

Lucent Technologies
Bell Labs Innovations

Network Security

HIGHLIGHTS

- Only 37 percent of respondents currently have a comprehensive network security program implemented.
- For 40 percent of respondents, the top concern about a network security breach comes from either inadequately trained or unconcerned users, or from insufficient or poorly implemented security processes.
- External sources of security attacks keep IT professionals up at night. For 77 percent of respondents, external attacks are most frequent, and for 67 percent they are the most damaging.
- Despite greater security demands, satisfaction with security capabilities has risen significantly since 1998, while satisfaction with security products has also risen, although by only a minimal amount. The high cost of products is a significant barrier to improving network security capabilities for half of respondents, up by 8 percent over the last year.
- Half of respondents cite the difficulty of determining network security requirements as a significant barrier to improving their capabilities. This issue is exacerbated by the lack of experienced staff, a problem for 48 percent of respondents.
- Forty-two percent of respondents would consider using a managed network security service, and 17 percent already employ this strategy. The leading reason for doing so is to obtain more security functionality and capabilities.

CONTENTS

1 Highlights
2 About Lucent Technologies Worldwide Services
3 Introduction
3 The Bottom Line
4 Sources of Security Concerns
7 Importance of and Satisfaction with Security Capabilities/Products
10 Elements of a Comprehensive Network Security Program
14 Tapping External Providers of Security Services
17 Respondent Demographics
18 Respondent Comments
19 About Lucent Worldwide Services Network Industry Surveys
20 Methodology

About Lucent Technologies Worldwide Services

Lucent Technologies Worldwide Services offers service providers and enterprises a comprehensive portfolio of network consulting and software solutions for the full lifecycle of a network, including planning and design, implementation, and operations. Lucent Services provides professional services, technical support services, mobility solution services, engineering and installation services, and software solutions for network and application performance management, comprising VitalSuite', VitalQIP', and VitalAccess'. Lucent Technologies is headquartered in Murray Hill, New Jersey, USA. Visit the Lucent Services Web site at **http://www.lucent.com/businessunit/worldwide.html**

For information regarding Lucent network consulting and software solutions capabilities, call 1-888-767-2988 in the U.S., or 1-650-318-1020 outside the U.S., or email: networkcare@lucent.com.

For more information regarding this survey, please contact:

Rick Blum
Senior Research Programs Manager
(781) 848-5500, Ext. 320
Email: rickblum@lucent.com

Introduction

Network security is in the headlines... all too frequently. For IT managers, the imperative for improving the security of their networks has never been higher. But with the ubiquity of email and ecommerce, maintaining access to information for a wide number of remote users in a secure environment has never been more challenging.

From April 30 through May 31, 2001, Lucent Technologies Worldwide Services conducted a Web-based survey on network security, which was completed by 156 people around the globe. Previous surveys on network security were conducted in May 2000 and July-August 1998.

Together, these survey results yield valuable insights into the past, current, and future network security strategies of today's service providers and enterprises. Moreover, these results identify the significant barriers and challenges network professionals face as they plan, design, and implement network security strategies for their organizations. These results should enable networking organizations to better understand how their operations compare with others in the industry and identify possible areas for improvement. Complete results for all three surveys are available at www.lucent.com/knowledge/resourcelib

For the purposes of this survey, network security was defined as the set of activities required to protect and secure information from harmful and/or unwanted intrusion of internal or external sources.

The Bottom Line

There's no escaping the need to increase network security. The demand for instant communications across far-flung enterprises is accelerating, as is the desire to access growing volumes of information stored in massive centralized databases. Considering the continual discovery of security holes in many of the software products that enable this communication and remote access, strong network security is even more critical.

For network managers and security professionals, the spotlight on security is an opportunity to elicit the support they need to upgrade and strengthen their security systems. As they proceed along this path, they need to focus on the most critical areas of concern.

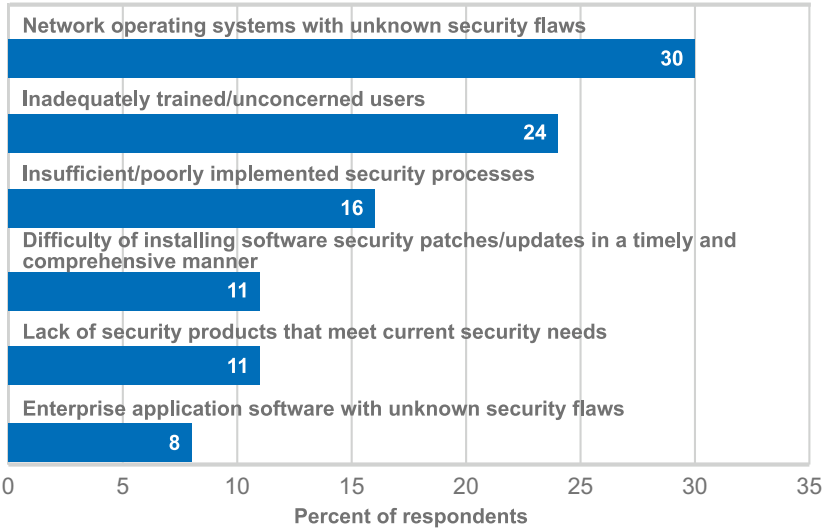
- Workstation email is the most frequent source of parasitic attacks from external sources, and also the most costly. Ensure that network perimeter firewalls are properly situated and configured to intercept these attacks before they can infiltrate email systems.
- Not every attack can be detected and repelled by technology alone. Spend equal time developing processes and procedures to minimize proliferation and resulting damage from new, insidious parasitic attacks. Make sure that end-users are aware of the damage potential and their responsibilities to both detect breaches of network security and deter further spread of its damage.
- Don't become too satisfied. Even with a comprehensive security plan implemented, unanticipated dangers lurk. Constantly test and audit current security programs using security specialists who are most familiar with the latest dangers and defenses.

Sources of Security Concerns

Security is a difficult goal simply because potential breaches of systems and networks can occur in many places and can come from many sources. Security flaws in today's operating systems can't be anticipated, and for 30 percent of survey respondents, unknown sources causes them the most concern for a potential breach of their network's security.

For 40 percent of respondents, the source of a breach is most likely not technology related. Rather, it is likely that their security processes are either insufficient or poorly implemented, or that their users are either inadequately trained on the processes or unconcerned about them. It is evident that a total security plan must include not just technological solutions, but also take into account the people and processes to support that technology.

