



ASSURANCE AND ADVISORY
BUSINESS SERVICES

 **ERNST & YOUNG**

Quality In Everything We Do

Global Information Security Survey 2004

Issues at a Glance

- Just 20% strongly agreed that their organizations perceive information security as a CEO level priority
- Respondents named “lack of security awareness by users” as the top obstacle to effective information security, however, only 28% listed “raising employee information security training or awareness” as being a top initiative in 2004
- “Employee misconduct involving information systems” was cited as a *distant* number two concern behind “major virus, Trojan horse or Internet worms” regardless of geographic region, industry or organizational size
- Less than half of the respondents provided their employees with ongoing training in security and controls
- Only 24% gave their information security department the highest rating in meeting the needs of the organization
- Only 11% deemed government security-driven regulations as being highly effective in improving their information security posture or in reducing data protection risks

A Message from Edwin Bennett



Edwin Bennett
TSRS Global Director

When we conducted our first information security survey in 1993, it was a joint-ventured project with *InformationWeek*. At that time, we weren't at all sure what the response would be or what value our participants and readers would derive from it. We learned quickly that the reaction was excellent. In 1997, Ernst & Young decided to continue this project under its own sponsorship. The effort has materialized into one of the longest-running annual surveys within the global information security arena.

We have come to realize that there will always be a need for the kind of information contained in this survey. After all, the effective protection of information assets is vitally important to global business. Surveys such as this one provide useful benchmark data that help participants understand how their own programs compare with industry peers—and to discern possible trends.

One thing is certain: good information security posture requires a multifaceted approach. Technology-oriented solutions and ensuring adequate inflow of investment are both important, but the people and organizational issues are equally important.

There is evidence that the human element is beginning to bubble to the top of executive consciousness—which is an encouraging development. This year's survey showed that the lack of user awareness was the number one obstacle to achieving a good information security posture. In our opinion, this bodes well if organizations act effectively to address training issues and if they give hiring, employee orientation, communication, and other human resource decisions the careful scrutiny they deserve.

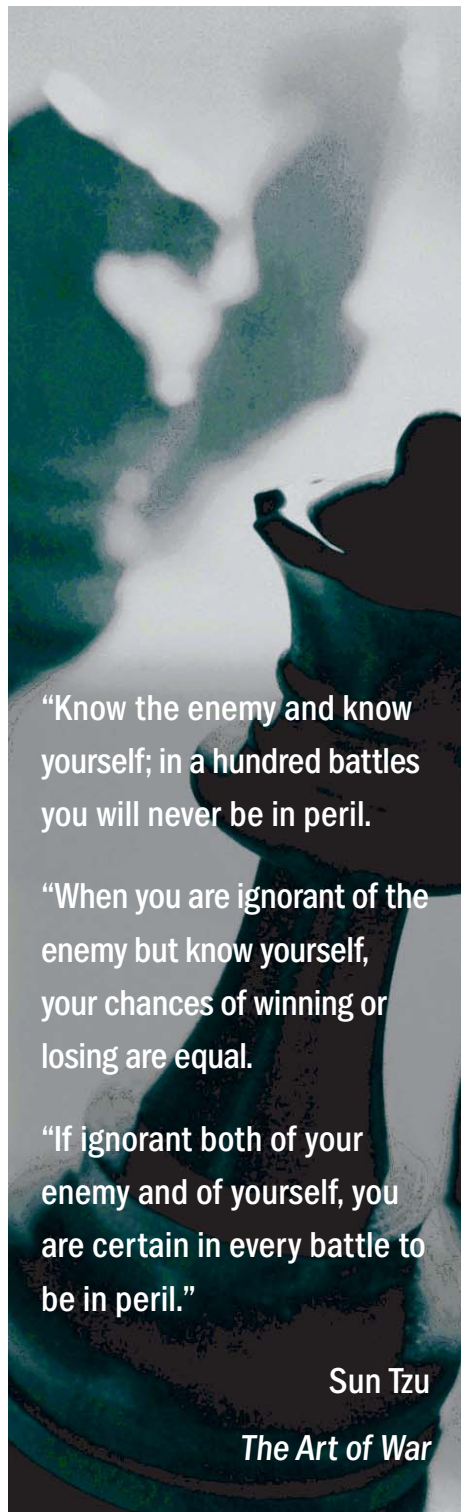
The indications are encouraging that this realization is gaining the attention it deserves in the executive suite. The survey does not, however, provide equally encouraging news that leaders are acting on it.

My personal thanks to all our survey participants for their valuable input and to all the Ernst & Young team for producing this year's survey and this report. We hope you find it useful in improving your own information security program.

A handwritten signature in black ink that reads "Edwin". The signature is fluid and cursive, with a long horizontal stroke at the end.

Edwin Bennett
Global Director
Technology & Security Risk Services

Executive Summary



“Know the enemy and know yourself; in a hundred battles you will never be in peril.

“When you are ignorant of the enemy but know yourself, your chances of winning or losing are equal.

“If ignorant both of your enemy and of yourself, you are certain in every battle to be in peril.”

Sun Tzu

The Art of War

Why is Sun Tzu's *The Art of War*, written approximately 27 centuries ago, relevant to an organization's efforts to effectively protect itself against information security threats?

If an organization followed Sun Tzu's key concept – that one needs to know itself as well as its enemy to remain successful – the resulting insight would enable it to focus its information security preparations on the credible threats rather than taking a reactive strategy. An organization's very survival requires that it knows enough to adapt itself to changes in the environment. Our survey results suggested that many organizations may neither know themselves nor their enemy as well as they should, resulting in a myopic approach to the rising number and variety of threats.

Since the release of our first survey in 1993, Ernst & Young has examined the various dimensions of information security as practiced by global organizations. Ironically, this year's survey seems to echo the sentiments of previous years, as organizations apparently continue to rely on luck rather than proven information security controls. Perhaps the remarkable thing is how *little* attitudes, practices, and actions have changed since 1993—during a period when threats have increased significantly. Two factors lead us to believe matters have deteriorated.

First, the threats are more lethal than they were in 1993. What many organizations are slow to recognize is that what they don't know is hurting them and hurting them badly. While scaremongers focus the public's attention upon the external threats with questionable damage guess-estimates, organizations face greater damage from insiders' misconduct, omissions, oversights, or an organizational culture that violates pre-existing policies and procedures. Because many insider incidents are based on concealment, organizations often are unaware they are being victimized.

Second, there is little visible change in how security is practiced in many organizations. In 1994, a respondent told us, “*It is apparently going to take a major breach of security before this organization gets its act together.*” Some 10 years later, that sentiment is still quite evident and still typifies organizations' reluctance to deal with the significant threats and to invoke well-accepted controls. What we found in 2004 is that too many organizations feel that information security has no value when there is no visible attack. Below are the issues that stand out:

KNOW YOURSELF

- **Tempting Fate** – As more organizations enter into close collaboration with other organizations, the less likely that senior management truly comprehends the organization's ever-growing risk interdependencies. This phenomenon has fundamentally changed the security landscape in which the behavior of a single organization

can have a wide-ranging impact on others in the extended enterprise. Unfortunately, senior management is more trusting than prudent. They may feel, wrongfully so, that their organization is adequately protected, when in reality their significant technology investments are undermined by any number of process flaws. For example:

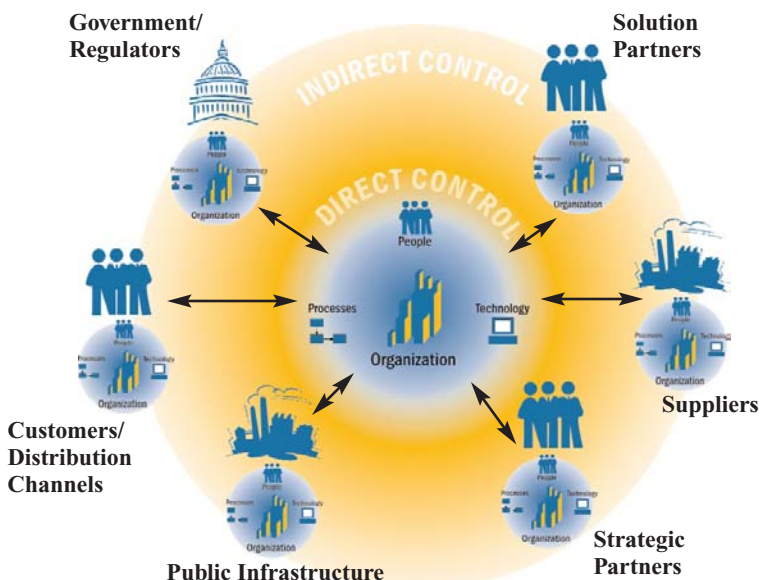
- 80 percent failed to conduct a regular assessment of their IT outsourcer’s compliance with the host organization’s information security regulatory requirements
- 70 percent failed to conduct a regular assessment of their IT outsourcer’s compliance with the host organization’s information security policies

- **Human dimension is neglected** – The common thread between this and past surveys is that the human aspect of protecting information assets—the will to commit resources—is not reflected in outward actions. No amount of technology can reduce the human dimension. Senior management says that information security is important, but persistent gaps continue to exist in the amount of diligence and resources that are deployed to improve the degree of protection, particularly in security awareness and training. Based on our findings, we remain convinced that more could and should be done to develop people into an organization’s strongest layer of defense. What the survey said:
 - Management is hesitant to assign priority to human capital but will readily commit to technology purchases
 - Less than half provide their employees with ongoing training in security and controls

KNOW YOUR ENEMY

- **Internal threats underemphasized** – While many respondents appeared fixated on external threats such as viruses, the more likely and most lethal threats are those originating from within an organization’s growing extended enterprise. The fact that internal incidents don’t garner media scrutiny isn’t because they don’t happen. On the contrary, they simply are either discovered but not made public or, even worse, undetected. Survey findings:
 - “Employee misconduct involving information systems” cited as a *distant* second behind “major virus, Trojan horse or Internet worms,” the top threat to organizations
 - Less than 30 percent listed “raising employee information security training/awareness” as a top initiative in 2004
- **Culture and governance are instrumental** – We expect that incidents—particularly internal ones—will proliferate unless senior management makes information security a core management and governance function—a cultural imperative. No single activity in information security is more important than setting the tone at the top, which drives behavior. Done well, it adds to the organization’s resilience. Done poorly, it invites disaster from the smallest of incidents. The current realities:
 - Close to 70 percent of the respondents’ board of directors failed to receive a quarterly report about the organization’s information security status
 - No more than 20 percent strongly agreed that their organizations perceive information security as a CEO-level priority

In studying the responses to our survey questions, it appears that quite a few organizations aren’t “doing security right.” It is a combination of a failure to invest and a failure to enforce. The number of unaddressed security areas suggests that many organizations should not feel comfortable and secure, since they neither know themselves nor their enemies very well.



