BT INS IT Industry Survey

Ethical Hacking

By Rick Blum, Senior Manager, Strategic Marketing

Highlights

- The top three benefits of ethical hacks, in order of importance, are to improve overall security, protect against theft of intellectual property and fulfill regulatory/legislative mandates.
- Most organizations conduct ethical hacks on at least an annual basis. Wireline networks and operating systems are most frequently tested, while applications and wireless networks are tested less often. Organizations with security budgets of more than $1 million conduct ethical hacks far more often than those with budgets of less than $100,000.
- Only five percent of respondents think there is no chance of being hacked in the coming year. Nearly half place the odds of being hacked at greater than 50 percent.
- When respondents' IT organizations don't conduct ethical hacks, the most frequent reason given is that management does not value it.
- More than half of respondents have found some vulnerabilities with moderate impact when conducting an ethical hack of their networks, operating systems or applications.
- When using a third-party vendor strategy to conduct multiple ethical hacks, 24 percent of respondents will choose the best vendor and stick with them, while 25 percent will rotate vendors on a regular basis.

The Bottom Line

Cyberspace is becoming an evermore dangerous place, especially to IT organizations that are charged with protecting sensitive data and maintaining web sites that generate revenue. Along with these dangers, studies show that internal threats are just as dangerous, particularly to applications that are readily accessible over intranets. Since locking down all networks is not a viable option, the only response that security managers can realistically execute is to harden their networks, applications and operating systems to a reasonable level of safety, and go on conducting business.

A critical tool in the battle to identify IT infrastructure vulnerabilities is the ethical hack, which simulates an attack in order to truly understand the effectiveness of current security controls. Trying to secure a network without conducting an ethical hack is little more than guess work. Without proper validation, real assurance of security is impossible.

Regular ethical hacks can create value beyond just identifying vulnerabilities. They can also help comply with regulatory mandates, protect against lawsuits and justify security investments. This latter benefit is particularly important as gaining the support of corporate management can be a major obstacle, particularly when using third-party ethical hacking vendors that provide an objectivity and expertise that internal resources simply can't guarantee. Ethical hacks are truly a necessity in today's computing environment, and any IT organization that forgoes this activity for long risks putting the entire enterprise in jeopardy.

Introduction

Identifying risks and vulnerabilities is crucial to preventing exposure of sensitive data, as well as for protecting the corporate reputation. IT organizations must proactively manage risk by conducting ethical hacks on a regular basis in order to identify potential vulnerabilities in their networks, operating systems and applications.

From January 13 through February 14 2007, BT INS conducted a Web-based survey on Ethical Hacking, which was completed by 150 IT professionals around the globe. This survey was designed to yield valuable insights into the usage of ethical hacking to improve network, systems and application security. Results of this survey are also compared, when appropriate, to the results published in January 2005 of an ethical hacking survey BT INS conducted in late 2004.

For this survey, ethical hacking, also called penetration testing, was defined as a method for verifying the true state of security controls for the protection of assets and information by simulating an attack on a network in a controlled and safe manner. Ethical hacks are typically conducted by a third party in a manner similar to naturally occurring attacks to provide an unbiased assessment of the security of a system and the viability of implemented controls.

The survey was posted on BT INS' Web site at
http://www.ins.com/knowledge/surveys/industrySurvey.asp

Invitations to participate in the survey were sent to individuals who had requested information from BT INS as well as former BT 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.