Top Network Security Issue Concerns



N=157

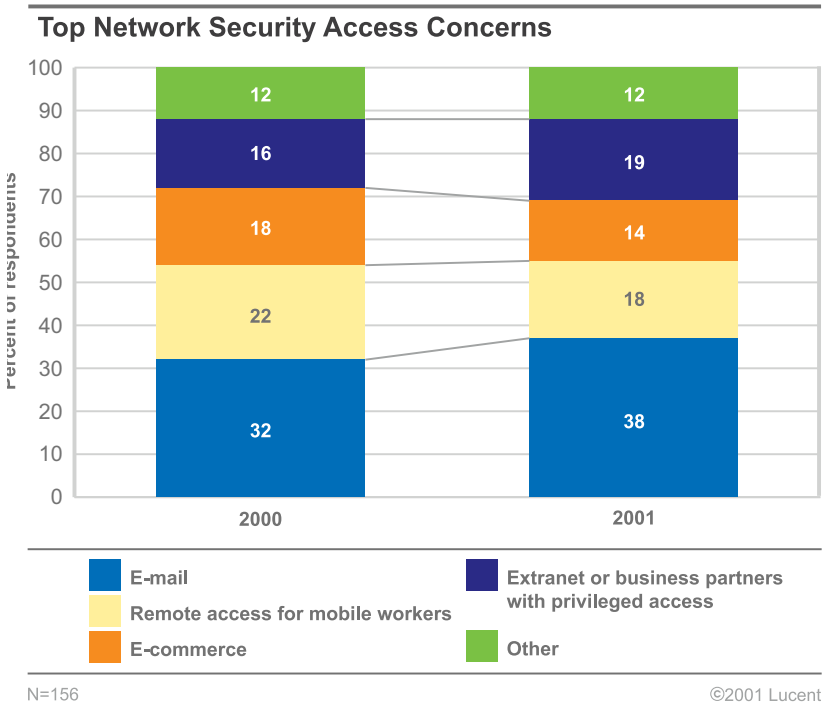
©2001 Lucent

Email is ubiquitous in the corporate world; it is also the source of a potential security breach that causes the most concern for 38 percent of respondents, a 6 percent increase from last year's survey.

Remote access for mobile workers, ecommerce, and extranets (or business partners with privileged access) are other common sources of potential security breaches. Each generates the highest concern for between 14 percent and 19 percent of respondents. However, the larger the network, the more the concern shifts to remote access and extranets. For respondents whose annual data networking budgets exceed $25 million, 33 percent identify extranets as their top concern and 24 percent identify remote access.

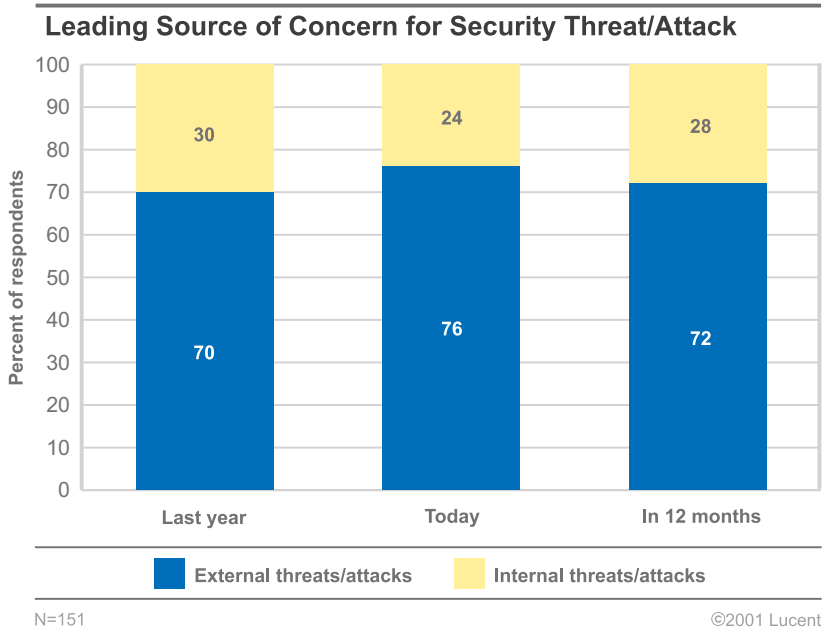
Other sources that can create high concern about network security breaches include floppy disks brought in from home by end users and links to the IS department.

Breaches of network security to access sensitive information or damage the network can come from internal (employees) or external sources. For the last two years, and for the year to come, external sources are the top concern of the large majority (70-76 percent) of survey respondents.



N=156

©2001 Lucent



N=151

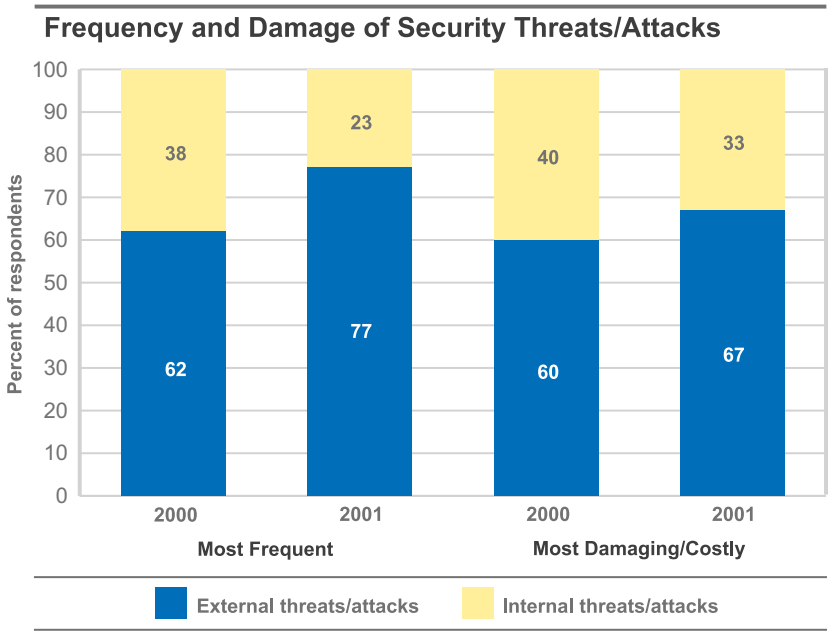
©2001 Lucent

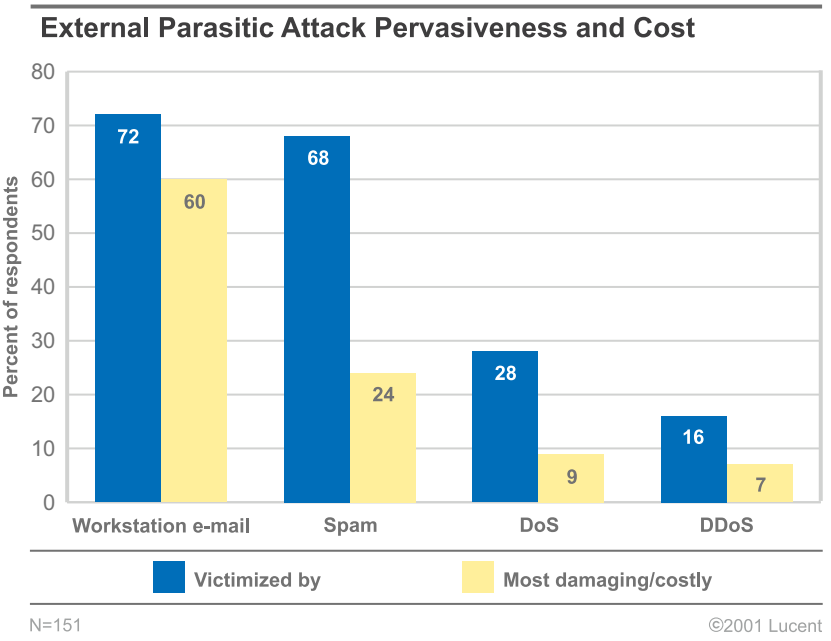
In last year's survey, 13 percent of respondents had expected to shift their concern from external to internal threats, but that has not occurred, perhaps a reflection of the fact that external sources of security threats and/or attacks has increased in the last year. External sources are now the leading source of threats and/or attacks on information systems for 77 percent of respondents, up from 62 percent in 2000. Similarly, external sources of security threats and/or attacks are even more likely to be the most damaging or costly this year, cited by 67 percent of respondents compared to 60 percent in 2001.

