



Information Security

By Rick Blum, Senior Manager, Strategic Marketing

Highlights

- 91% of respondents place improving security among their top priorities over the next 12 months. 29% say it is their number-one priority.
- More than three-quarters of respondents are satisfied with their current security capabilities as well as the products available to improve those capabilities.
- Email and remote access for mobile workers are the top two sources of concern for potential information security breaches. Inadequately trained and unconcerned users is the top issue.
- External hackers are the top source of attacks, which prove to be the most damaging or costly. However, internal sources are quickly catching up on both measures.
- The two most important elements of a comprehensive security program are the security infrastructure and remote access and authentication services.
- The most frequent, significant barrier to improving security capabilities is the high cost of security products and tools, which contributes to the second most frequent barrier: justifying costs/benefits for upper management.

The Bottom Line

Because the sharing of data, both internally and externally, has become such an integral part of most enterprises, protecting network and systems and the data contained within them is critical to ensuring smooth and safe business operations. While most organizations have boosted their efforts to improve security, doing so can be difficult to justify in tight budgetary times. Still, the high visibility of data theft along with new regulatory requirements has convinced most IT organizations, along with business units, to put security high on their priority lists.

Based on this survey, security professionals should consider the following:

- *The most difficult task on the road to improved security capabilities is overcoming upper management resistance to investments that can't show a corresponding financial return. A solid business case must include the potential cost of a successful network breach and data loss, including financial damages (outright theft), recovery costs (notification of affected parties, etc.) and loss of reputation (leading to loss of business).*
- *While the focus has rightly been on external threats in the past, it is time to look inward. Internal sources of attacks and data theft are catching up to external sources and require a new set of strategies and technologies (e.g., identity and access management) to safeguard valuable data.*
- *Mobile workers, mobile devices and wireless networks are putting a whole new set of security problems on the table – ones that must be dealt with sooner rather than later. You can't stop the train, so make sure the tracks are built from the start with the proper safeguards.*
- *All the technology in the world won't prevent a user from giving away his password. A complete security program must include a sizable effort to build, implement and enforce processes and procedures that will strengthen security. However, this effort will be for naught if an equal emphasis and effort is not expended on training users on good security practices and demonstrating to them the cost of indifference.*

Introduction

With incidents of data theft and general malicious activity on the rise, information security is at or near the top of the priority list for many business units as well as IT organizations. Developing a comprehensive security plan can mean different things to different companies. Budgets are not as tight as they once were, but IT organizations are still having to determine what is the best use of their limited resources based on perceived potential dangers (for instance, external attacks versus internal theft) and what security activities will drive the greatest benefits.

From June 15, 2006 through July 31, 2006, INS conducted a Web-based survey on information security, which was completed by 84 IT professionals around the globe. This survey was designed to yield valuable insights into the current state of and future plans for information security in respondents' IT organizations. The results of the survey are also compared in some instances to the results of a similar survey conducted by INS in early 2003.

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

The information security survey was posted on the INS Web site at <http://www.ins.com/knowledge/surveys/industrySurvey.asp>.

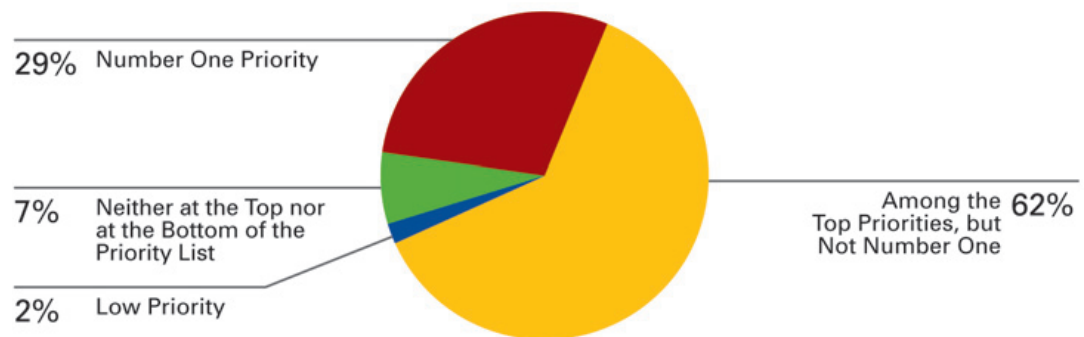
Invitations to participate in the survey were sent to subscribers of the INS NetKnowledge newsletter and former INS industry survey participants. All Web survey responses were automatically collected into a survey tool. Any questions skipped or incorrectly answered by survey respondents were not included 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.