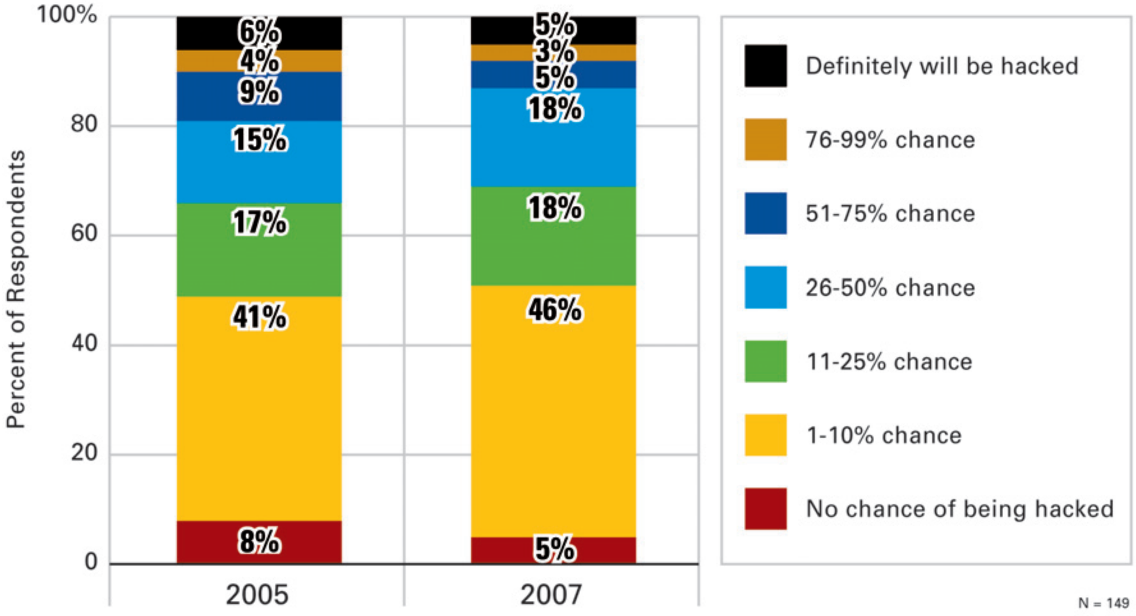
Hacking Concerns

Ethical hacks are typically thought of as being defensive measures, that is, the object is to identify weak points in the network, operating systems or applications that an attacker might exploit, then close those weakness to prevent compromise of data or other destructive actions. Over the last few years, it has become increasingly clear—not only to IT security professionals, but also to the public in general—that many, if not most, networks are still vulnerable to attack. This reality is reflected in the finding that 95 percent of survey respondents believe that there is some likelihood that their network will be successfully hacked in the coming year. This result is up slightly from the 2005 survey, when only 92 percent of respondents acknowledged the likelihood of being successfully hacked.

> *"...the percentage of respondents who place the likelihood of being successfully attacked at 50 percent or less has increased over the last couple of years..."*

The good news, however, is that the percentage of respondents who place the likelihood of being successfully attacked at 50 percent or less has increased over the last couple of years—from 81 percent to 87 percent. Although this is a small gain, it is, at least, a step in the right direction. Similarly, the percentage of respondents who think the likelihood of being hacked is 10 percent or less also increased to over half. While this progress can be hailed, the improvement is marginal for two years of effort, indicating more that people who want to attack networks continue to find new and successful tools and strategies for doing so than a lack of effort on the part of IT organizations.

Likelihood of Being Successfully Hacked in Next 12 Months



To better protect their networks (wireline and wireless), operating systems and applications from attack, the vast majority (79-86 percent) of respondents' IT organizations conduct ethical hacks, though with varying degrees of regularity.

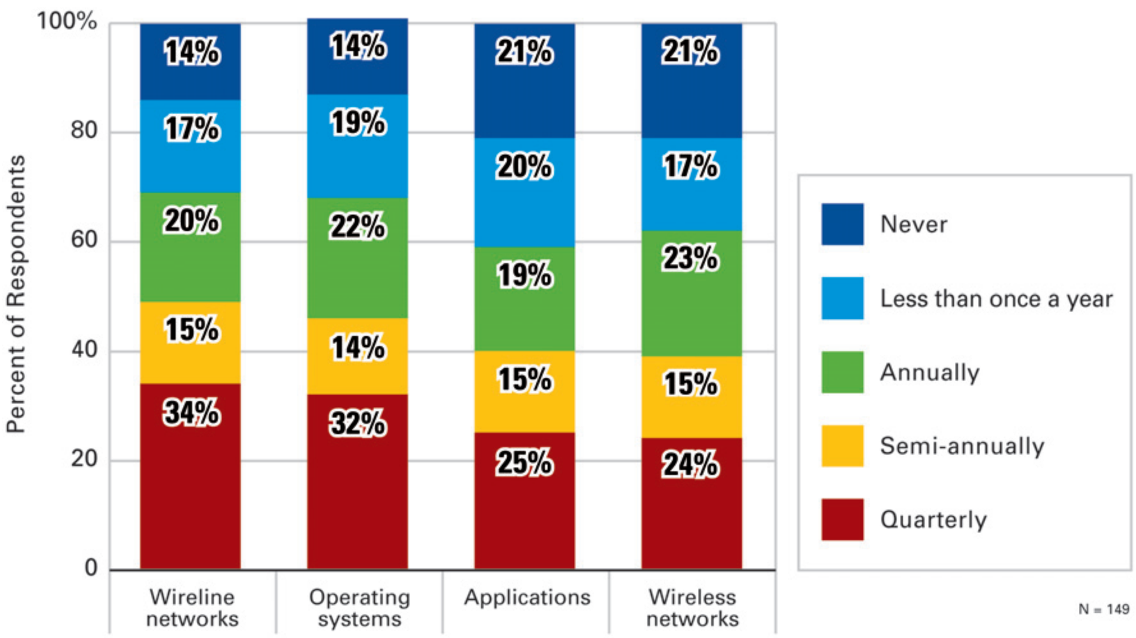
"Wireline and operating systems are most frequently subject to ethical hacks...wireless networks and applications don't receive as much attention..."