Focusing on external threats and attacks, nearly three-quarters (72 percent) of respondents have been victimized by workstation email parasitic attacks in the last year. Not far behind, 68 percent of respondents have been spammed in the last year. Both of these results are similar to what was reported in the 2000 survey.

Denial of service (DoS) and distributed denial of service (DDoS) attacks have also been experienced by a sizable percentage of respondents (28 percent and 16 percent, respectively), though far less often than workstation email attacks and spam. These results are also similar to last year's survey.

Workstation email attacks, although experienced by slightly more respondents than spam, is clearly more damaging and costly. Sixty percent of respondents identify workstation email attacks as the most damaging or costly security breach, as opposed to only 24 percent who finger spam. While spam can be annoying, workstation email parasitic attacks wreak the most havoc.

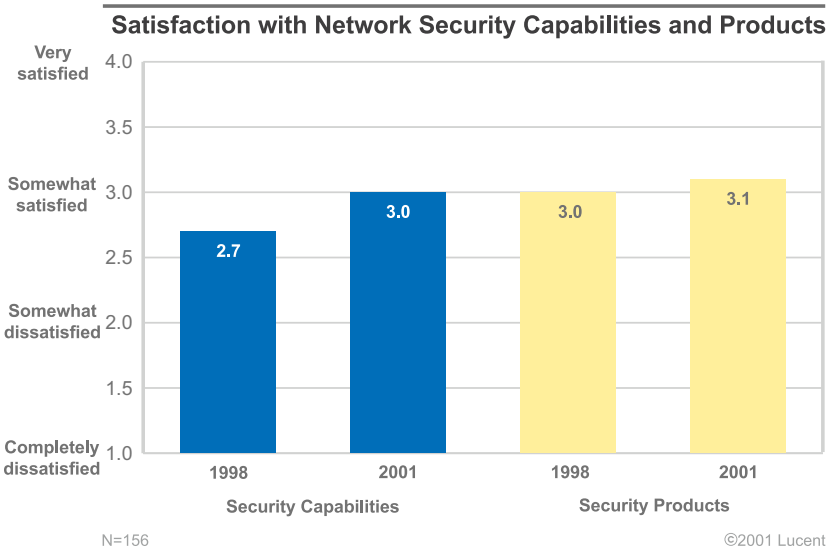


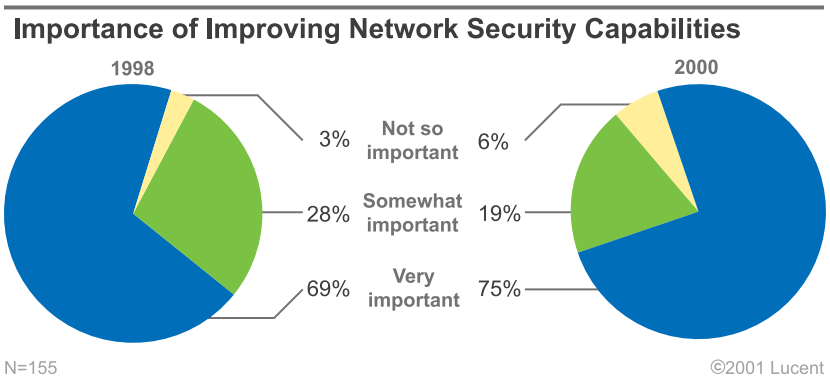


Importance of and Satisfaction with Security Capabilities/ Products

While respondents continue to struggle against attacks on their security systems from within and without the network, the trend is clearly toward higher satisfaction with security capabilities. In the 1998 network security survey, 62 percent of respondents were very or somewhat satisfied with their organizations' security capabilities (a rating of 2.7). In the 2000 survey, that percentage had climbed to 72 percent (a rating of 2.8). In this year's survey, 79 percent of respondents are satisfied, for a rating of 3.0 percent. This, of course, is very good news and indicates that the efforts of security professionals to deal with the many different types and sources of network attacks have been more successful.

Security professionals rely in good measure on security tools to help them in their battle, although tools are only part of the equation. Most respondents (82 percent) are at least somewhat satisfied with the products available to help them improve their network security, although only 28 percent would describe themselves as very satisfied. Still, this is a marked improvement from last year, when only 19 percent described themselves as very satisfied.





At the same time that network security satisfaction levels have been going up, the importance of improving these capabilities also has been going up. In 1998, 69 percent of respondents felt that it was very important to improve their network security capabilities. Rather than declining, that figure rose even higher – to 75 percent – this year.

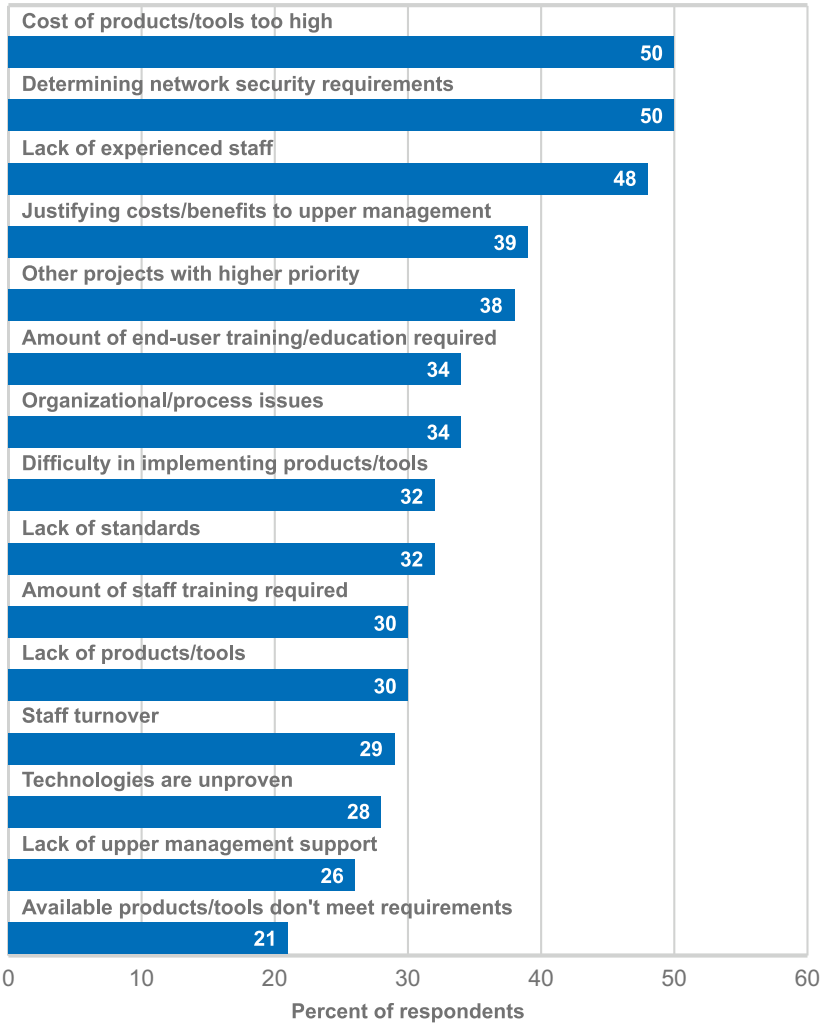
The increases in both satisfaction levels and the desire to keep improving indicates that security has grown in visibility, not only within IT organizations but across entire companies. This holds especially true for large companies (annual data network budget of $25 million or more), where 86% of respondents consider improving their security capabilities as very important.