In the extended enterprise, the actual functional effectiveness of information security naturally gravitates to the lowest level achieved by anyone in the network. If one trading partner has a poor identity management program, another never tests its disaster recovery plan, and a third does not regularly assess its IT outsourcers’ compliance with information security policies, one’s own security posture cannot logically rise above the lowest point achieved by these other entities.

Methodology

To ensure that the survey met the highest quality standards, we asked the Ernst & Young Quantitative Economics and Statistics (QUEST) Survey Team to assist us in designing and implementing the questionnaire. Established in 1994, QUEST has been engaged by numerous entities to tackle difficult economic, policy, and quantitative issues. The QUEST Survey Team has used its skills to implement and analyze surveys for numerous large corporations and organizations.

After a review of the survey questions for bias and ambiguity, QUEST distributed the survey to designated Ernst & Young professionals in each country. Since most survey results were gleaned from actual interviews, QUEST included a guideline sheet created to help minimize possible interviewer bias.

During February through June 2004, we conducted face-to-face interviews using a structured questionnaire with chosen respondents, usually chief information officers (CIOs) and chief information security officers (CISOs).

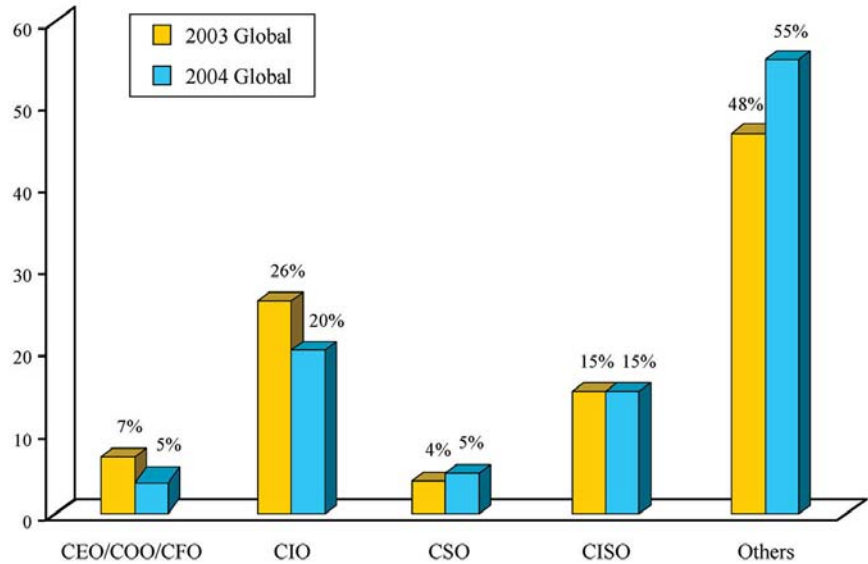
In those cases where a face-to-face interview was not possible, the survey was delivered electronically. More than 1,230 organizations participated in the survey. Among them were some of the largest and best companies in the 51 countries that were represented.

In giving a historical context, we have referred to Ernst & Young and Ernst & Young/*InformationWeek* information security surveys carried out as far back as 1993 to point out trends and illustrate findings that have not changed dramatically over the year.

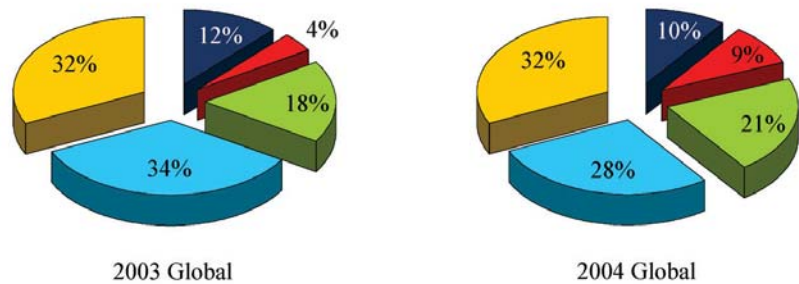
Please note that some graphs contained in this document do not add up to 100% due to rounding. All information is based on the 2004 survey unless otherwise noted.

Respondents

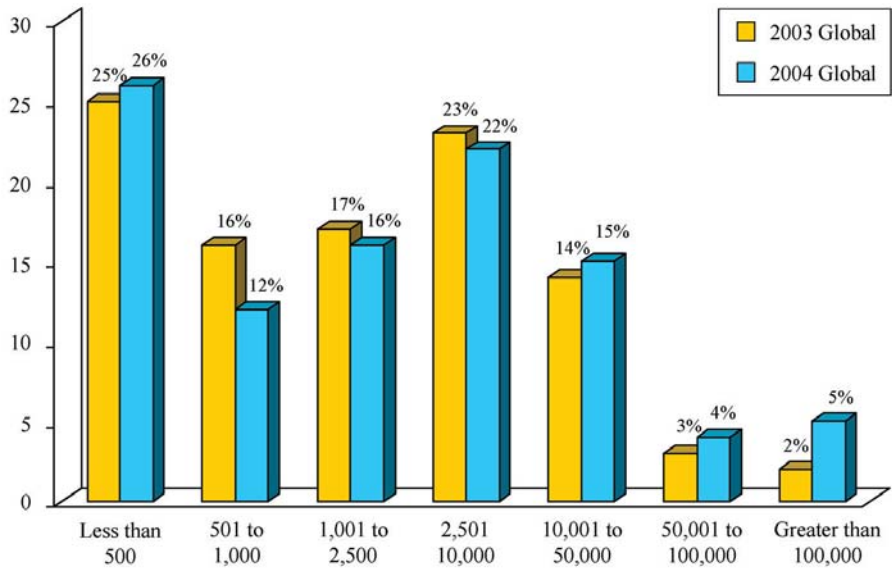
By Job Title



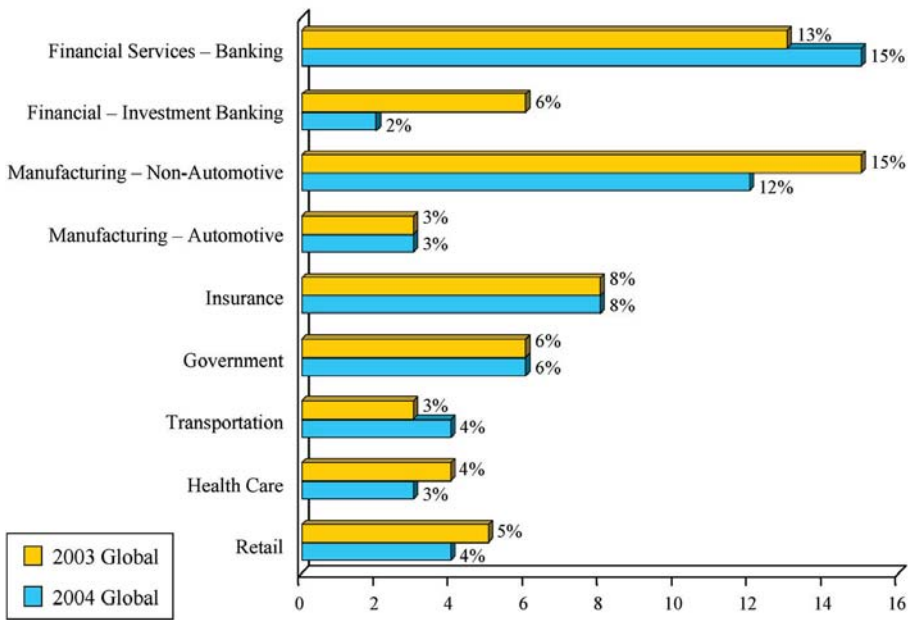
By Revenues



By Employee Population



Largest Representation by Industry



Ernst & Young

Ernst & Young, a global leader in professional services, is committed to restoring the public's trust in professional services firms and in the quality of financial reporting. Its 103,000 people in more than 140 countries around the globe pursue the highest levels of integrity, quality, and professionalism to provide clients with solutions based on financial, transactional, and risk-management knowledge in Ernst & Young's core services of audit, tax, and transaction advisory services. Ernst & Young practices also provide legal services in some parts of the world where permitted. Further information about Ernst & Young and its approach to a variety of business issues can be found at www.ey.com/perspectives. Ernst & Young refers to all the members of the global Ernst & Young organization.



Security Starts at the Top

No one expects organizations to achieve 100% security. Ultimately, information security is a human enterprise, as demonstrated by respondents citing “lack of security awareness by users” as the top obstacle to effective information security. However, no amount of technology can reduce the overriding impact of human complexities, inconsistencies, and peculiarities. Any strategy that overlooks this realization is inherently flawed. With proper training and education, however, people can become the most effective layer in an organization’s defense-in-depth strategy. The first step is making sure they operate in a security-conscious culture.

There is no factor more influential than senior management setting the tone that information security is important and that individuals—including senior and middle management—will be held accountable for their actions. Senior management must develop an appreciation for the capabilities and limitations of information security. If senior management doesn’t believe in it, why should anyone else follow it?