Wireline and operating systems are most frequently subject to ethical hacks—approximately one-third of respondents do so on a quarterly schedule. Wireless networks and applications don't receive as much attention, with only about one quarter being ethically hacked on a quarterly basis.

As might be expected, respondents who conduct ethical hacks quarterly on both their wireless and wireline networks are significantly more likely (68 percent) to believe that the chance of their networks being successfully hacked in the next year is less than 10 percent than those who conduct ethical hacks less than once a year or never (45 percent). Still, seven percent of respondents who conduct ethical hacks quarterly believe that their networks will definitely be hacked successfully in the coming year.

Fourteen percent of respondents' wireline networks and operating systems are never ethically hacked, as are 21 percent of wireless networks and applications. For these organizations, the motto seems to be "What we don't know won't hurt us."

Frequency of Ethical Hacks

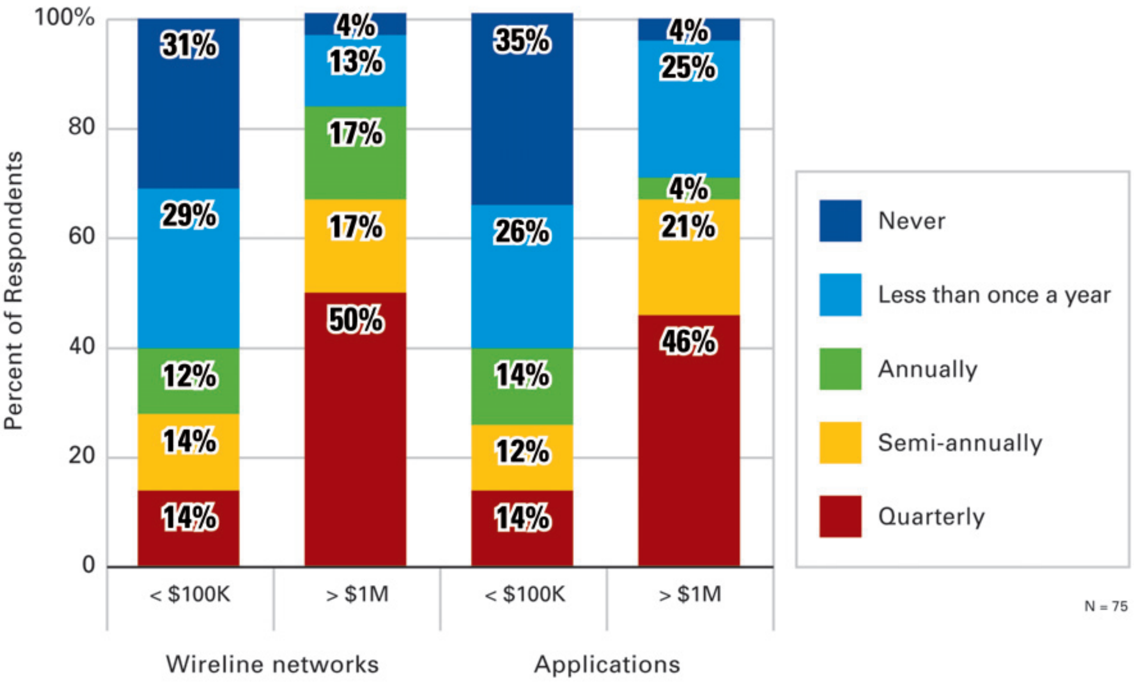


While companies that never conduct ethical hacks are taking a risk, the reason behind this approach may be related primarily to budgetary considerations. Companies that annually spend less than $100,000 on security are far less likely to regularly conduct ethical hacks. For example, only 14 percent of these companies conduct quarterly ethical hacks on wireline networks and applications, while 46-50 percent of companies that spend more than $1 million on security do so. On the other end of the scale, 31-35 percent of companies with small security budgets never conduct ethical hacks, while only four percent of companies with large security budgets take this course. The results for operating systems and wireless networks are similar.