The Current State of Security

While everyone recognizes the importance of securing networks, systems and data from both internal and external intruders, information security initiatives must still compete with other IT objectives and projects for both mindshare and budget.

Perhaps it is the amount of publicity that data theft and other malicious activities have received in recent years that explains why more than 90 percent of respondents say that improving information security is among their top priorities. Furthermore, 29 percent of respondents consider improving information security their number one priority. If companies' networks and systems are breached, it is not for lack of attention to security considerations.

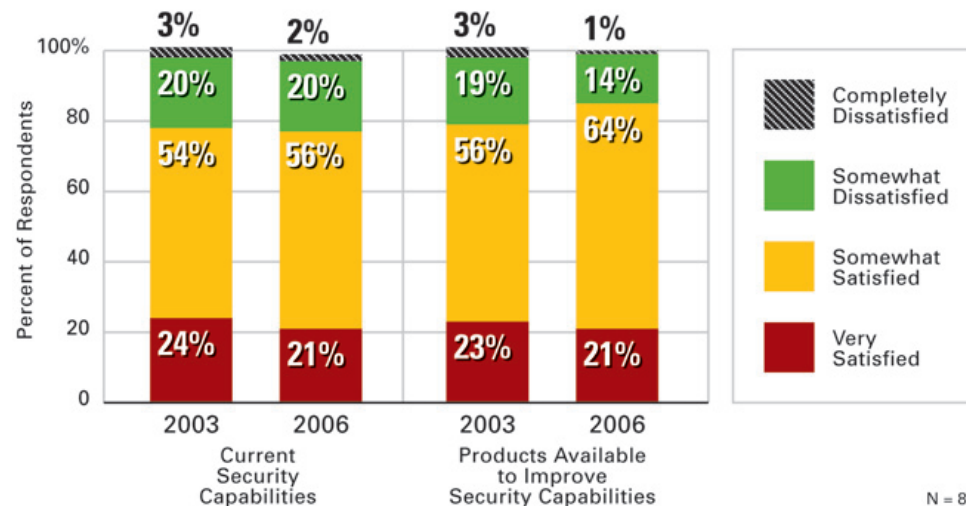
Improving Security Compared to Other IT Priorities



N = 84

We asked respondents to tell us how satisfied they are with two aspects of security: first, their current security capabilities and second, the products available to improve those security capabilities. We then compared their answers to the results from the same questions that we posed to a similar group in 2003.

Satisfaction with Security Capabilities and Products



N = 86

Surprisingly, and despite all the attention security has received, the satisfaction IT professionals have with their information security capabilities has changed little. In 2003, 78 percent of respondents were very (24 percent) or somewhat (54 percent) satisfied with their security capabilities. This year, the combined figure is 77 percent, with a nearly identical split between the *very satisfied* and *somewhat satisfied* responses. Perhaps we can conclude from this that even as security capabilities have increased over the last three years, the level of threats has increased at an equal rate. As a consequence, satisfaction has remained constant. With this seeming balance of capabilities and threats, it becomes imperative for IT security organizations to constantly monitor and measure the effectiveness of their security program to make sure it is optimized to meet the new and evolving threats.