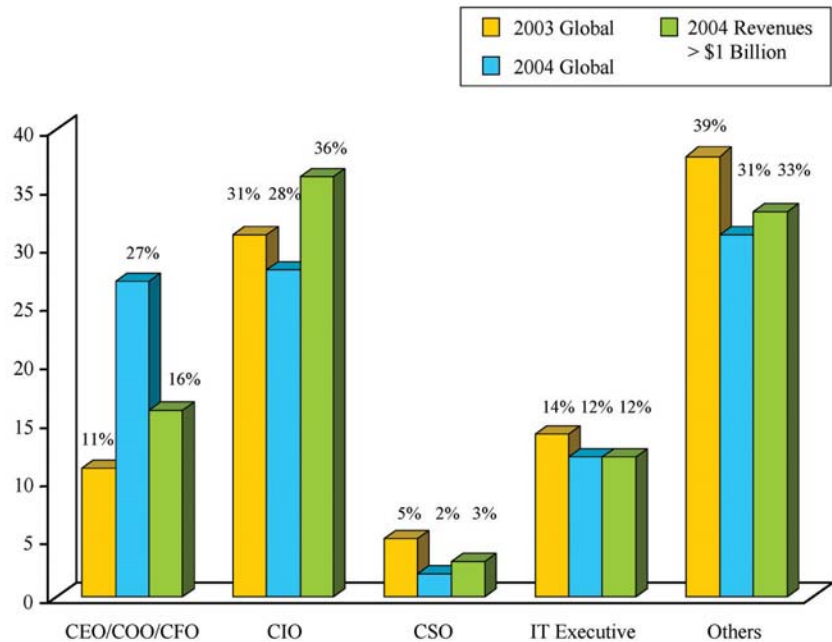
Although setting the tone, by itself, will not repel a single external or internal attack, the controls that can safeguard an organization are made dramatically more effective with senior management’s support. With that support, the countless activities an organization must perform take on purpose and direction and add to an organization’s strength. Lack of top management support invites weakness—even against weaker threats.

Although perception does not equal reality, survey results suggested strongly that when senior management has a strong belief in the value of information security, the measures taken by that organization are more effective or, at least, confidence in them is high. When we sorted the results to focus on those who declared information security to be very important to achieving organizational goals and objectives, we found an even higher

Organizational Factors

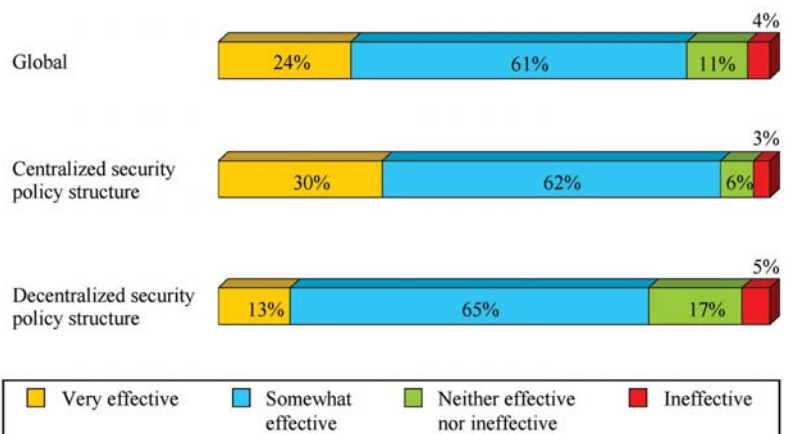
Locating the Information Security Department

Q. To whom does your organization’s information security department report?



Information Security Organization Effectiveness

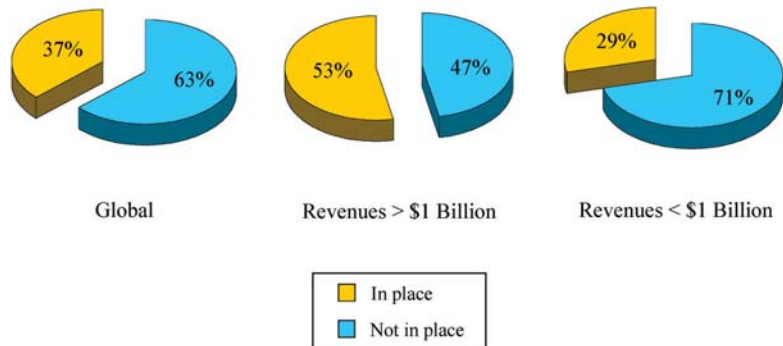
Q. How effective is your information security department in meeting the needs of the organization?



Please note that those organizations that responded “Very effective” above are denoted throughout the remainder of the survey as “Confident Respondents.” Those that responded “Neither effective nor ineffective” or “Ineffective” are denoted throughout the remainder of the survey as “Unconfident Respondents.”

Organizations With a CISO

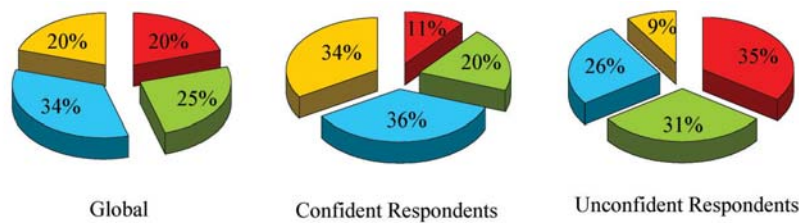
Percentage of respondents stating that their organizations employ a CISO.



Tone at the Top Cascades Down

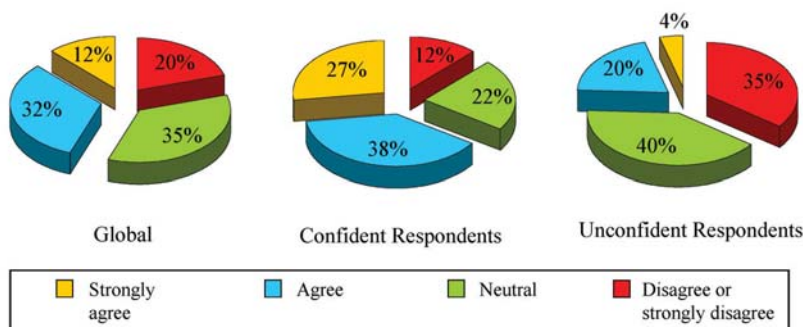
Organizations with high self-assessments evidence the importance of setting the tone for responsible information security from the top echelons ...

Percentage of respondents that agreed information security is a CEO-level priority.



and then cascading this through the entire organization right down to the front-line manager.

Percentage of respondents that agreed business unit leaders appreciate the value of information security.



level of agreement than the global benchmark had regarding information security's overall value and the priority assigned to it by the CEO.

On the other hand, where survey results indicated that senior management was unresponsive, all concerned tend to ignore controls or, even worse, circumvent them in the name of expediency — to the detriment of the organization. When we isolated the responses of those who rated information security as less important to achieving organizational goals and objectives, the percentages that agreed or strongly agreed that they were confident in the effectiveness of their information security departments diminished significantly. Without this important “tone at the top,” security policies become unenforceable and behaviors are unlikely to change. In light of the survey finding that a mere 20% of respondents strongly agreed that information security was a CEO-level priority in their organizations, we found it encouraging that survey respondents named “enforcing information security policy” as the top-rated initiative in 2004.

To meet stakeholders' ever-demanding expectations for managing risks effectively, senior management's perceptions about information security must change. They must lead the charge in creating a security-conscious culture based on individual awareness and personal accountability for conduct. Creating such a culture is a challenge, but it can happen with those in the top jobs walking the talk. We sense that if organizations fail to make information security part of their corporate culture, additional government involvement might be forthcoming.

Awareness Counters Indifference

Comparing our 2004 survey results with those of years past, we found that many organizations are still indifferent to information security. One needs to look no further than the frequency with which organizations reported to their boards of directors about security status and incidents. Conventional wisdom says that the average individual is not instinctively aware that security is something to be concerned about as he or she goes about daily routines. The 2004 survey revealed that in four out of six levels of frequency of making reports to the board of directors, organizations actually reported a lower frequency of communication with their boards than in 2003.

These findings are not a good sign and reflect that a great deal of work is needed to transform information security into an issue that gets equal status with other major concerns in the boardroom. If anything, the complexity of today's organizations produces challenges that call for increased awareness of information security issues—not less. Any number of risks or failures can accumulate to expose an organization to a major business disruption and both financial and reputational losses.

To provide effective information security, organizations must have a clear focus on what they seek to protect and the corresponding threats. Experience shows it is easier to protect against a threat that senior management can understand, even partially, than to counter one that is an enigma. Awareness based on investigating and understanding the unique characteristics of many threats is a far better basis for decisions and actions than relying on preconceived notions, generalizations, or media hype of a particular threat that has recently been in the news.

So, how does an organization gain awareness? The key is communicating with the entire organization regarding the threats that exist and the countermeasures that are available. Information security places a heavy emphasis on the judgment of

Organizational Pers

Information Security Value

Q. How important is information security for achieving your organization's overall business goals and objectives?

	Very Important	Somewhat Important	Neither Important or Unimportant	Unimportant
2003 Global	56%	34%	6%	5%
2004 Global	67%	26%	4%	3%
Financial Services	78%	20%	2%	1%
Manufacturing	52%	38%	8%	2%
Confident Respondents	85%	12%	2%	1%
Unconfident Respondents	41%	44%	11%	4%

Building Board Level Situational Awareness

Q. How often is your board of directors or equivalent provided a report on information security status or security incidents?