There are a number of barriers, however, that stand in the way of improving security capabilities. The typical respondent identified 5 from a list of 14 possible barriers. Three, in particular, stand out as common across many organizations: the high cost of products/tools, determining network security requirements, and the lack of experienced staff.

The high cost of security products and tools, of course, is beyond the control of network security professionals. Unfortunately, it is a situation that has gotten worse over the last year. In the current economic conditions, where many companies are tightening their fiscal belts, this situation is not likely to improve in the foreseeable future.

Two related concerns – the difficulty in implementing products and tools, and the fact that many technologies are unproven – are barriers for significantly fewer respondents. That is the good news. The bad news is that both of these, like the high cost of products and tools, are affecting more respondents this year than last.

Significant Barriers to Improving Network Security Capabilities

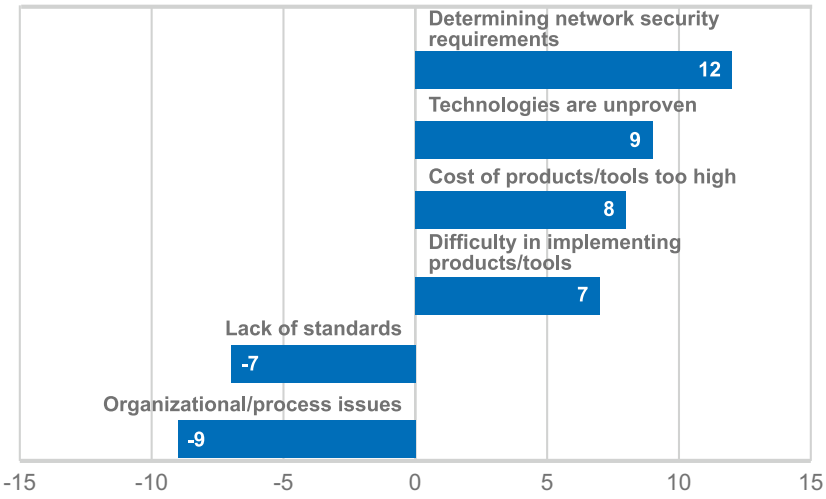


N=151

©2001 Lucent

Although the current industry slowdown has eased the hiring crunch somewhat, the supply of highly skilled network security professionals has not gotten better, and for nearly half of respondents, it is a significant barrier to improving their security capabilities. As a result, many organizations have used outside consultants to obtain the requisite expertise, or even out-tasked their security to a managed security services firm.

Change in Significant Barriers, 2000 to 2001



©2001 Lucent

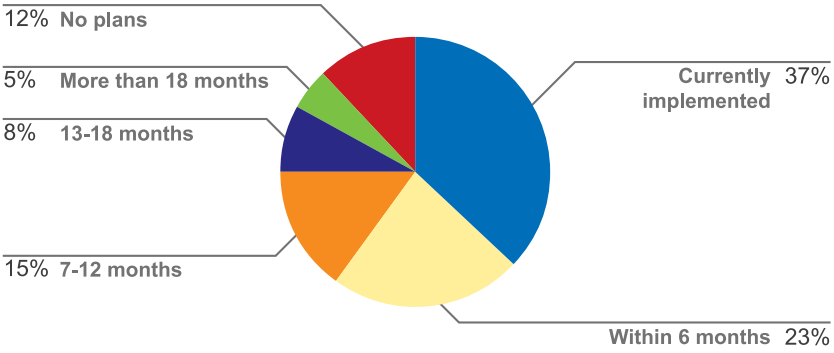
The on-staff skill shortage relates directly to the third leading barrier, which is trying to determine network security requirements. This problem has become more widespread in the last year. Without staff skilled in security issues – both technological and organizational – network managers are hard-pressed to understand exactly what security requirements they should be working toward. And without this understanding, they can't adequately scope their security needs in terms of systems, staffing, tools, etc. Again, many are turning to outsourcing and out-tasking to overcome this hurdle.

The few bright spots in the picture are that two barriers have shown significant improvement over the past year: the lack of standards and organizational/process issues. Still, both affect more than 30 percent of respondents, so they are far from disappearing from the radar screen.

Elements of a Comprehensive Network Security Program

Thirty-seven percent of respondents report that they already have a comprehensive network security program implemented. Another 23 percent of respondents plan to have a comprehensive program implemented within 6 months, and an additional 15 percent within a year. Whether those plans will be fulfilled is questionable, since the results in last year's survey were similar, indicating that not much progress has been made in the past year. Perhaps the urgency for increased network security will help make these plans a reality in the coming year.