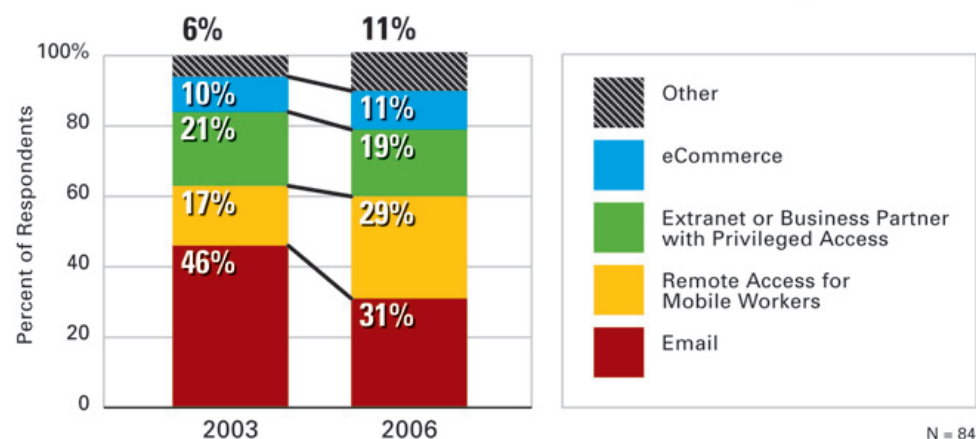
The situation for satisfaction with products available to improve security capabilities is similar; although, satisfaction increased a bit – from 79 percent in 2003 to 85 percent in 2006. Again, products are struggling to keep up with the dizzying changes in tactics to breach networks and systems, as well as the expansion of potential vulnerabilities to new technologies such as wireless and mobile computing and voice over IP. The battle seems to be never ending.

Sources of Concern

Intruders have a number of entryways into enterprise networks. Chief among them are email, remote access for mobile workers, extranets (or business partners with privileged access) and ecommerce. Currently, the first two are the primary sources of access that concern respondents about their potential for a security breach. Email is the top concern of 31 percent of respondents, while remote access for mobile workers is the top concern of 29 percent of respondents.

This result is significantly different than the concerns in 2003, when nearly half of respondents listed email as their top concern, and only 17 percent listed remote access for mobile workers. This dramatic shift over the last three years accurately reflects the growth of mobile computing and the maturing of email systems. Other sources of concern include stolen laptops and mobile devices.

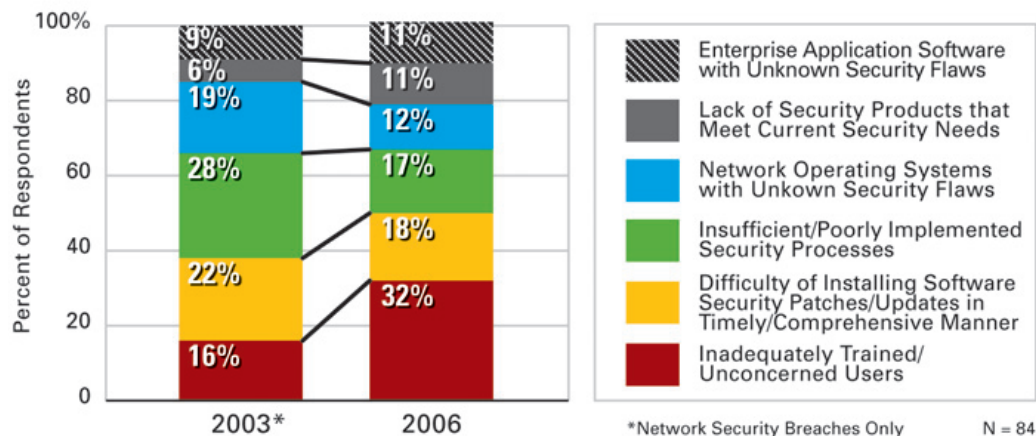
Access Source of Most Concern for Potential Security Breaches



The second question we asked of respondents is which of six issues causes them the most concern for potential information security breaches. Again, the results show a significant shift over the last three years.

In 2003, the top issue causing concern was network operating systems with unknown security flaws, cited by 28 percent of respondents. Today, that number has shrunk to just 17 percent, dropping it to only the third most frequent concern.