	Monthly	Quarterly	Semi-Annually	Annually	Ad Hoc	Never
2003 Global	15%	21%	12%	19%	19%	14%
2004 Global	15%	16%	8%	10%	39%	11%
Financial Services	21%	24%	6%	8%	36%	6%
Manufacturing	5%	10%	9%	14%	46%	16%
Confident Respondents	22%	19%	10%	8%	34%	7%
Unconfident Respondents	16%	10%	9%	8%	44%	13%

pective

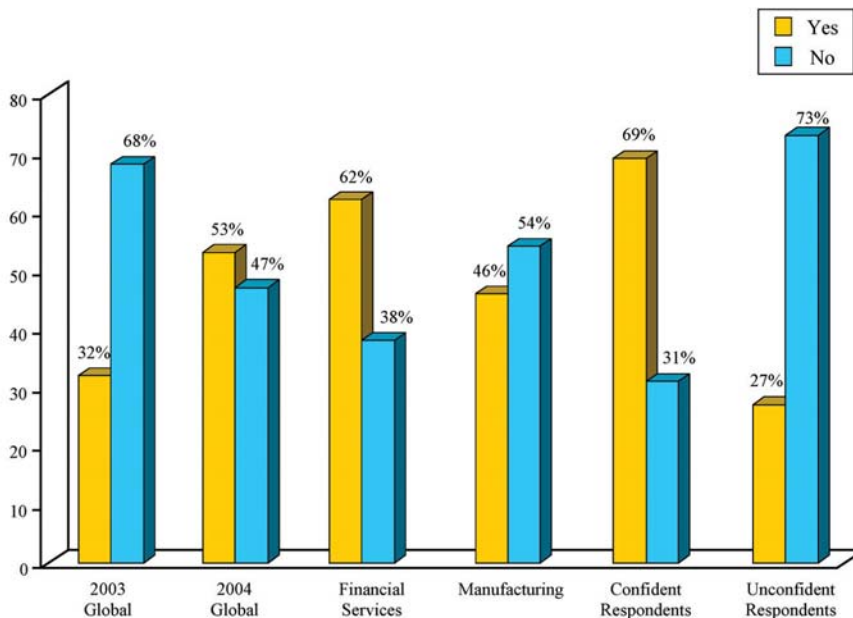
More Collaboration Yields Better Security

Q. How often do information security individuals meet with business unit leaders to understand their business objectives and information security needs?

	Monthly	Quarterly	Semi-Annually	Annually	Ad Hoc	Never
2003 Global	25%	20%	13%	13%	22%	7%
2004 Global	27%	23%	15%	11%	18%	6%
Financial Services	32%	26%	14%	10%	15%	3%
Manufacturing	15%	26%	15%	17%	18%	10%
Confident Respondents	40%	27%	14%	8%	8%	2%
Unconfident Respondents	15%	9%	16%	13%	28%	19%

Reinforcing User Security Awareness

Percentage of information security organizations that communicate with their user population on a regular basis.



individuals at all levels—particularly middle management. However, uninformed judgment, even in the presence of genius or intuition, is no substitute for accurate and timely information about the threats that an organization faces. Awareness also helps ensure that individuals understand security risks and the importance of security in their daily functions.

The survey established clear benefits to those organizations that already make regular reports to their senior governing body or board on information security topics. Respondents who rated their information security departments as “very effective” tended to communicate more often, with 23% reporting to their boards monthly or more often—7 percentage points higher than the global benchmark. There is also a significant connection between organizations that rated their departments highly and the proportion of them that communicate frequently with system users.

Several years ago, many organizations lacked the incentive to discuss information security risks at the board level and typically underinvested time in information security matters. Today, that attitude is being forced to change. Laws that focus on financial reporting and data protection, such as the Sarbanes-Oxley Act and Health Insurance Portability and Accountability Act, are supplying senior management with the motivation to be more concerned about these critical issues. Trust begins with confidence and familiarity, but our survey findings leave us skeptical that many organizations have performed the due diligence that would merit trust in their controls. It is clear that, relatively soon, the legislative process at work in many countries will force information security to be placed under the same scrutiny that financial reporting and internal control issues have received.

Instinctive Security Behavior

In information security, the defender has an inherent disadvantage in having to be vigilant everywhere. On the other hand, the attacker only needs to identify one flaw among a multitude of vulnerabilities to be successful. To repel the attacker, the defender needs the support of the entire organization because overall security is only as strong as its weakest link. The recklessness or simple carelessness of a single employee can undermine even the best technological countermeasures. Many security breaches are simply the result of human negligence enabled by weak operational practices. So attackers invariably focus first on weaknesses based on people or processes.

The survey findings reveal a certain irony. Although respondents placed relatively low priority on people-based measures, organizations very typically depend on human involvement to prevent most security breaches—particularly internal incidents. The unpleasant reality is that good information security practices are not second nature to most employees. A case in point: how can one explain the number of individuals who open an e-mail from a complete stranger with an alluring subject line but containing a suspicious attachment?

Successful organizations understand that countermeasures work best when security technology and a management-based approach—the process controls—complement one another. By deploying a well-crafted, clear, and enforceable set of security policies, organizations provide clear guidance to users as to what is and is not allowed. On the surface, process controls are cheaper than their technological counterparts, and they also appear easier to implement. But the limitation is that controls are often difficult to enforce without the support of middle management. When enforcement is lax for a long period of time, the repairs and the consequences can be expensive.

Senior management's leadership is key to successful security, but middle management plays the critical role in

Process Adoption

Control environment practices are those that establish the tone of an organization, influencing the control-consciousness of its employees	Percent Practicing	Effectiveness (Mean values reported on five-point scale)
Security policies have been communicated	83%	3.28
Control practices are introduced as new technology is adopted	80%	3.46
Security policies and procedures are reviewed and revised on a regular basis	79%	3.52
A high level information security officer has been appointed	48%	3.74

Risk assessment practices allow an organization to consider how potential events might affect the achievement of objectives	Percent Practicing	Effectiveness (Mean values reported on five-point scale)
Threats that could harm and adversely affect critical operations have been identified	85%	3.52
Controls have been defined that provide sufficient protection against threats	84%	3.47
Systems that are critical to the organization have been identified, and preparations have been made to operate without them in the event of disruption	83%	3.55
Sensitive or confidential information has been identified	77%	3.58
Functions and assets are identified and ranked by their value, sensitivity, and criticality of effect should a threat materialize	57%	3.46

“Percent Practicing” signifies which of the specific controls the respondents employed.

“Effectiveness” indicates how effective the specific control was in improving the respondents’ information security posture or in reducing data protection risks. Respondents were given a sliding scale where 1 denoted very low effectiveness and 5 denoted very high effectiveness.

Control activities are the policies and procedures that help ensure risk reduction measures are properly executed	Percent Practicing	Effectiveness (Mean values reported on five-point scale)
A unique user account has been established for each individual authorized to use the system	94%	4.18
Each user is limited to accessing only the information they need to perform their job duties	93%	3.92
Users are required to change passwords on a regular basis	88%	3.98
Unauthorized use of user accounts is enforced by passwords that are difficult to guess	83%	3.71
Help desk assistance requires positive identification before resetting/changing user password or providing other services	78%	3.89

Monitoring practices help an organization to measure both the presence and functioning of its components and the quality of their performance over time	Percent Practicing	Effectiveness (Mean values reported on five-point scale)
Security violations result in immediate response	81%	3.69
Sensitive actions are logged to assign responsibility	75%	3.59
The operation of the overall control structure is evaluated and adjusted to adapt to changing conditions	71%	3.42
Compliance with information security procedures is evaluated with periodic compliance reviews	61%	3.48

determining what employees will do and won’t do on a daily basis. Without this managerial endorsement, individuals will often ignore controls or, even worse, circumvent them. This puts the entire extended enterprise at great risk and possibly exposes the organization to liability. Without managerial coherence, accountability, awareness, and education, even well-articulated information security policies and plans become nearly worthless.

By vigorously enforcing its policies, an organization makes security the responsibility of everyone—not just its cadre of information security professionals. Controls should be as straightforward, clear, enforceable, and as instinctive as looking both ways before crossing the road.

We asked respondents several questions about their use of a number of commonly invoked security procedures, as recommended by the Committee of Sponsoring Organizations of the Treadway Commission (COSO).

While many organizations report a high adoption rate of best practices, we believe that survey respondents report more action taken than is actually the case. Some high adoption rates reported in the survey contrast with our engagement experience, particularly with identifying risks; defining controls to provide sufficient protection; and testing solution or service providers. For example, 93% of respondents claim that users are limited to accessing only the information they need to perform job duties, which does not square with what we find in our client work.

Although security is dynamic and requires routine updates to remain effective—especially when new technology is introduced—our survey found that 39% failed to periodically review their security policies for compliance.

Low occurrences of monitoring practices are cause for concern. Nearly 20% do not respond in an expeditious way to security violations. Nearly 30% said they do not evaluate and adjust the operation of control structure in response to changing conditions.

No Better Defense

With people as important as they are for an adequate and appropriate level of security, we expected our survey to show more and better attention paid to awareness and training than it did. Surprisingly, respondents' stated actions show that persistent shortfalls continue to exist in the amount of diligence, human capital, and other resources that are deployed—particularly in educational initiatives. We found that barely half the respondents have deployed a training and awareness program—a fundamental component of an effective information security strategy.

Logically, it is hard for employees to be aware of occupational fraud activities unless they are provided with information on what the indicators are, as well as how to alert the proper authorities when they appear. This is borne out by respondents citing “lack of security awareness by users” as the top barrier to achieving the required level of security. For instance, security technology is defenseless against individuals doing the “wrong thing” that their job descriptions allow them to do. Experience shows that the most effective methods of detection are by a tip or accident rather than through other means such as formal internal controls.

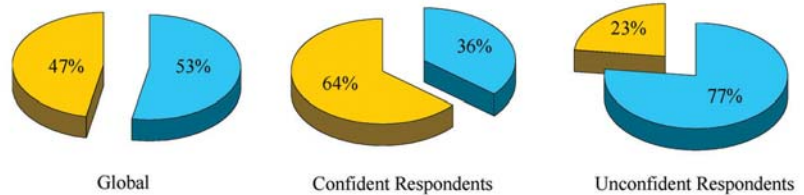
Among global respondents, only 56% said they train system users to identify and report suspicious activities. Even more telling is that among even the most confident organizations, only 70% did so. And among the same group, less than two-thirds give employees continuous training in security and controls.