> *“...31-35 percent of companies with small security budgets never conduct ethical hacks.”*

Small companies understandably are less likely to spend a portion of their security budget on activities that don’t have immediate impact, but they must understand the risk of doing so. While a large company that gets attacked may be able to survive a lawsuit (or web-site downtime) with minimal impact, the effect on a small company could be fatal. These companies must carefully and consciously judge the level of risk and the sensitivity of stored data against the palliative effects of ethical hacks.

Frequency of Ethical Hacks by Annual Security Budget Size



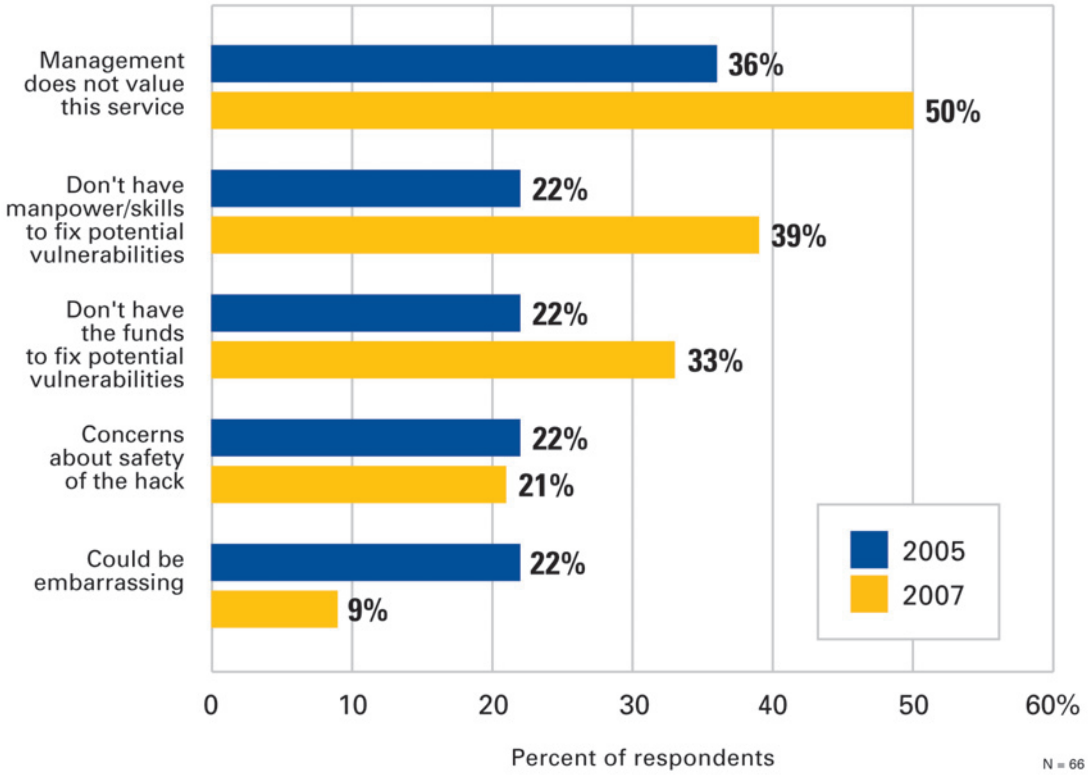
So what are some of the other reasons for not conducting ethical hacks? Respondents who never conduct ethical hacks in any one of the four categories say the most common reason (selected by 50 percent of respondents) is simply that management does not understand the value of ethical hacks and, presumably, will not allocate the time and money required to conduct them. What is most surprising about this result is that, despite the extremely negative publicity a number of companies that have lost sensitive data have encountered over the last couple of years, management's perception of the value of ethical hacking seems to have decreased since 2005. Security professionals need to reexamine how they are presenting ethical hacking to management, perhaps with greater focus on business consequences.