Issue that Causes Most Concern for Potential Security Breach



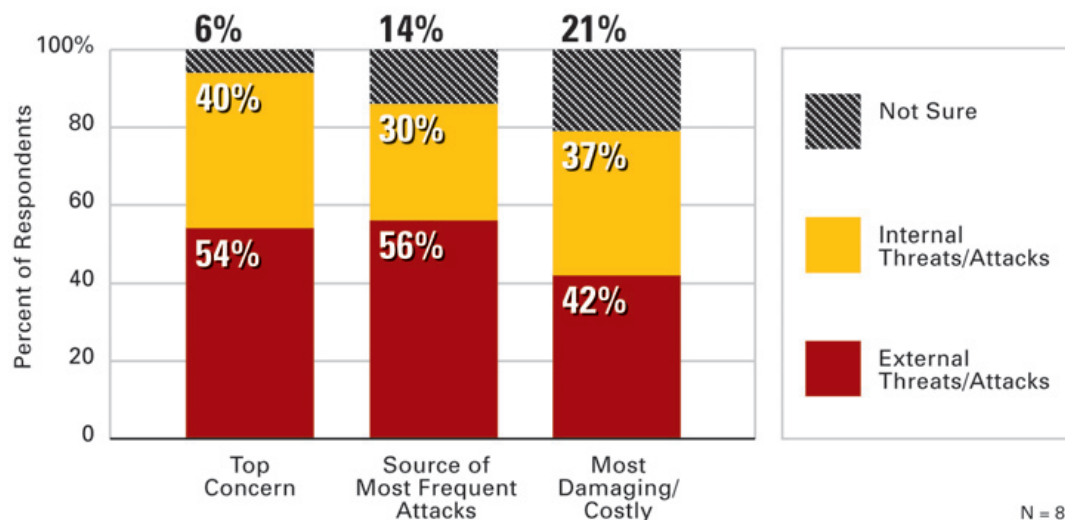
The top concern today is inadequately trained and unconcerned users, cited by nearly one-third (32 percent) of respondents. This is double the percentage in the 2003 survey. Undoubtedly, users have not gotten less savvy or aware of security requirements in the last three years; more likely, the importance of security has gained visibility in the business while IT has come to realize how weak a link users are compared to technological vulnerabilities. (It should be noted, however, that the 2003 survey was specifically about network security, not the broader information security, which undoubtedly accounts for some of the shift in concerns.)

Currently, the second leading concern is the difficulty of installing security patches and updates in a timely and comprehensive manner. The patch problem is ongoing as the volume increases with every new attack. Clearly, it is one that many IT organizations are still struggling to effectively resolve.

Email continues to be the top access concern and users the top issue for security breaches. The third leg of the stool is external and internal threats. We asked respondents three questions around this topic: Which is the bigger concern? Which is the source of most frequent attacks? Which is the most damaging and costly?

By a slight margin, external threats and attacks are more frequently the top concern as compared to internal threats and attacks. However, internal concerns are up 16 percent from 2003, showing a significant change in IT professionals' perspective about the source of potential security breaches.