Therefore, an organization could increase its level of protection significantly with cost-effective awareness and training initiatives. If people are typically considered the weakest link in an organization's attempt to secure its systems and networks, then it follows that the linkages become weaker as more people become involved. Based on our findings, we believe that more could and should be done to transform an organization's weakest link—people—into its strongest and most effective layer of defense-in-depth.

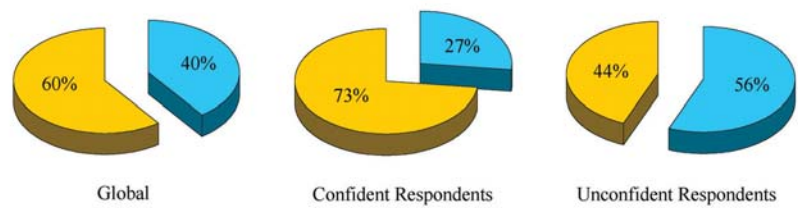
Human Dimension

Are You Building a Security-Conscious Culture?

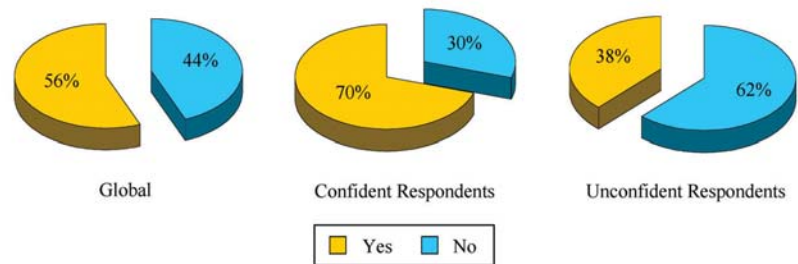
Employees get continuous training in security and controls



Users are provided with instructions on classifying data (e.g., confidential)



System users are trained to identify and report suspicious activities



Information Security Priorities in 2004

Failure to invest in people and process improvements puts an organization at great risk because information security is as much a *human issue* as it is a technology issue. Information below is based on specific respondents' ranking out of 16 initiatives.

Note: Multiple responses allowed

	Enforcing information security policy	Raising employee awareness/training	Improving data privacy
CEO/COO/CFO	1st	6th	10th
CIO/CTO/IT Executive	2nd	8th	9th
CISO/CSO/IS Executive	2nd	6th	10th

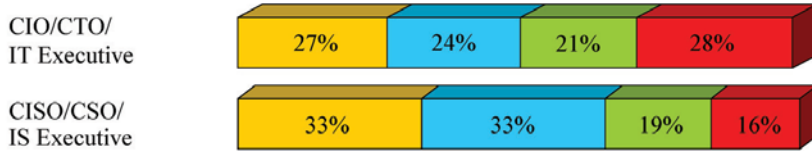
The Enemy Within

Respondents' level of concern about the following security issues in their organization over the next 12 months.

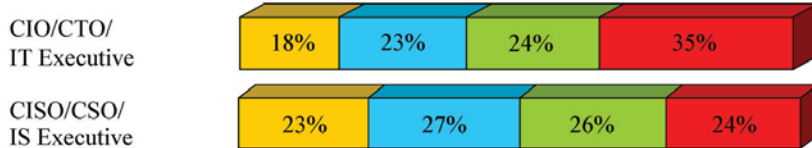
Employee misconduct involving information systems



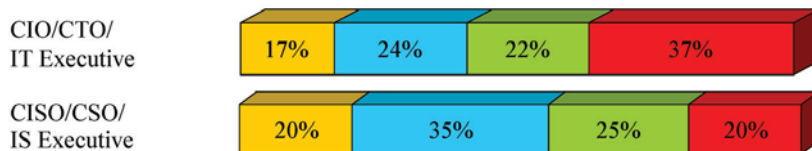
Loss of customer data privacy/confidentiality



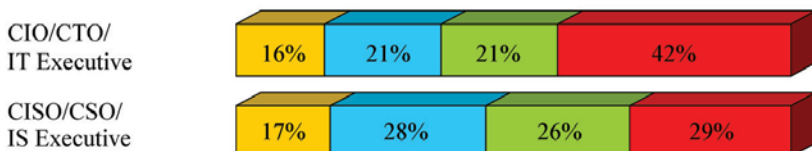
Financial fraud involving information systems



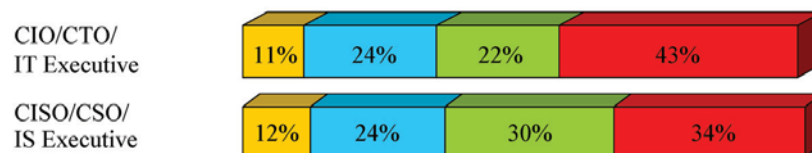
Misconduct involving third parties who have access to your information systems



Theft of proprietary information or intellectual property



Former employee misconduct involving information systems



No Worse Enemy

Respondents repeated their observation from the past years that they were more vulnerable to external attack than internal breaches. This was despite the ongoing confirmation of leading research groups that the more likely and most lethal threats are those originating from legitimate network users. These are the individuals—current, temporary, and former employees—who are already inside an organization's growing and heavily populated extended enterprise. As organizations allow more and deeper access to their information, their security risks increase exponentially with the number of individuals who can get access and view it.

Insiders can operate with limited risk of detection through their intimate knowledge of the system, its plausible access requirements, and the organization's controls. Typically, insiders' motives are for personal gain, but they can launch malicious attacks, too. Insiders can become the enemy through carelessness or pure ignorance that undermines even the best controls or technologies. Survey respondents correctly identified insiders as the second highest rated threat—yet they seemed to underprovide for it.

So, how real is the threat? Although there is no explicit reporting on insider-perpetrated losses, the Association of Certified Fraud Examiners (ACFE) estimates that the typical U.S. organization loses 6% of its annual revenues to fraud. When placed in context with the U.S. Gross Domestic Product for 2003, this amounts to roughly \$660 billion in total losses.

Fraud affects practically every organization regardless of geographic region, industry, or size and generally goes undetected. In Ernst & Young's latest study of fraud, one in five employees reported personal awareness of other individuals stealing from the employer. Logically, as organizations become larger and more complex, the opportunities for fraud increase and the rate of detection becomes lower. To that end, how many break-ins and resulting losses are going undetected? Right now, many organizations would have to admit they just don't know.

Countering the Threats

What do organizations perceive as their most pressing threats and how rationally are they addressing them? To provide effective information security, an organization must have a firm focus on what it wants to protect and where it is most vulnerable. Once it has this understanding, it can take appropriate actions that make the most effective use of its resources.

The survey showed, in some cases, that organizations are reinforcing already-implemented controls devoted to areas of high urgency. However, in other cases, the survey also provides ample evidence that organizations could be misallocating resources to some less-than-effective controls, and underemphasizing other higher-value initiatives.

For example, respondents consistently cited major viruses as well as unsolicited commercial bulk mail—primarily spam—among their top three concerns. However, oddly, these are also the areas where most, if not all, respondents have protection in place—100% have anti-virus systems, and 71% have specific anti-spam protection for their networks. On the other hand, most organizations undermine these protections by failing to educate their employees so they will avoid opening dubious attachments to their e-mail messages.

Why this myopic behavior? We suspect that some respondents are influenced by either media or vendor dramatizations that escalate interest in viruses and worms instead of focusing their attention on the most lethal threat—the insider.

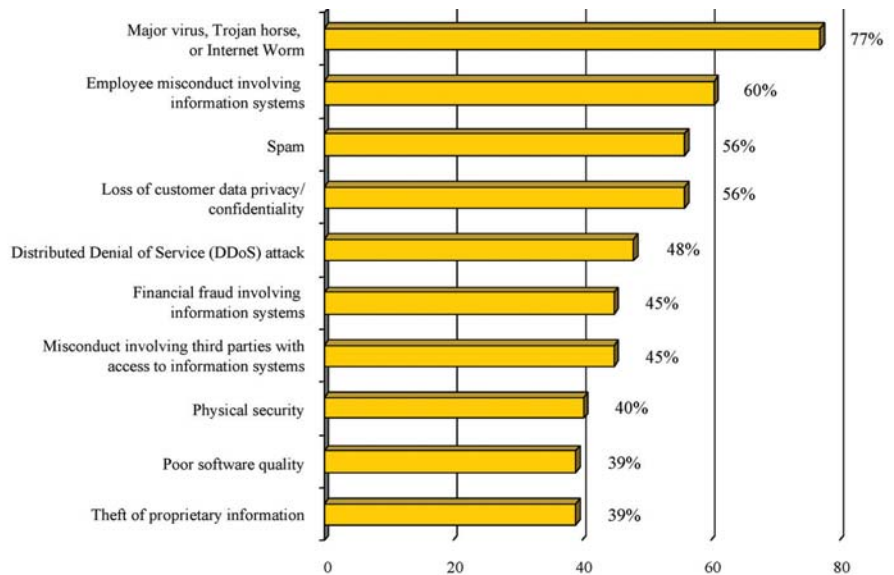
Organizations' reluctance to admit when they have been victimized by an insider's actions may be motivated by the sense of security they and others falsely receive that the threat isn't so widespread. Unfortunately, and with uncertain economic times, the opportunity for personal gain provides ample motivation for fraud, so the threat is real.

The non-technical and human-behavior-based forms of intrusion that can occur are common. What makes the insider threat so prevalent is that most breaches

Organizations' Security

Threat Matrix: Top Ten Security Concerns

Percentage of respondents that indicated a high level of concern with the following information security-related issues and challenges to their organization over the next twelve (12) months.