The next most common reason for not conducting ethical hacks, selected by 39 percent of respondents, is that the IT organization doesn't have the manpower and/or skills to fix potential vulnerabilities that are uncovered during the hack. This "excuse" is a bit like an ostrich sticking its head in the sand; choosing not to know is a dangerous course to take.

Similarly, 35 percent of respondents say their IT organizations don't have the funds to fix potential vulnerabilities. Again, a head-in-the-sand approach won't cut the mustard when the CEO wants to know how customer data was stolen, or why the web site was down for hours (or days) due to an attack. Better to know the problem—and the cost of a fix—than to plead ignorance.

Only one-fifth of respondents are concerned about the safety of the hack, and less than one in ten is worried that the results of an ethical hack could be embarrassing.

Reasons for Not Conducting Ethical Hacks



Note: includes only respondents who never conduct ethical hacks on their wireline networks, wireless networks, operating systems or applications.

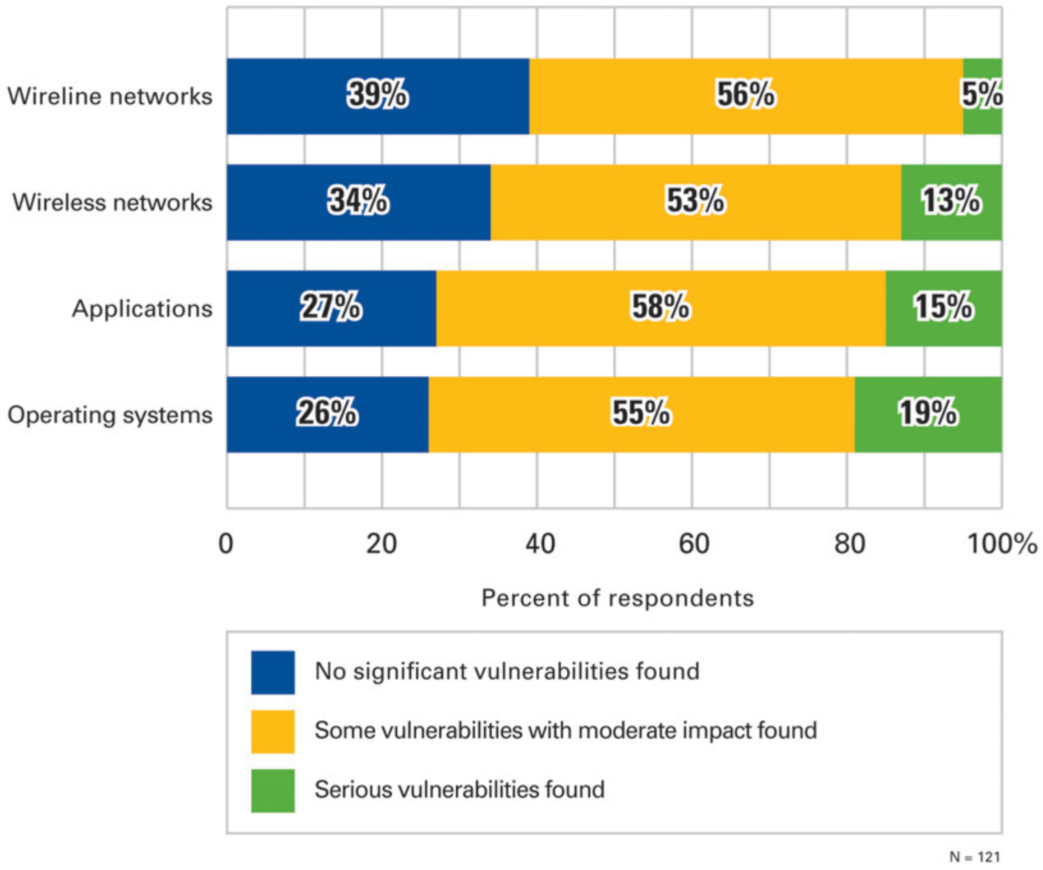
We then turned to respondents who have conducted at least one ethical hack and asked them to tell us for each of the four categories what level of vulnerabilities were found — either serious, moderate, or insignificant.

Operating systems are most likely to be insecure, with 19 percent of those tested having serious vulnerabilities, and another 55 percent having some vulnerabilities with moderate impact. Barely more than one-quarter had no significant vulnerabilities. Applications fare slightly better than operating systems, although not by a significant amount.