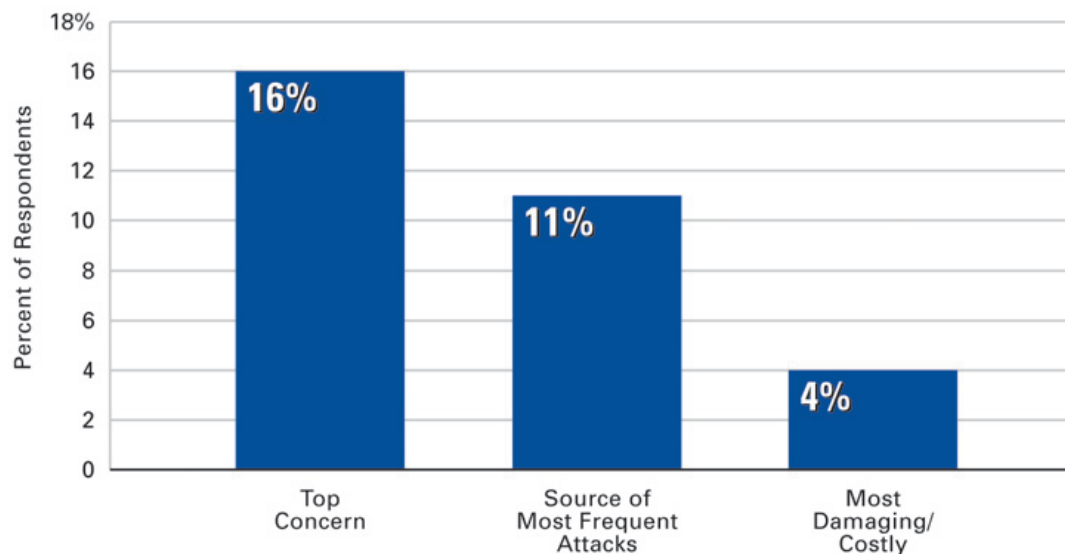
External vs. Internal Security Threats



As for the frequency of attacks, external hackers are still the top source of attacks for 56 percent of respondents; although, that number is down from 63 percent in 2003. Internal sources, on the other hand, are up from 19 percent in 2003 to 30 percent this year, consistent with the shift to internal threats as the top concern overall. Quite a few respondents are uncertain where attacks are coming from, thereby demonstrating a major vulnerability.

On the third question – most damaging and/or costly source – respondents’ uncertainty jumps up to 21 percent. As a consequence, neither external (42 percent) nor internal (37 percent) sources are cited as most damaging or costly by as many as half of respondents. However, the ratio of internal to external is the highest among the three measures, raising the urgency to not just add more firewalls to the network, but to implement security systems that manage identity and access.