Timeframe for Implementing a Comprehensive Network Security Program



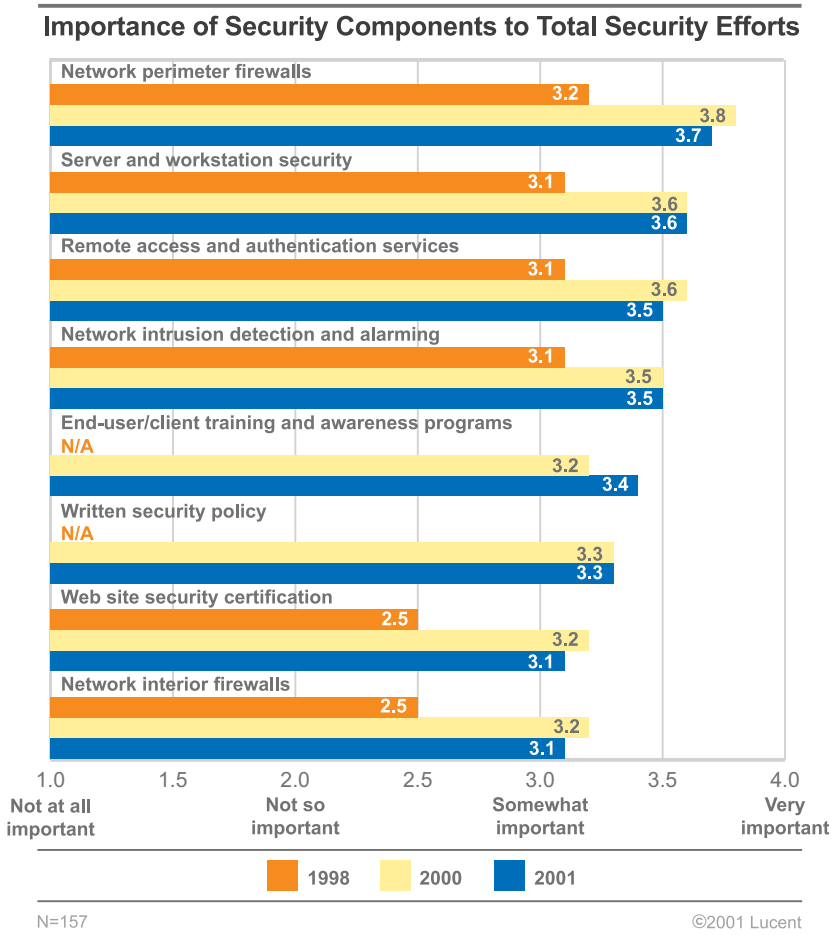
N=157

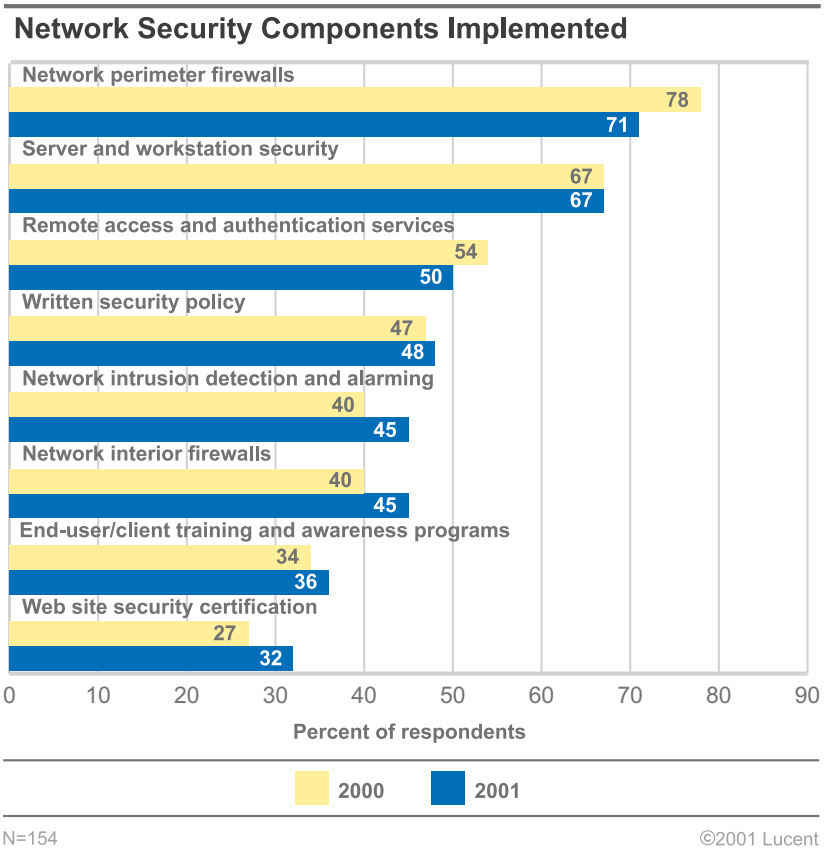
©2001 Lucent

We've already highlighted the significant increase in importance that respondents place on improving their network security capabilities. Likewise, we see an across-the-board increased importance placed on specific components of security efforts.

According to respondents, the most important security component is network perimeter firewalls, a prime deterrent to external attacks. Nearly as important are server and workstation security, followed by remote access and authentication services, and network intrusion detection and alarming.

While all of these components are rated slightly less than or equally as important as last year, end-user/client training and awareness is rated much higher. Last year only 44 percent of respondents rated this component as very important; this year that figure jumped to 55 percent of respondents. Clearly, the people and processes side of the security equation is gaining visibility as a key element of a total security program.





Unfortunately, the increased recognition of the importance of end-user/client training and awareness programs did not translate to significantly higher implementations – only 36 percent of respondents have already implemented programs this year as compared to 34 percent in 2000. However, nearly all respondents plan to address this shortfall in the coming year.

As would be expected, network perimeter firewalls are most often implemented today, up to 78 percent of respondents who have firewalls this year as compared to only 71 percent in 2000. Server and workstation security is unchanged from last year, implemented by two-thirds of respondents.

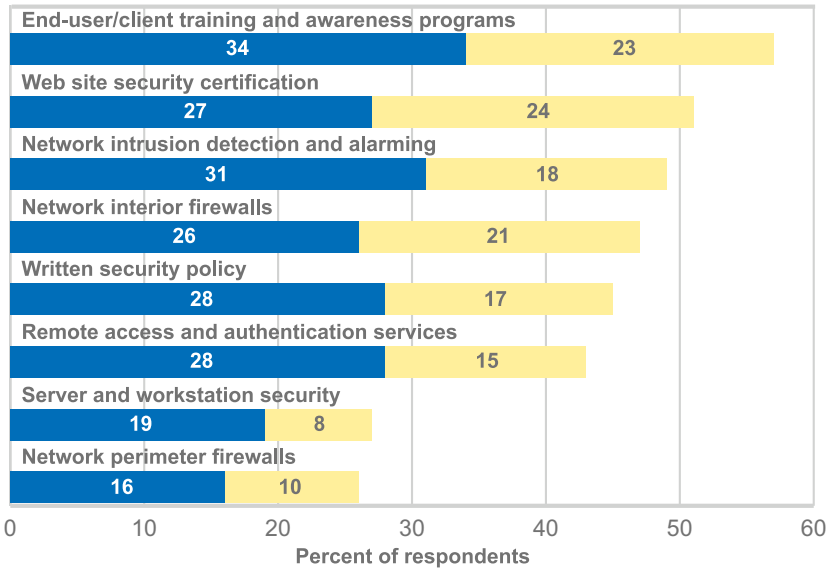
Written security policies are found in nearly half of respondents' security programs, although their effectiveness is highly dependent on end-user awareness; the survey indicates that two-thirds of IT shops lack awareness programs.

In the coming six months and year, most respondents plan to fill the gaps in their network security programs, ranging from Web site security certification to network interior firewalls. It is an ambitious goal and, if even half their intentions are met, will greatly improve network security.

With much of the efforts in the coming year being expended on end-user/client training and awareness programs, it is no wonder that nearly half of respondents identify their biggest challenge in resolving network security issues as people-related, and another 32 percent cite process issues as their biggest challenge. A scant 19 percent of respondents feel that technology is their biggest challenge.

In the coming six months and year, most respondents plan to fill the gaps in their network security programs...