Networks, both wireline and wireless, have the lowest levels of significant vulnerabilities, especially wireline networks, for which only five percent of ethical hacks turned up significant vulnerabilities.

Overall, the picture is not bright, although not completely bleak either. Ethical hacks uncovered some vulnerabilities of moderate to high impact in at least six out of ten networks, applications and operating systems. The industry is going to have to do much better than that to win back the public's trust.

Significance of Vulnerabilities Uncoverd by Ethical Hacks



Ethical Hacking Strategies and Benefits

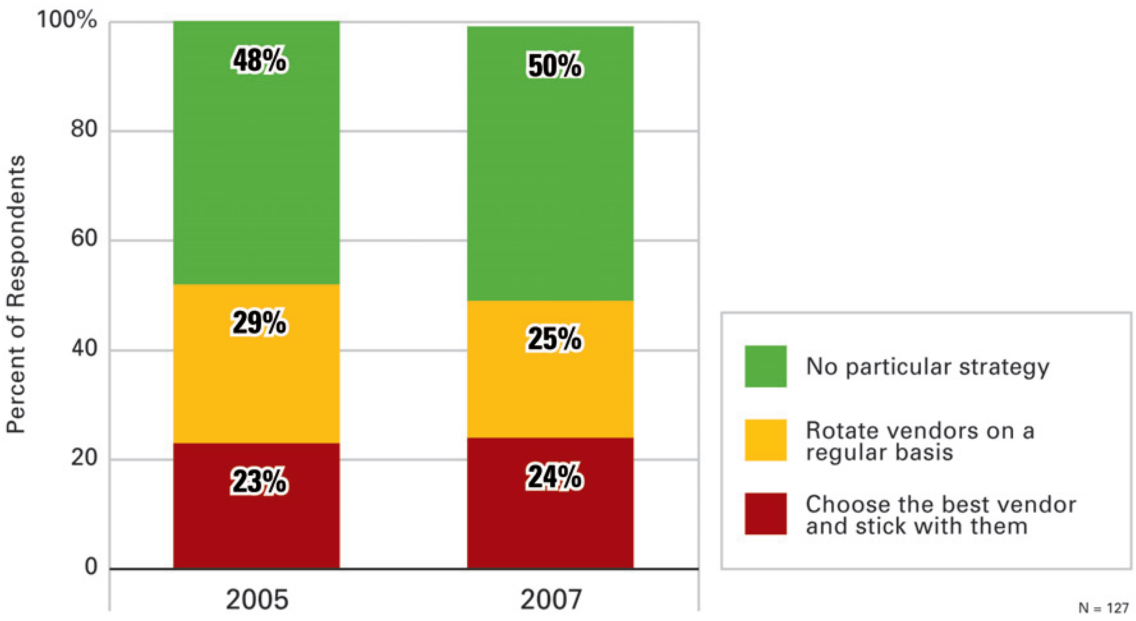
Most IT organizations use third-party providers of ethical hacking services to test for vulnerabilities in their networks for a number of reasons including:

- Ethical hacking specialists have more expertise and tools than in-house resources
- Tests can be conducted with zero-knowledge to truly mimic a random intruder
- Testing can be done without the knowledge of other IT employees

For the more than 80 percent of respondents whose IT organizations have used third-party, ethical-hacking vendors, their approaches varied widely. Half of these respondents do not have a strategy, formal or informal, for working with ethical hacking vendors. This is nearly the same results as in the 2005 survey, indicating the maturity of this critical element of security is still in its early development stages. We can only assume that these organizations operate on an ad hoc basis, making a decision whether to use the same or a new vendor with each ethical hack. While not necessarily a terrible approach, it doesn't show the level of concern that the other respondents display for the ethical hacking process by actively selecting a multivendor or single-source strategy.

One quarter of respondents rotate vendors on a regular basis to gain an extra layer of insurance that all vulnerabilities will be identified over time. Twenty-four percent prefer to choose the best vendor for ethical hacking services, and then stick with that vendor. If the vendor is fully aware of the latest vulnerabilities, uses proven methodologies and has a staff that is well experienced, this can also be a successful strategy, and it allows building of a relationship that may lead to long-term improvements in the underlying security architecture.