Change since 2003 in Internal Sources as Security Threats

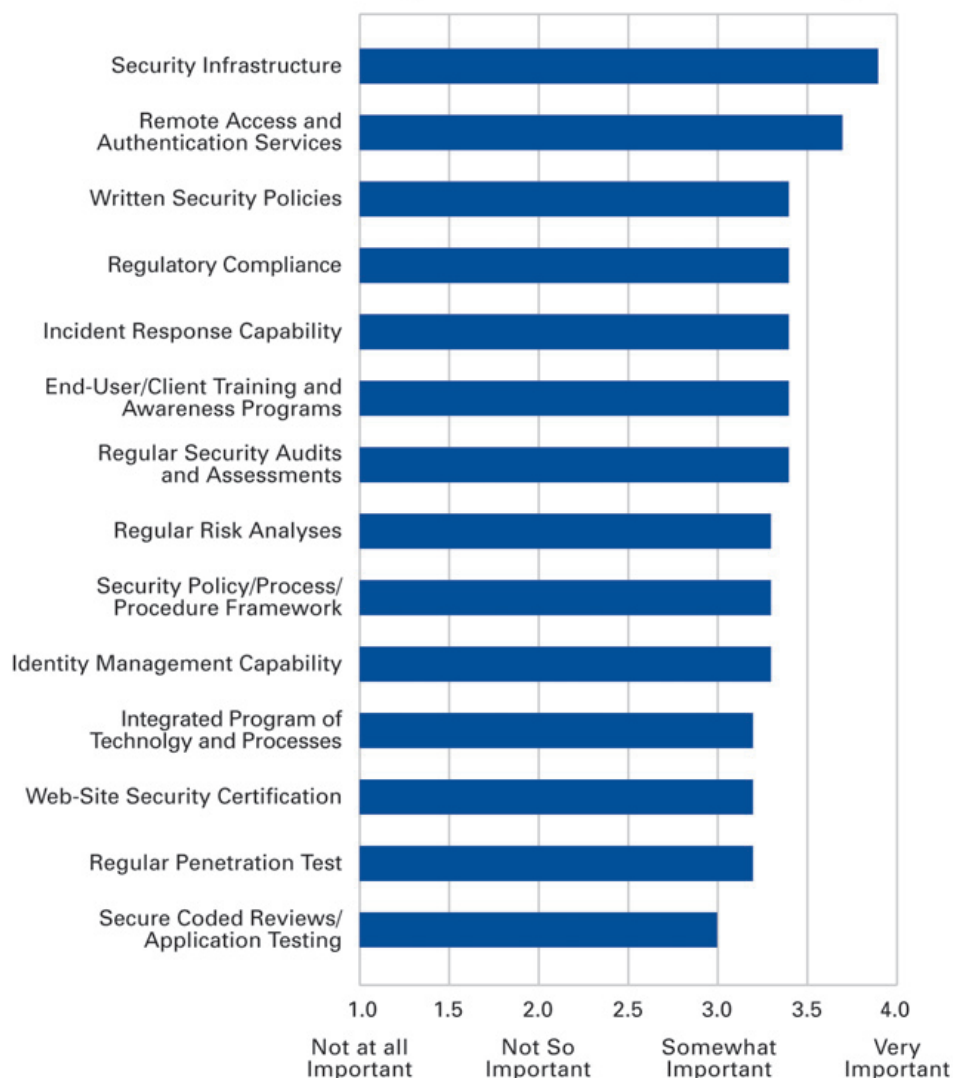


Security Importance and Barriers to Improvement

There are many elements to a complete security program. We listed 14 common ones and asked respondents how important each is to their total security efforts.

Without any question, security infrastructure is the most important element of respondents' security efforts, with 92 percent rating it as very important and the remainder as somewhat important. The second standout element is remote access and authentication services, which 69 percent rate as very important and 29 percent as somewhat important. Though not nearly as universally important as security infrastructure, this still stands well ahead of other elements.

Importance of Various Security Elements to Total Security Effort

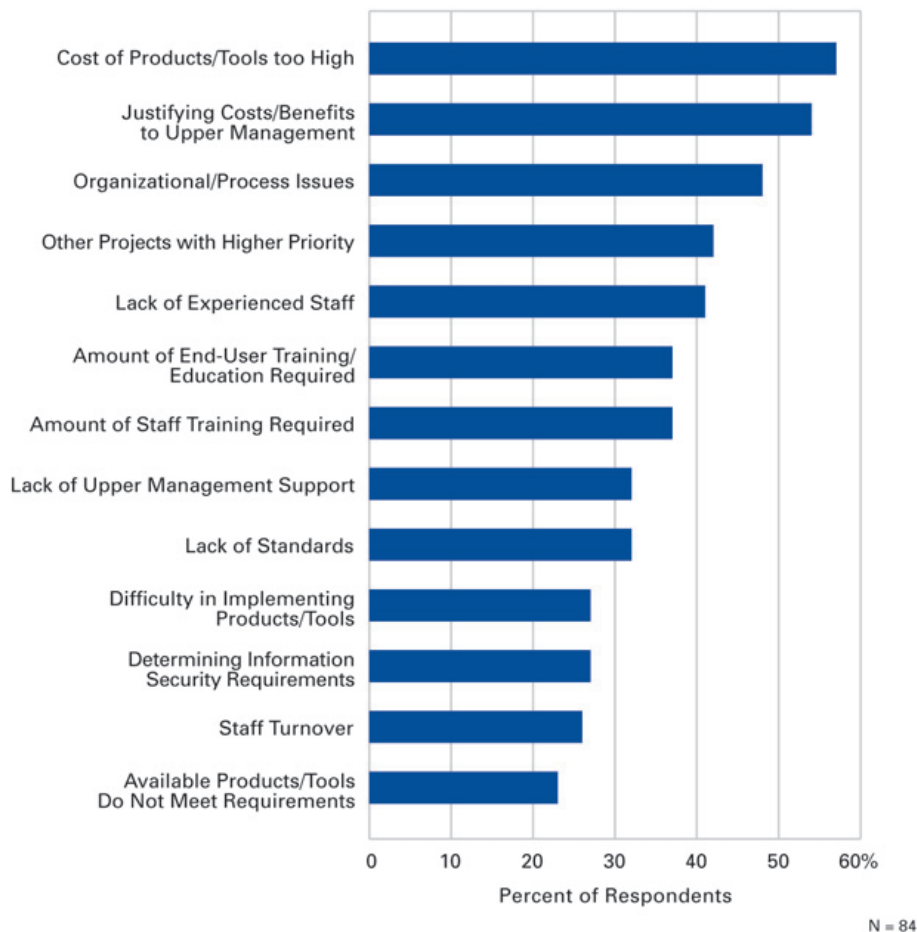


After the top two elements, the differences in importance of the other elements are not very large, with the exception of secure coded reviews/application testing, which only one-third of respondents consider very important. The obvious conclusion is that a well-designed and implemented security program is not a simple goal to reach, and requires multiple skills and much effort.