Loss of Availability: Top Ten Incidents

Percentage of respondents that indicated the following incidents resulted in an **unexpected** or **unscheduled** outage of their critical business systems in 2003.

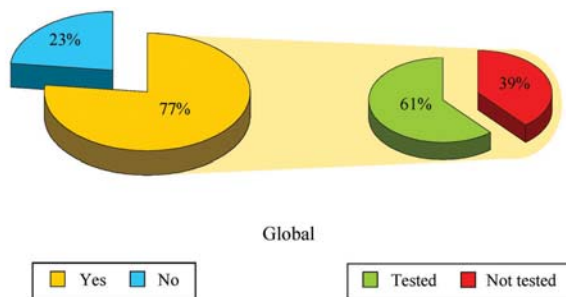
Note: Multiple responses allowed.

Incident	Occurrence	Origination		
		Internal	External	Unknown
Hardware failure	72%	87%	9%	4%
Major virus, Trojan horse, or Internet worms	68%	21%	76%	3%
Telecommunications failure	64%	26%	72%	2%
Software failure	57%	78%	16%	6%
Third party failure, e.g., service provider	47%	9%	87%	4%
System capacity issues	46%	91%	6%	3%
Operational errors, e.g., wrong software loaded	42%	91%	6%	3%
Infrastructure failure, e.g., fire, blackout	42%	49%	49%	2%
Former or current employee misconduct	24%	84%	12%	4%
Distributed Denial of Service (DDoS) attacks	23%	10%	85%	5%

Security Concerns

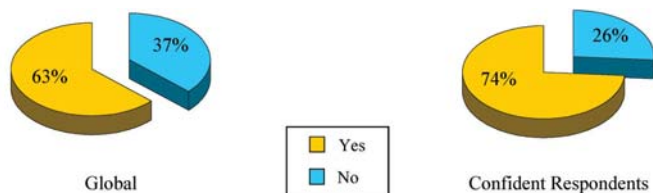
Incident Response Plans

Percentage that have an incident response plan.



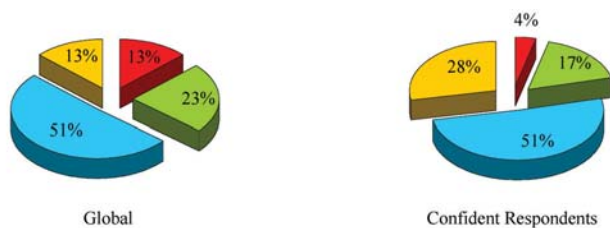
Vulnerability and Penetration Assessments

Percentage that have vulnerability and penetration assessments conducted on a regular basis.

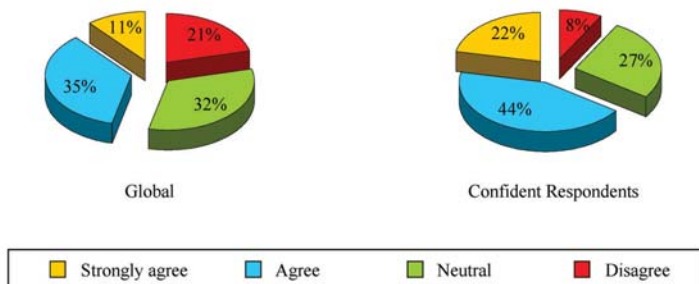


External Attack Vulnerability

Percentage that agree that their level of protection is adequate to defend against external attacks.



Percentage that agree that their foreign operation's level of protection is adequate to defend against external attacks.



use unsophisticated methods to gain access, and occur during normal working hours at the organization's location. In other cases, disgruntled employees may simply want to cause damage to an organization and its reputation. It is common for organizations to fail to revoke access on a timely basis, so that former employees—including contractors and temporary employees—may still maintain their network credentials for more than two weeks after they leave.

Despite the security measures they have taken, a majority of the survey respondents had experienced incidents in 2003 related to hardware or software failure that brought down critical business systems. Obviously, security does not come free and organizations must be willing to pay the costs for better quality products. They must also demand that technology vendors conduct more rigorous testing for vulnerabilities before releasing their products rather than allowing end-users to serve as implicit beta testers to locate the flaws on their own.

Although many organizations have a business continuity plan, the survey suggests few have adequately tested it beyond a tabletop exercise. With so many interdependencies in the enterprise, we recommend that an organization regularly put its plan into actual motion to observe how it would work if needed. Past experience demonstrates that most plans never survive contact with reality. Of course, the alternative to not testing is that the plan will likely get its first scrutiny in the aftermath of a disruption to operations.

Unexpected downtime has serious consequences. As the survey showed, organizations built on shaky foundations will incur downtime more often than others. Despite the apparent preference that most organizations have to conceal important security incidents from outsiders, that downtime is more likely to become public information, and it can tarnish an organization's reputation.

Creating the Incentive

Several leading security researchers such as Ross Anderson of Cambridge University's Computer Laboratory theorize that information security is so poorly practiced because the liability is so dispersed. In other words, the organization best situated to reduce the risks has insufficient motives to do so because it perceives that the liability due to failure will be borne by others. If this entity did bear more liability for the damages to others, then presumably it would have a strong incentive to deploy sufficient controls. Some predict that the entities will eventually file, for example, product-liability actions against software companies to ensure that the party best situated to reduce the risks did, in fact, carry the liability for the failure of that protection.

We know from our observations and interviews that organizations don't act without the appropriate incentives. They often need some convincing that reducing risk by improving information security is worth the investment because the measure of value is elusive and the benefit is visible only through events that do not happen. Consequently, many organizations invest the minimum necessary to protect themselves. The result: a decrease in the overall security level for everyone on the network.

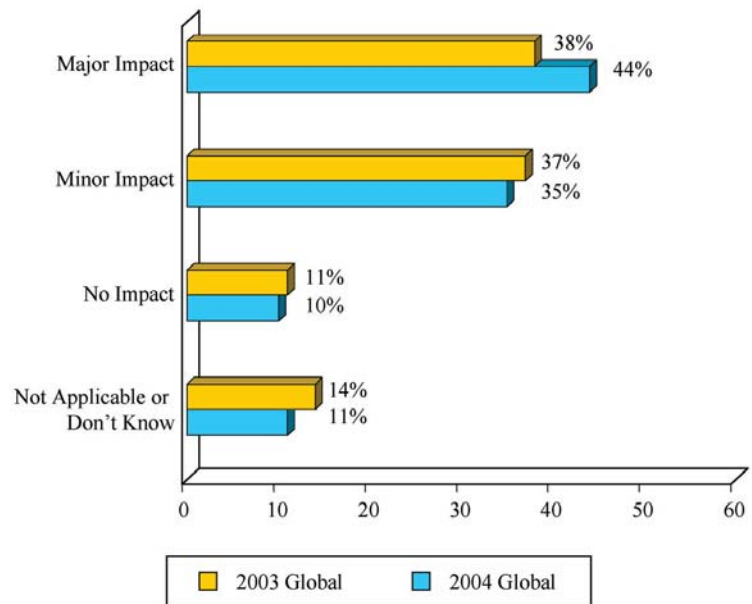
As the network is interdependent, a successful attack on one system is then likely to succeed on other systems as well since they typically share the same vulnerabilities via a common platform. This means that one organization's security is negatively affected by the poor security behavior of another member of the network.

In our interviews, several respondents openly acknowledged that they could never achieve 100% security on their own because their risks are often created by the behaviors of others who also lack the incentive to heighten security. Theoretically, it follows that an organization's "perverse incentives" not to invest drive others to underinvest as well. To deal with that, governments have enacted security-related laws to correct the perceived market imperfections and provide the incentive for organizations to

Regulatory Incentive

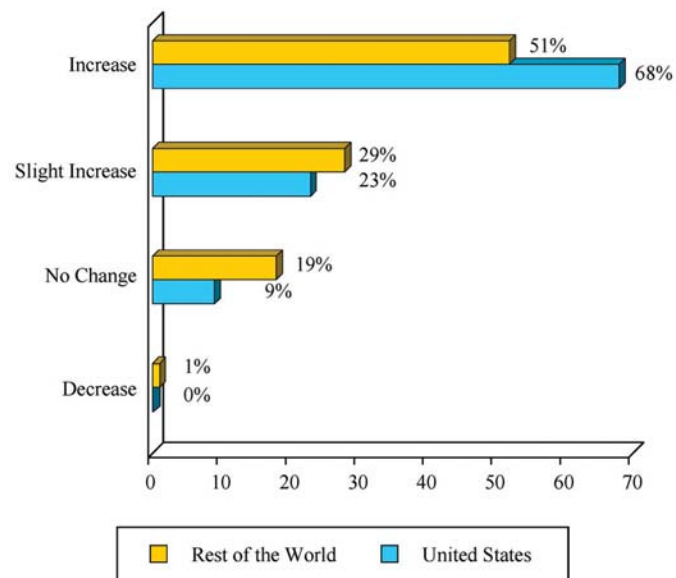
Regulatory Impact on Information Security

Q. To what extent are government security-driven regulations impacting your industry and organization?



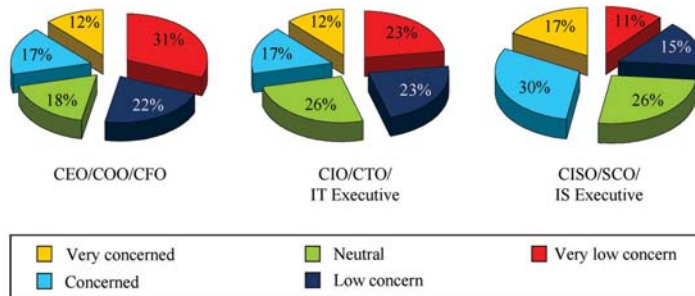
Compliance Effort Demands

Q. Do you expect your organization's time spent on information security-related regulatory matters to increase or decrease in 2004 as compared to 2003?