Third-Party Vendor Strategy for Ethical Hacks



N = 127

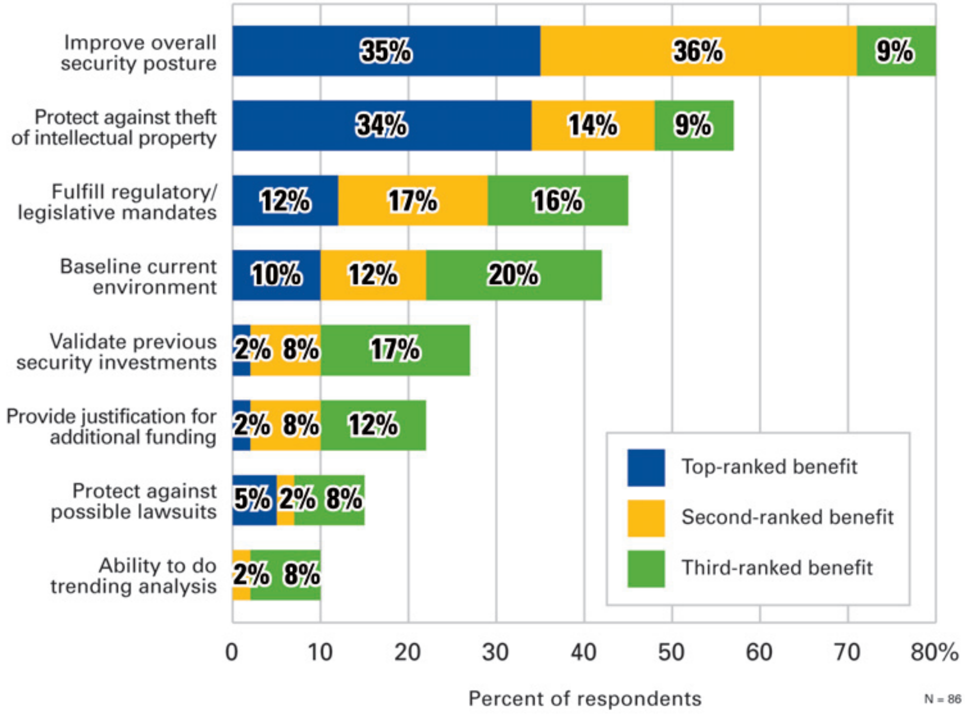
The reason for conducting an ethical hack is, obviously, to identify and remediate any vulnerabilities in networks, operating systems and applications. In doing so, however, a number of benefits can be achieved. We presented respondents with a list of eight potential benefits they could possibly receive from conducting an ethical hack, and asked them to rank the top three in order of importance. Not surprisingly, improving the overall security posture is the number one benefit by a wide margin, being listed in the top three by 80 percent of respondents, and the most important benefit by more than one-third.

Also ranked in the top three benefits by more than half of respondents is protecting against theft of intellectual property (IP). Thirty-four percent of respondents listed this as their top benefit. Taken together, more than two-thirds of respondents consider the top benefit of ethical hacks to be protection against theft of IP or improving security overall. Compared to the results in the 2005 survey, both of these benefits increased in popularity. In fact, theft of IP was listed as the top benefit by only 23 percent of respondents in 2005, compared to 34 percent this year.

The third most frequently reported benefit is fulfilling regulatory and legislative mandates. Twelve percent of respondents consider this their top benefit, 17 percent consider it the second most important and another 16 percent make it the third most important. With the spotlight on the Sarbanes-Oxley Act, Gramm-Leach-Bliley Act and numerous regulations and mandates, it is surprising that the total number of respondents who ranked this as a top-three benefit is exactly the same as the 2005 survey. Perhaps if the survey had been aimed at business executives, this benefit would have scored much higher.

Only one other benefit was selected by more than forty percent of respondents in their top three: baselining of the current environment. While this is useful data, clearly we can see why it is not ranked in the top three more often. Validating previous security investments hit the top three benefits ranking by 27 percent of respondents, while providing justification for additional funding was selected in the top three by 22 percent of respondents. Protecting against possible lawsuits and trending analyses were further down the list.

