
- Overall, only 16.4% of survey respondents believe Microsoft Vista will address *most* of the patch and vulnerability lifecycle management issues.
- Most organizations reported that mobile laptops posed the greatest security threats and are the most difficult to maintain.
- In 27% of the cases, it was reported that it took longer than 10 days to deploy critical patches to mobile laptops.

Most organizations viewed patch management as critical to their operations

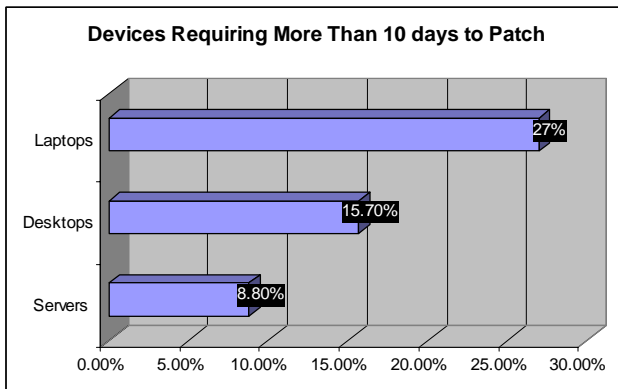
It was clear from the survey results that effective patch management is viewed as being critical to most organization's overall IT and security posture. The level of automation is also key. Over ninety percent (90.60%) of survey respondents felt that it was "important" or "very important" for vulnerability management to be fully automated. However less than a fourth, (23.3%), of the organizations reported that they actually were fully automated. Thirty one percent (31.40%) had either no vulnerability management automation whatsoever or had only some portions automated.

Most respondents also felt that integration of vulnerability management with other systems such as network access control (NAC) and compliance management auditing and reporting was very important. Eighty percent (80%) of the participants reported that it was "important" or "very important" for vulnerability management to be fully integrated with both NAC and regulatory compliance systems. Forty-six percent (45.90%) indicated "very important".

Mobile laptops are the biggest concern and the most difficult to keep secure

The numbers and percentages of mobile laptops are quickly expanding. Over forty-one percent (41.5%) of survey participants had more than a thousand mobile laptops within their organization and almost eleven percent (10.70%) had more than five thousand mobile laptops. With the significant and growing number of laptops now within organizations, survey participants expressed ample concern about their security.

When asked which of laptops, servers, or desktops posed the greatest threat to maintaining their security posture, over sixty percent (60.4%) said mobile laptops posed the greatest threats. Only eighteen percent (18.2%) felt desktops were the largest threat and twenty one percent (21.4%) felt servers were the greatest issue.



It also took the longest to deploy security updates and patches to mobile laptops. In only 8.80% of the cases did it take longer than 10 days to deploy critical patches to servers. Laptops however, took significantly longer. In 27% of the cases, it was reported that it took longer than 10 days to deploy critical patches to laptops.

How fast are critical vulnerabilities patched?

We asked survey participants how fast critical patches were deployed to their production servers, desktops, and mobile laptops.

- Critical vulnerabilities on production servers were patched within 10 days in 91% of the cases, and in 49% of the time, within 2 days.
- Critical vulnerabilities on desktops were patched within 10 days in 84% of the cases and within 2 days in 35% of the cases.
- Critical vulnerabilities on mobile laptops were patched within 10 days in 73% of the cases and within 2 days in 24.5% of the cases. However in 27% of the cases it took longer than 10 days.

Leadership and staff generally agree – except on level of automation and Vista

Throughout the survey, answers among varying levels of leadership and responsibility levels were strikingly similar. Executive and mid-level IT management as well as their staff were in remarkable agreement on most issues. One exception was in regards to Microsoft Vista. When asked how much of the patch and vulnerability lifecycle management task Microsoft Vista would effectively handle, senior executives were much more optimistic than midlevel management and staff. Thirty percent (30.6%) of senior executive management believed that Vista would solve *all* of the related problems whereas only 6.2% and 6.5% of mid-level management and staff members respectively said Vista would address all of the patch and vulnerability lifecycle issues. Overall, only 16.4% of the respondents felt Microsoft Vista would address *most* of the patch and vulnerability management issues.

One other interesting difference among the way participants with different levels of responsibility responded is worth noting. When asked how much of the patch / vulnerability lifecycle has been automated within their organization, nearly forty five percent (44.9%) of senior executive management believed that *all of the functions were automated* whereas only 11% (10.9%) of the IT staff members felt that all functions were automated. Since the actual IT staff members are much more likely to have an accurate and full understanding of this issue, it appears that senior management tends to have somewhat of a false sense of security in this area.

Summary Conclusions

Vulnerability life cycle management is an integral and crucial part of an organization's IT operations, and securing laptops is the biggest challenge. While most organizations have some level of automation, nearly all agree that full automation and integration with other related systems is critical yet fewer than a quarter of them have it in place. Some may have been holding out to see what Microsoft Vista would address, but now that it's imminent very few believe it will do the trick.