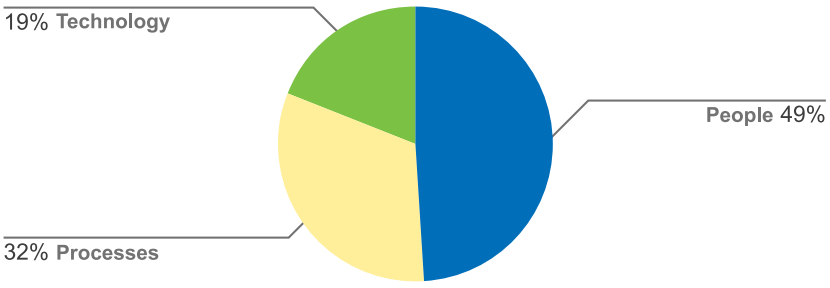
Network Security Components Implementation Plans



N=154

©2001 Lucent

Area That is Biggest Challenge to Resolving Network Security Issues



N=155

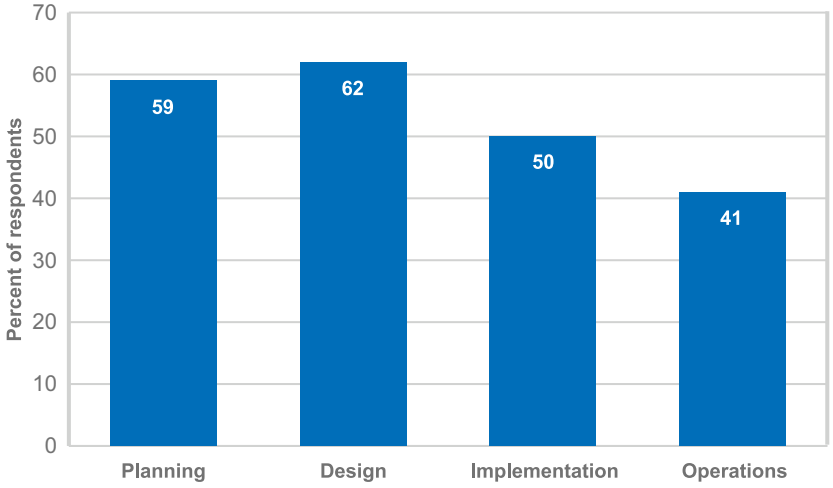
©2001 Lucent

Tapping External Providers of Security Services

The typical survey respondent needs help in implementing or enhancing their network security capabilities in two of the four network lifecycle phases, that is, planning (including technology decisions), design (including vendor selection), implementation, and operations. The first two phases – planning and design – are most often cited as areas where respondents need help, but both the implementation and operations phases also are areas where in-house capabilities often fall short.

Network managers can meet this need in several ways, including hiring a firm that provides security services or using a managed network security service to simply offload much of their security requirements. More than 40 percent of respondents would at least consider this second option, while 17 percent have already implemented this solution. Despite the fact that security is becoming more complex and urgent, the percentage of network managers who would consider a managed security service has not changed significantly since 1998.

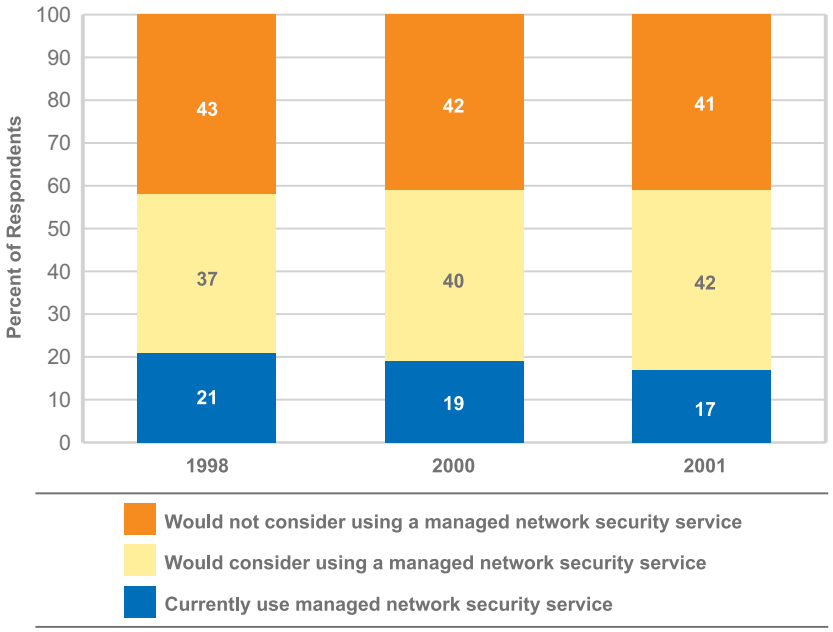
Network Lifecycle Areas in which Help is Needed to Implement or Enhance Network Security Capabilities



N=123

©2001 Lucent

Use/Consideration of Managed Network Security Services



N=155

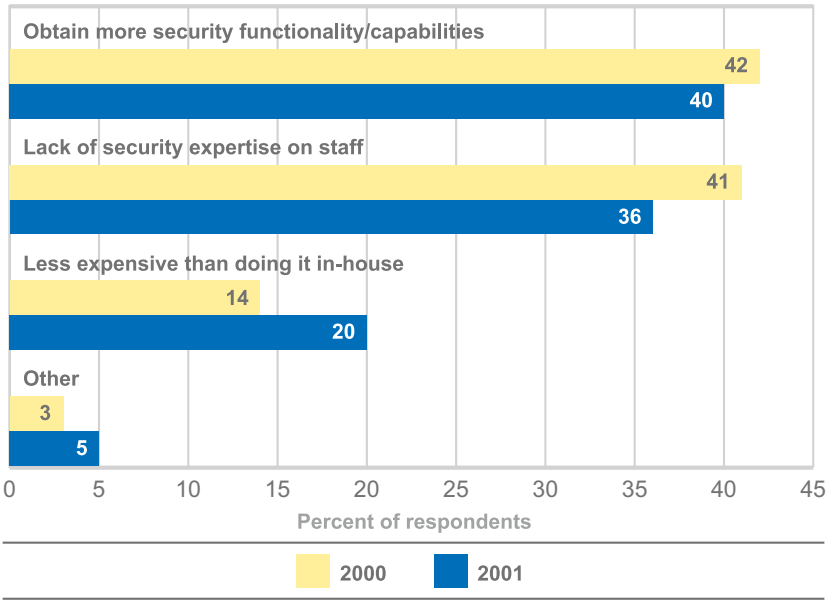
©2001 Lucent

For the 59 percent of respondents who are either using or willing to consider a managed network security service, the primary reason for doing so is most often to obtain more security functionality or capabilities (40 percent of respondents), followed by the lack of security expertise on staff (36 percent of respondents). The last year has brought a small but decided increase in the percentage of respondents who look to a managed security service as a cost saver. Given the high cost of salaries for network professionals with security skills and increasingly complex security requirements, this could well signal the start of a trend.

The 41 percent of respondents who would not consider using a managed network security service most frequently cite the lack of trust in these providers as the primary reason. A surprising 23 percent of respondents don't believe that their security needs are high enough to warrant using an outside service. Not surprisingly, all but a handful of these respondents are in organizations whose annual data networking budgets are less than $10 million.

...23 percent of respondents don't believe that their security needs are high enough to warrant using a (managed security) service.