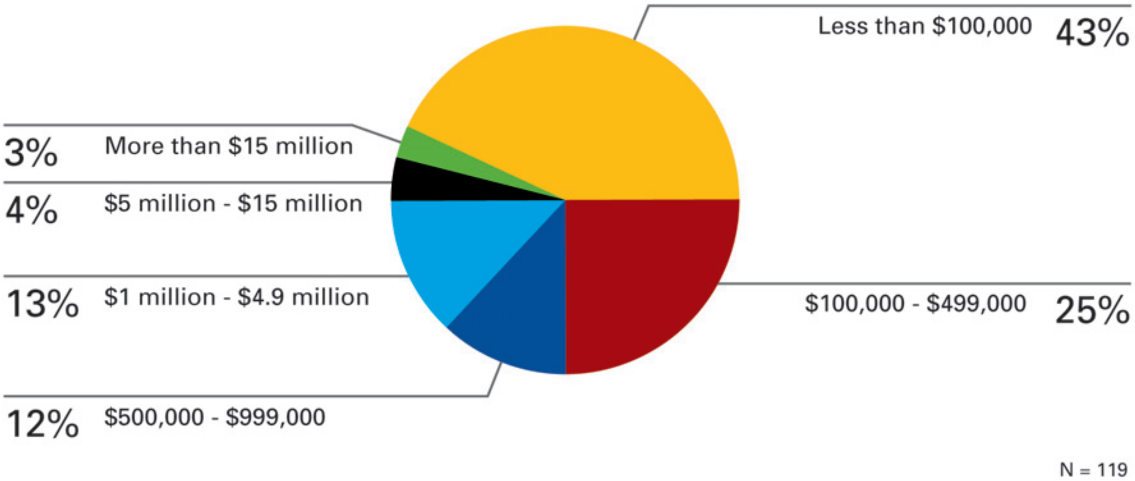
Ranking of Ethical Hacking Benefits



Security Budgets

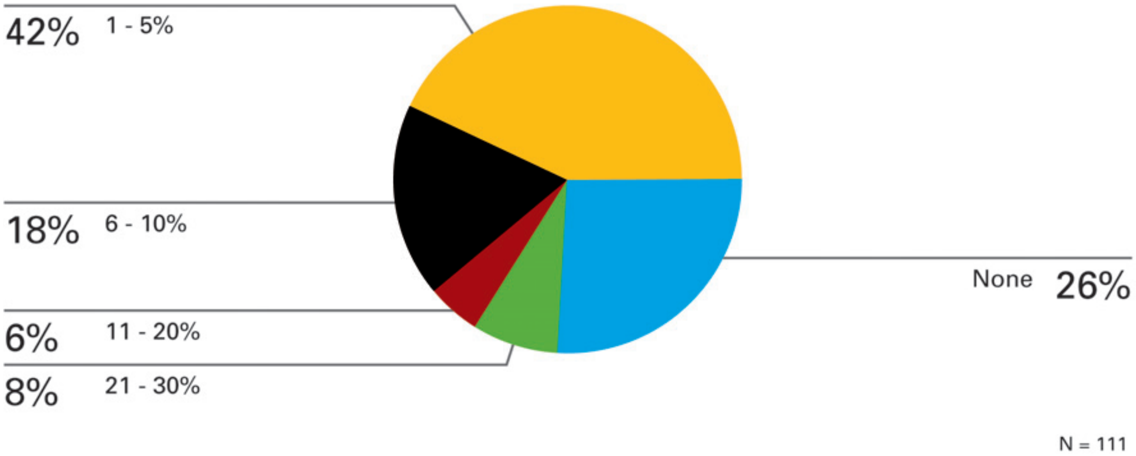
Two-thirds of respondents' IT organizations have annual security budgets of less than $500 thousand — the greater portion of those falling below the $100 thousand threshold. Another large chunk (25 percent) fall in the $500 thousand to $5 million range.

Respondents' IT Organizations' Security Budgets



Approximately one-quarter of respondents do not specifically allocate a portion of the security budget for ethical hacking, down from 32 percent in 2005. Forty-two percent of respondents allocate from 1-5 percent and 18 percent allocate from 6-10 percent of their security budgets for ethical hacking.

Percentage of Security Budget Used for Ethical Hacking



About BT INS

BT 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 unique 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. BT 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 http://bt.ins.com or contact BT 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 BT INS IT Industry Surveys

BT 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 (2004)
- Ethical Hacking (2005)
- Information Security
- IP Address Management
- IPv6
- IT Infrastructure Library (ITIL)
- Malicious Code
- Network and Systems Management Total Cost of Ownership
- Network Operations Centers
- 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://ins.com/resources/surveys.asp*
For more information regarding the IT industry survey program, please contact:

Rick Blum
Senior Manager, Strategic Marketing
Email: rick.blum@bt.com

All 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 BT INS products or services.