With it clear that building a world-class security program is a difficult task, we asked respondents to indicate which of 13 possible barriers to improving their security capabilities are significant for them. There is more differentiation in the responses to this question than the last.

The most common barrier is the high cost of security products and tools, which 57 percent of respondents say is a significant problem. The problem with products and tools appears to be strictly cost, though, as the least common significant barrier is that products and tools don't meet security requirements. Additionally, only 27 percent of respondents say that the difficulty of implementing security products and tools is a significant barrier for them.

Significant Barriers to Improving Information Security Capabilities

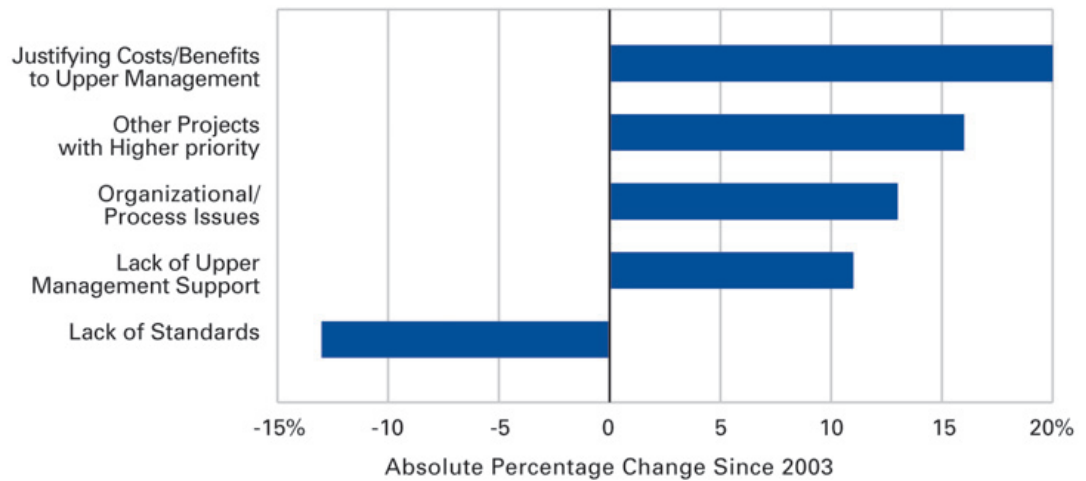


The perception of high product and tool cost probably plays into the next most common significant barrier, which is justifying costs/benefits of improving security capabilities to upper management, an issue for 54 percent of respondents. Obviously, the higher the cost of products, the more difficult it is to justify their benefits. This is particularly true in the security space, where improving capabilities does not generally create more revenue opportunities – just a reduction in risk, which management may or may not see as a priority. Furthermore, cost/benefit justification has become a more frequent problem since 2003, when only one-third of respondents identified it as a significant barrier.

Beyond cost and cost/benefit justification, more than 40 percent of respondents see organizational and process issues, other projects with higher priority and lack of experienced staff as significant barriers. This last barrier is frequently overcome by working with security consulting firms. It does not seem, however, to be tied to staff turnover, which is a significant barrier for only 26 percent of respondents.

As previously mentioned, justifying cost/benefits to upper management has become more common as a significant barrier over the last three years. Other barriers that also increased a substantial amount in this timeframe are: other projects with higher priority (16 percent), organizations/process issues (13 percent) and lack of upper management support (11 percent). The only significant barrier that has substantially decreased in frequency over the last three years is lack of standards, which is down from 45 percent to 32 percent.