Primary Reason for Using an External Service Provider for Network Security

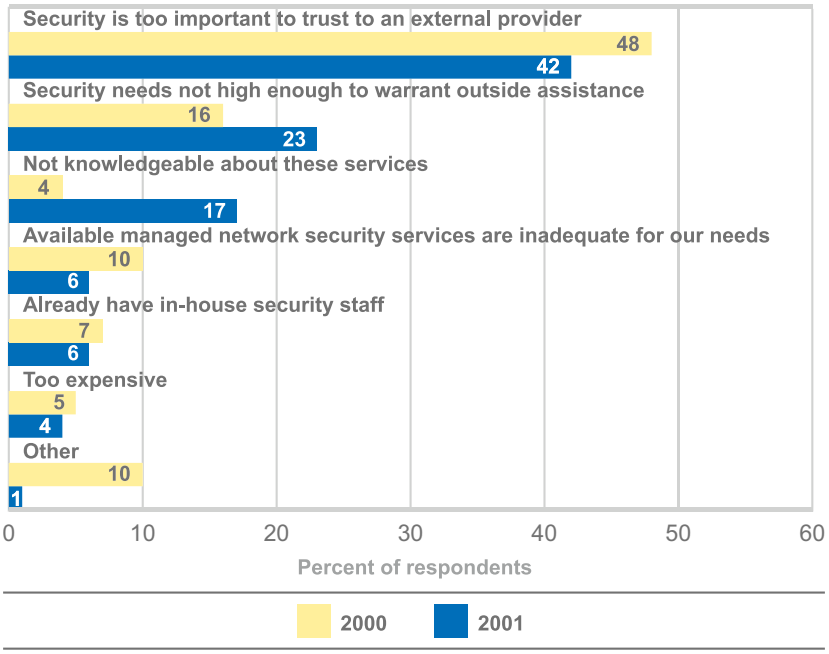


Note: Includes only respondents currently using or willing to consider a managed network security service.

N=90

©2001 Lucent

Primary Factor in Not Being Willing to Consider a Managed Network Security Service

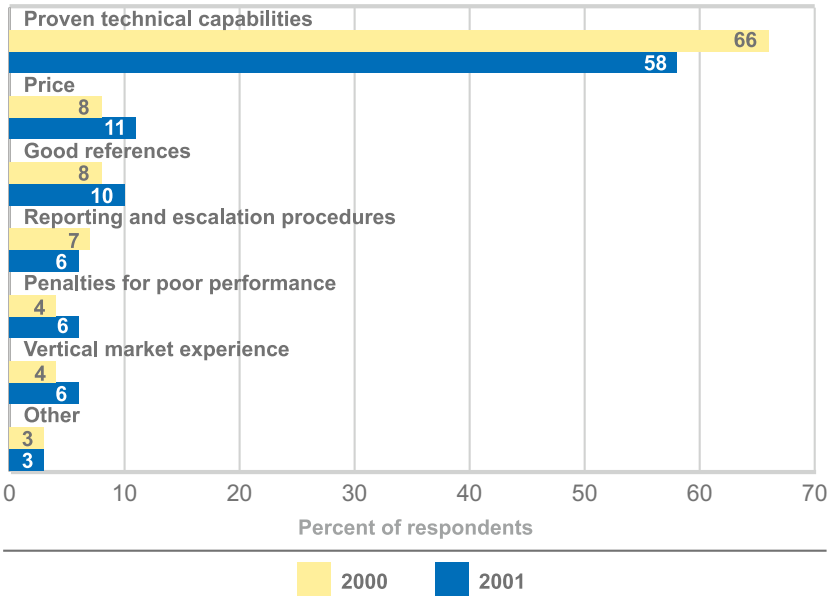


Note: Includes only respondents not willing to consider a managed network security service.

N=64

©2001 Lucent

Most Important Factor in Choosing a Managed Network Security Provider

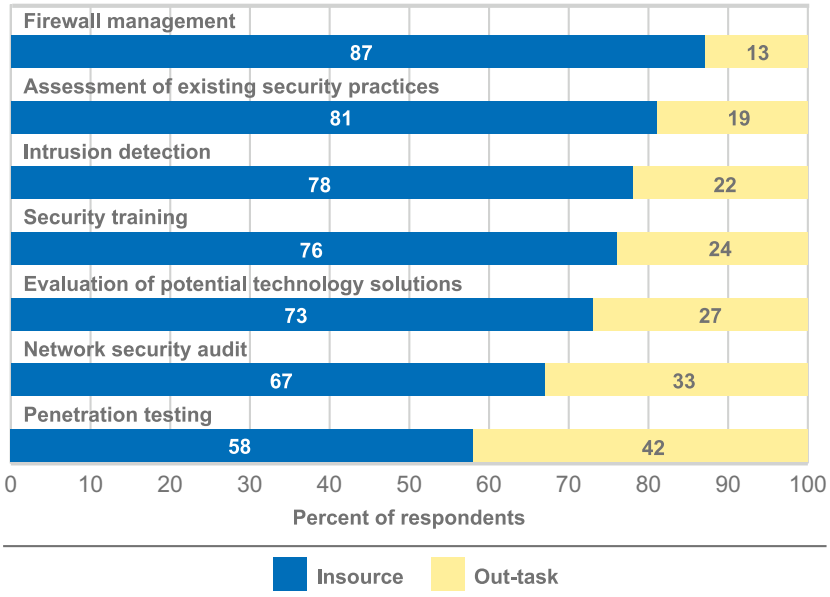


Note: Includes only respondents currently using or willing to consider a managed network security service.

N=89

©2001 Lucent

Preference for Insourcing vs. Out-Tasking Network Security Activities



N=155

©2001 Lucent

For respondents who are either using or willing to consider a managed network security service, the majority (58%) cite proven technical capabilities as the most important factor in making their vendor selection. Other factors, such as price and references, are cited as the primary factor by only a small percentage of respondents.

An alternative to outsourcing network security to a managed service provider is to out-task specific tasks rather than do the entire program in-house. Penetration testing is most often seen as a task better performed by an external provider. The advantage, of course, is that using an external provider can protect against bias, conscious or unconscious. For similar reasons, one-third of respondents say an out-tasking strategy makes sense for network security audits.

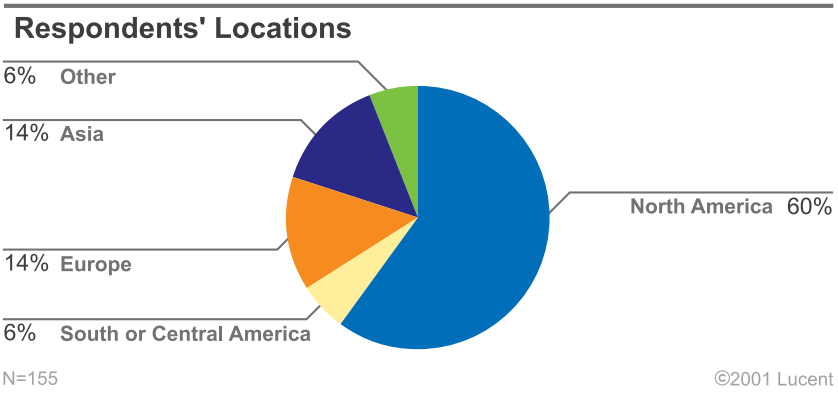
Least likely to be out-tasked are firewall management and assessing existing security practices.