Regulatory Compliance Concerns

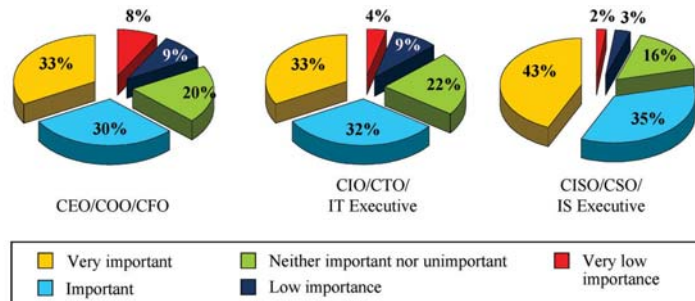
Percentage that indicated their level of concern with regulatory compliance-related issues and challenges in their organization over the next 12 months.



Note: Multiple responses allowed

Importance of Regulatory Compliance Initiatives

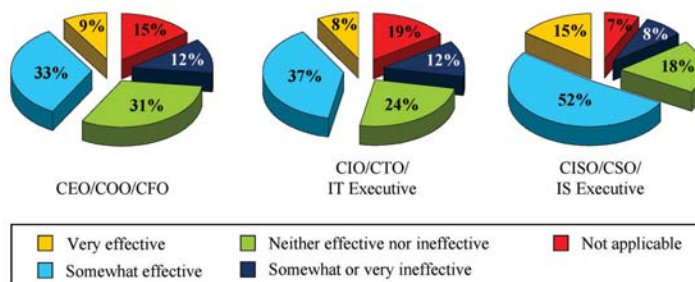
Percentage indicating the level of importance of regulatory compliance initiatives at their organization in 2004.



Note: Multiple responses allowed

Information Security Regulation Effectiveness

Q. How effective are government security-driven regulations in improving information security posture or in reducing data protection risks in your industry and in your organization?



align their investments with societal goals such as safeguarding privacy or preserving economic viability.

Broadly speaking, government intervention only provides a minimum guarantee to the extent the regulation is monitored and enforced. The survey told us that organizations are being affected, with almost 75% acknowledging that these regulations are impacting them. Unfortunately, less than 25% believe that these regulations are very effective in improving information security posture or in reducing data protection risks.

We expect information security-related regulations to expand their sphere of influence—holding organizations to a higher level of accountability for their information security. Eventually, these regulations will prompt organizations to integrate their concerns and action plans dealing with information security and financial reporting controls into the same overall thought process—and with the same heightened level of urgency.

Survey respondents who said they are not very concerned about regulatory compliance may have this attitude because they are not aware of the regulations themselves, or of the potentially large risks in not complying with them. For some, we believe that rigorous monitoring and enforcement of regulations will correct this attitude. For others, exposure to liability within the court system should provide the incentive.

California has already enacted a law that requires any organization that possesses personal information of a California resident to disclose any breach of the security of that information.

Spending Magnets

In our earlier surveys, few organizations told us they were investing aggressively in information security. Most spending was tactical or reactive. More recently, the onslaught of government regulations has stimulated organizations to invest in securing their systems. Our survey confirms an upward spending trend, as organizations devote more energy and resources to comply with regulations—and expect these investments to rise in the future.

Invariably, organizations will wonder whether they are spending too little or too much. This analysis is only half of the picture. The other half is looking at what kind of resources are being purchased. We believe that many organizations could ultimately discover that they spend less by diverting more resources to people and organizational issues. For example, we feel organizations should expend more effort and resources to create a security-conscious culture that includes setting the tone at the top. The other major magnet for spending, we believe, should be correcting the shortcomings in monitoring the organization's extended enterprise.

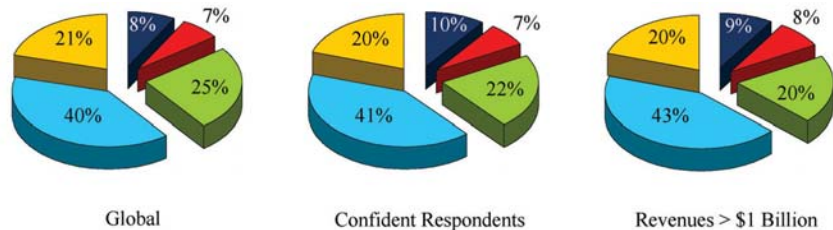
Some organizations appear too focused on the external threats. Viruses, for instance, do constitute a real risk, but our findings suggest that organizations are fairly well-prepared with anti-virus countermeasures. The rapid spread of malicious code can cause significant damage, but even the best technology is worthless if one employee decides to ignore a control. To quote one of the many corollaries to Murphy's Law, "It is impossible to make anything foolproof because fools are so ingenious."

In our 2003 survey summary, we concluded that too much money was being spent on technological tools while too little was directed to organizational and people issues. In 2004, we believe this is more true than ever.

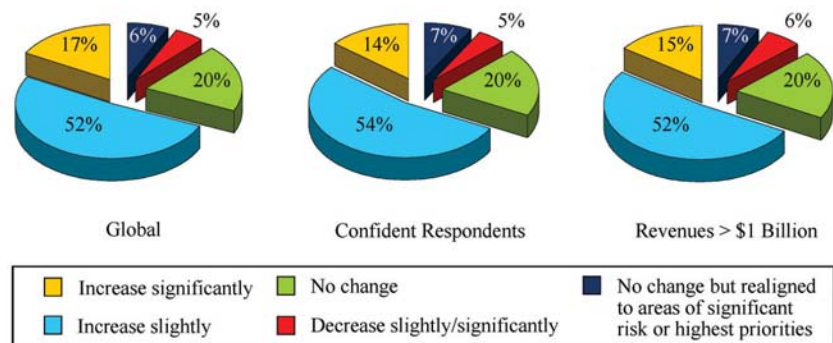
Budget & Initiatives

Information Security Spending

Compared to 2003, your organization's spending in 2004 will ...

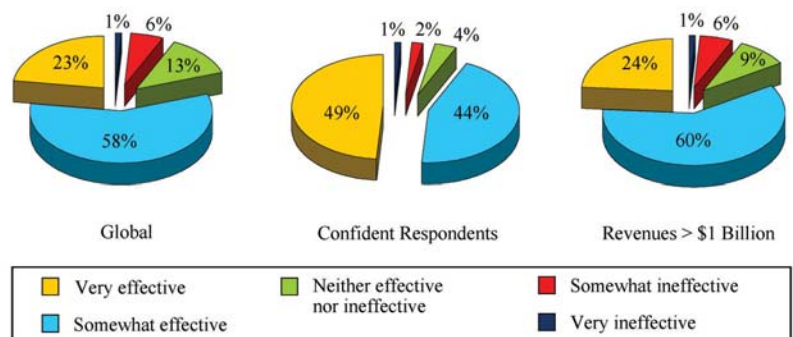


Compared to 2004, your organization's spending in 2005 will ...



Information Security Spending Effectiveness

Q. How would you characterize your organization's spending on information security threats?



Top Five Initiatives in 2004

Global	Revenues > \$1 Billion	Financial Services	Health Care	Manufacturing
1. Enforcing information security policy	Enforcing information security policy	Complying with information security-related regulatory requirements	Enhancing IT disaster recovery program	Improving network security
2. Enhancing IT disaster recovery program	Aligning security strategy with business goals and objectives	Enhancing IT disaster recovery program	Enforcing information security policy	Enforcing information security policy
3. Improving network security	Complying with information security-related regulatory requirements	Enforcing information security policy	Aligning security strategy with business goals and objectives	Enhancing IT disaster recovery program
4. Aligning security strategy with business goals and objectives	Standardizing info. security technology/policy/procedures	Enhancing business continuity program	Standardizing info. security technology/policy/procedures	Standardizing info. security technology/policy/procedures
5. Enhancing business continuity program	Enhancing IT disaster recovery program	Aligning security strategy with business goals and objectives	Raising employee information security training/awareness	Aligning security strategy with business goals and objectives

Top Obstacles to Effective Information Security

1994 Survey Results*	2003 Survey Results	2004 Survey Results
1. Lack of human resources	1. Budget constraints or limitations	1. Lack of security awareness by users
2. Budget constraints or limitations	2. Resource priorities	2. Budget constraints or limitations
3. Management awareness	3. Availability of skilled staff	3. Availability of skilled staff
4. Tools and solutions	4. Management commitment	4. Difficulty proving the value of information security
	5. Management awareness	5. Pace of information technology change

* Only four obstacles were designated for this year's survey results

Risk Interdependence

In today's environment, do organizations really know themselves as well as they should?

Advances in information technology and greater investor pressure for better financial performance have resulted in flatter, more decentralized, and far-flung organizations—more connected but more vulnerable. This dispersal, and having so many characters in the cast, comes at a cost: the more likely that senior management has lost its situational awareness and the less likely it truly comprehends the organization's ever-growing interdependencies. Single events can have profound impacts that cascade from one venue to another.

But an unsettling reality is that senior management frequently believes their organization is more resilient than their other survey responses suggest. Organizations generally have a lot of confidence in their infrastructures. A symptom of this is that management methodically blinds itself to risks and consequences of certain actions. Patterns emerge in which deviations from prescribed security practice become the norm. Or, instead, rules are changed rather than violated. Given these realities, deficiencies accumulate and take managers by surprise.