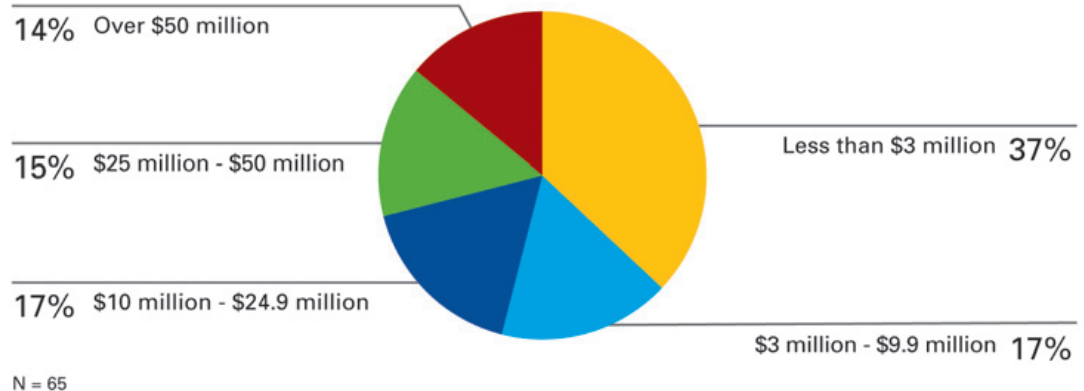
Biggest Changes to Significant Barriers



Respondent Demographics

Thirty-seven percent of respondents' IT organizations have an annual IT budget of less than \$3 million; fourteen percent have budgets exceeding \$50 million. The remaining respondents' IT organizations are fairly evenly distributed between these two amounts.

Respondents' IT Organizations' Annual Budgets



About INS

INS is a leading global provider of business-driven information technology consulting and software solutions. For more than a decade, we've been helping organizations effectively use technology to achieve strategic business goals. Our security consulting practice was founded in 1994, and helps reduce risk and mitigate vulnerabilities to threats to IT infrastructures through sound practices, applied security technology and a continuous improvement framework.

Our Security Portfolio is comprised of one of the largest and most experienced security consulting teams in the world. INS Security consultants maintain certifications across leading security disciplines and technologies, and have extensive knowledge and experience with current security standards, best practices and government regulations, including ISO 17799/BS7799, HIPAA, Sarbanes-Oxley and Gramm-Leach Bliley. INS is an NSA INFOSEC security-certified company, having received the highest rating of all certified companies. Because of the strength of our security expertise and scope of our services, we are an official go-to partner for Microsoft Security.

The INS solution portfolio enables our customers to reduce costs, increase flexibility, strengthen security, ensure compliance and improve efficiency.

- **Infrastructure Transformation** builds high-performing, resilient and scalable network infrastructures.
- **Information Risk Management** reduces risk, mitigate vulnerabilities and ensure ongoing compliance.
- **Business Productivity** streamlines collaboration, improve program execution and enable more effective decisions.
- **Enterprise Architecture and Governance** helps improve visibility and control over IT initiatives to better meet business goals.

We apply our structured methodologies, strategic alliances and diverse industry experience to deliver in-depth analyses and implement custom solutions aimed at driving business growth. Our consultants hold over 1,100 certifications in 96 categories and our KnowledgeNet database gives them access to over 15 years worth of intellectual property, solutions and proven techniques in an easily-searchable format.

Our customers include global enterprises and service providers in all major industries, including telecommunications, financial services, retail, pharmaceutical/healthcare, manufacturing, government and travel and transportation. INS is headquartered in Santa Clara, Calif., and has 38 offices in the U.S., Europe, Middle East and SE Asia.

For additional information, please visit www.ins.com or contact INS at 1-888-767-2788 in the U.S., 44 (0) 1628 503000 in Europe, 65 6549 7188 Asia, or 1-408-330-2700 worldwide.

About INS IT Industry Surveys

INS conducts industry survey projects intended to provide IT managers with insight into key issues impacting the ability to develop and deploy IT-infrastructure-dependent business initiatives.

Previous survey report topics include:

- Application Impact Assessment
- Ethical Hacking
- IP Address Management
- IPv6
- IT Infrastructure Library (ITIL)
- Malicious Code
- Network and Systems Management
- Total Cost of Ownership
- Network Operations Centers
- Network Security
- Outsourcing and Offshoring
- Quality of Service
- Performance Management and Engineering
- Security Patch Management
- Server Virtualization
- Service Level Management and Service Level Agreements
- Storage Networking
- Virtual Private Networks
- Voice Over IP
- Wireless LANs

To see the results of previous surveys, go to <http://www.ins.com/resources/surveys/>.

For more information regarding the IT industry survey program, please contact:

Rick Blum

Senior Manager, Strategic Marketing
Email: rick.blum@ins.com