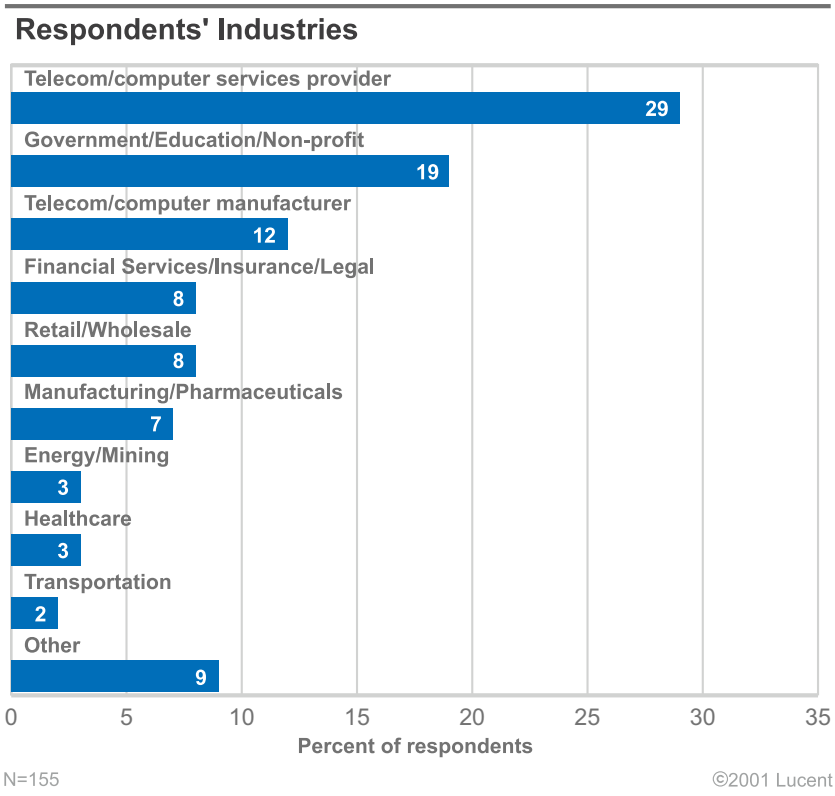
Penetration testing is most often seen as a task better performed by an external provider.

Respondent Demographics

Sixty percent of respondents are located in North America, while Asia (14 percent), Europe (14 percent), and South or Central America (6 percent) account for most of the remaining respondents. The "Other" category includes outposts such as Australia and Azerbaijan.

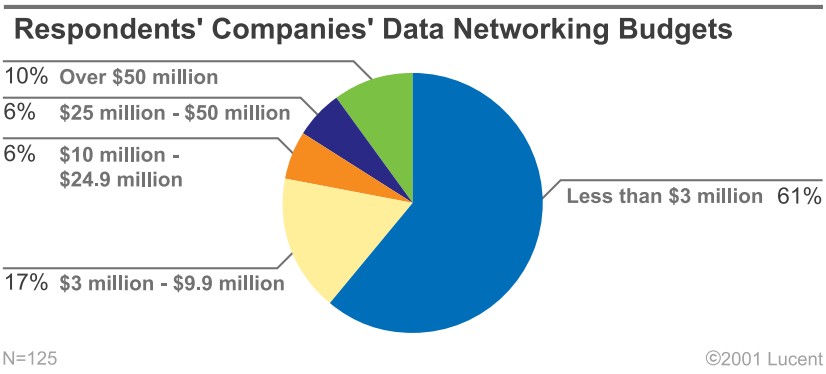
Survey respondents represent a fairly broad cross-section of industries, led strongly by telecommunications/computer services providers, which represent 29 percent of respondents. Other well-represented industries include government/education/nonprofit organizations (19 percent), telecommunications/computer hardware and software manufacturers (12 percent), financial services/insurance/legal firms (8 percent), and retailers/wholesalers (8 percent).

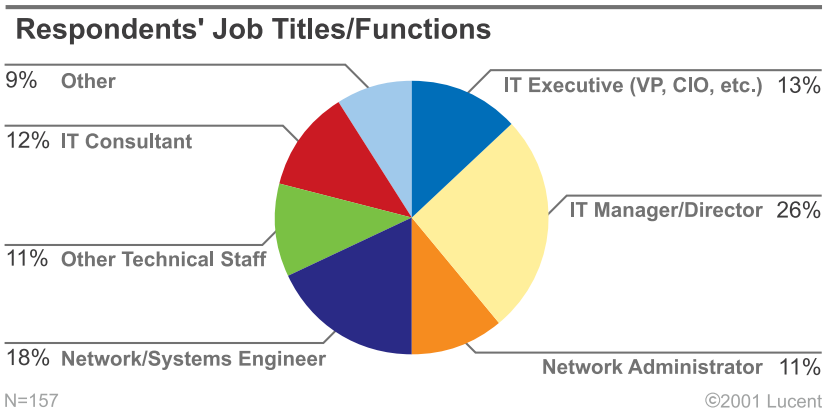




At the high end, 10 percent of respondents' companies budget in excess of $50 million annually for data networking. The majority of respondents' companies work with budgets of under $3 million.

The highest percentage job title/function category is IT manager/director (26 percent), followed by network/systems engineer (18 percent), and IT executive (13 percent).





Respondents Comments

- Budget constraints and the inability to hire or retain competent personnel are the biggest problems for us.
- In Latin America, the most important problem is people. The application of technology is relatively easy. The most important thing is to make the users conscious (of security) in the network.
- It is difficult to find the right balance between closing everything for maximum security and opening everything for the maximum resources availability.

About Lucent Worldwide Services Network Industry Surveys

Lucent Worldwide Services conducts monthly industry survey projects intended to provide IT managers with insight into key issues impacting the ability to develop and deploy network-centric business applications. Previous survey reports include:

- ASP Network Infrastructure
- Convergence and New World Services Providers
- E-Business Network Architecture/Infrastructure
- Enterprise Operating Systems and Directory Services
- Management Intranets
- Network and Systems Management Total Cost of Ownership
- Network Challenges and Opportunities in Uncertain Times
- Network Operations Centers
- Network Professionals Job Satisfaction
- Network Quality of Service
- Network Security
- Performance Management and Engineering
- Remote and Mobile Network Access
- Service Level Management
- Virtual Private Networks

To see the results of these surveys or to participate in the latest Lucent Technologies network industry survey, visit our web site at:

http://www.lucent.com/businessunit/worldwide.html

If you would like to learn how Lucent can help you implement or improve your networking capabilities, please call us at 1-888-767-2988 in the U.S., or 650-318-1020 outside the U.S., or email: networkcare@lucent.com.

Methodology

This survey was conducted over the World Wide Web from April 30, 2001 – May 31, 2001 at:

http://www.lucent.com/contact/current_survey.html

All Web survey responses were automatically collected into a survey tool. Any questions skipped or incorrectly answered by survey respondents were not included in the tabulations. Not-applicable responses were also not included in the tabulations. Each chart includes the number of valid responses for that particular question (e.g., N=100 indicates 100 responses). Percentages shown in charts may not equal 100 percent due to rounding.

For additional information, please contact your Lucent Technologies Sales Representative or your Lucent Advantage Reseller. You can also visit our web site at www.lucentservices.com or call 1-888-767-2988 in the U.S. or 1-650-318-1020 outside the U.S.

Lucent Technologies
Bell Labs Innovations



VitalSuite and VitalQIP are trademarks of Lucent Technologies Inc. All other trademarks and registered trademarks are properties of their respective holders. This document is for planning purposes only and is not intended to modify or supplement any specifications or warranties relating to Lucent Technologies products or services. ©2001 Lucent Technologies Inc. All rights reserved. Printed in U.S.A.Lucent Technologies Inc. Marketing Communications IS.SEC.8067.0701

1213 Innsbruck Drive
Sunnyvale, CA 94089

Bulk Rate
US Postage
PAID
Permit No.426
Sunnyvale, CA