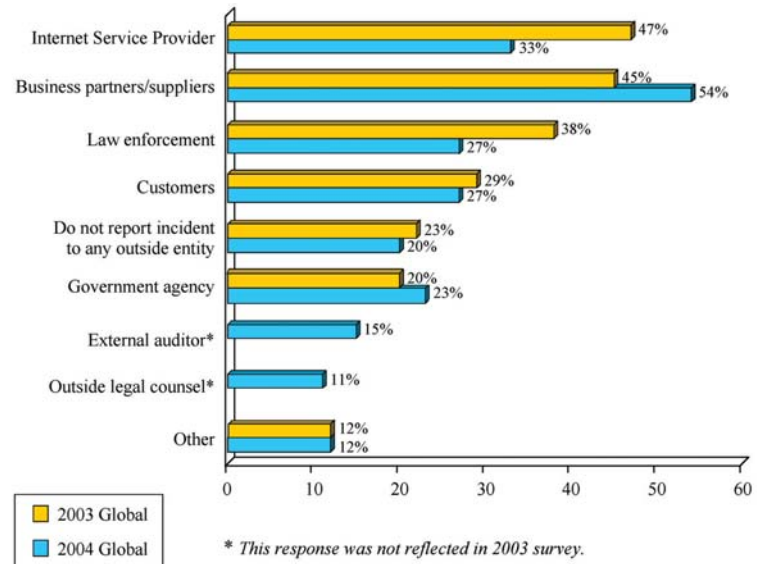
Our survey reveals that not only do many organizations pay insufficient attention to the full implications of their interconnectedness, but they lack the incentive to take into account the impact of their decisions—to invest or not invest—on others who are connected with them. Some of these impacts could be lethal to themselves and others in the enterprise because today's criminal can steal more with a keyboard than with a firearm.

Our surveys have demonstrated that a major share of organizations—when they have an incident—prefer not to disclose it for fear of a negative effect on their competitive stance, public image, and stock value. If an entity is networked with an enterprise that suffers an incident, its managers are just as likely not to know

Extended Enterprise

Information Security Incident Notification

Entities that would be contacted if organizations experienced an information security incident.



Organization Resilience

Percentage who gave the following entities their highest rating for the ability to continue operations in the event of a serious disruption.

	Global	Confident Respondents	Revenues > \$1 Billion
Own organization	10%	20%	8%
Foreign-based IT operation	14%	32%	12%
In country IT solution provider	12%	21%	12%
Foreign-based IT solution provider	13%	23%	8%

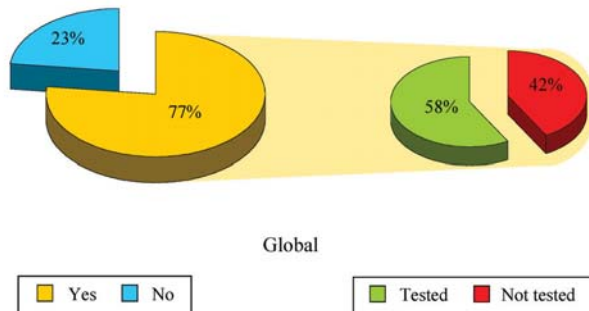
Percentage who gave the following entities their lowest two ratings for the ability to continue operations in the event of a serious disruption.

	Global	Confident Respondents	Revenues > \$1 Billion
Own organization	16%	8%	14%
Foreign-based IT operation	18%	8%	16%
In country IT solution provider	10%	7%	8%
Foreign-based IT solution provider	14%	14%	14%

Volatility

Business Continuity: Hope Is Not a Plan

Indicate whether your organization has a business continuity plan and has it been tested in the past 12 months.



External Compliance: Trust BUT Verify!

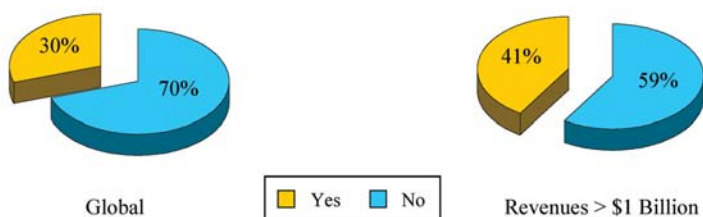
Organizations that outsourced information technology operation(s) to foreign-based solution providers:



Percentage that conduct a regular assessment of their IT outsourcer's compliance with the host organization's own information security regulatory requirements:



Percentage that conduct a regular assessment of their IT outsourcer's compliance with the host organization's own information security policies:



about it as they are to find out, because fewer than 55% of our respondents said they would notify their business partners about a problem.

Based on the survey's findings, many organizations continue to rely on trust or fate rather than accepted controls to secure their enterprises, even with the magnitude of threats to which the extended enterprise is exposed. Trust is a product of confidence and familiarity. From our standpoint, trust must be earned, and actions that undermine trust must be dealt with quickly and effectively. Unfortunately, 30% of organizations conduct a regular assessment of their IT outsourcers' compliance with information security policies. Fewer still, just 20%, conduct a regular assessment of these same service providers compliance with the organization's home country regulatory requirements.

How are organizations getting the confidence to know the real source of threats and that their security policies and procedures are being deployed effectively? Organizations can outsource a process, but they can't shed the responsibility of caring for the process—especially to protect against such costly events as a breach of consumer data confidentiality. Therefore, organizations must devote attention and resources to evaluate their partners' controls, vulnerabilities, and business continuity plans as they do their own.

As we have noted elsewhere, the existence of government regulations creates a culture of non-compliance when it is perceived that the regulated activity is not really monitored. For these regulatory initiatives to have a real beneficial effect, rigorous monitoring and enforcement will be essential. Each organization must work with its suppliers, business partners, customers, and solution providers to discover ways in which they can cooperate to develop fair and efficient standards for providing protection that works for everyone's mutual benefit.

Nuts and Bolts

Global	Yes	Maybe in 2004
Managed security services	60%	10%
Policy development	51%	17%
Vulnerability management services	50%	24%
Spam filtering services	50%	24%
Cyber-risk insurance	12%	10%
Anti-virus desktop/server software	99%	1%
Virtual private network	75%	11%
Spam filtering software	58%	25%
Intrusion detection systems	55%	21%
Information security audit tools	51%	22%
Public key infrastructure	29%	18%
Smart cards	19%	13%
Single sign-on	27%	22%
Cyber-certifications (e.g., WebTrust)	25%	13%
Wireless security products	24%	24%
Digital identity management software	22%	18%
Biometric systems	11%	10%

Health Services	Yes	Maybe in 2004
Managed security services	55%	11%
Policy development	56%	16%
Vulnerability management services	51%	31%
Spam filtering services	49%	29%
Cyber-risk insurance	9%	13%
Anti-virus desktop/server software	100%	0%
Virtual private network	82%	9%
Spam filtering software	55%	27%
Intrusion detection systems	44%	17%
Information security audit tools	47%	27%
Public key infrastructure	30%	19%
Smart cards	16%	20%
Single sign-on	13%	28%
Cyber-certifications (e.g., WebTrust)	26%	20%
Wireless security products	26%	24%
Digital identity management software	17%	24%
Biometric systems	2%	6%

Financial Services	Yes	Maybe in 2004
Managed security services	59%	11%
Policy development	54%	12%
Vulnerability management services	62%	20%
Spam filtering services	46%	27%
Cyber-risk insurance	19%	11%
Anti-virus desktop/server software	99%	1%
Virtual private network	76%	12%
Spam filtering software	58%	27%
Intrusion detection systems	66%	19%
Information security audit tools	62%	18%
Public key infrastructure	36%	20%
Smart cards	25%	15%
Single sign-on	32%	21%
Cyber-certifications (e.g., WebTrust)	31%	13%
Wireless security products	15%	28%
Digital identity management software	26%	18%
Biometric systems	10%	11%

Manufacturers	Yes	Maybe in 2004
Managed security services	59%	12%
Policy development	43%	20%
Vulnerability management services	39%	25%
Spam filtering services	56%	21%
Cyber-risk insurance	4%	7%
Anti-virus desktop/server software	100%	0%
Virtual private network	77%	8%
Spam filtering software	64%	22%
Intrusion detection systems	49%	25%
Information security audit tools	41%	28%
Public key infrastructure	20%	15%
Smart cards	11%	11%
Single sign-on	25%	22%
Cyber-certifications (e.g., WebTrust)	15%	13%
Wireless security products	34%	21%
Digital identity management software	16%	13%
Biometric systems	6%	8%

We asked organizations about their use or contemplated use of common information security solutions to improve their information security protection or to reduce data protection risks. The tables depicted in this section reflect the respondents' usage based on industry stratifications.

Public Sectors	Yes	Maybe in 2004
Managed security services	67%	7%
Policy development	47%	22%
Vulnerability management services	50%	22%
Spam filtering services	39%	34%
Cyber-risk insurance	5%	7%
Anti-virus desktop/server software	99%	1%
Virtual private network	78%	8%
Spam filtering software	41%	38%
Intrusion detection systems	52%	22%
Information security audit tools	48%	21%
Public key infrastructure	33%	19%
Smart cards	25%	10%
Single sign-on	22%	31%
Cyber-certifications (e.g., WebTrust)	21%	10%
Wireless security products	21%	19%
Digital identity management software	21%	12%
Biometric systems	16%	10%

Technology	Yes	Maybe in 2004
Managed security services	61%	9%
Policy development	54%	11%
Vulnerability management services	54%	23%
Spam filtering services	52%	24%
Cyber-risk insurance	15%	10%
Anti-virus desktop/server software	98%	1%
Virtual private network	83%	10%
Spam filtering software	68%	27%
Intrusion detection systems	69%	15%
Information security audit tools	58%	21%
Public key infrastructure	41%	15%
Smart cards	18%	17%
Single sign-on	28%	28%
Cyber-certifications (e.g., WebTrust)	27%	11%
Wireless security products	30%	28%
Digital identity management software	32%	22%
Biometric systems	25%	10%

Retail	Yes	Maybe in 2004
Managed security services	66%	15%
Policy development	51%	22%
Vulnerability management services	52%	30%
Spam filtering services	68%	19%
Cyber-risk insurance	7%	16%
Anti-virus desktop/server software	100%	0%
Virtual private network	70%	11%
Spam filtering software	68%	19%
Intrusion detection systems	38%	26%
Information security audit tools	49%	28%
Public key infrastructure	18%	22%
Smart cards	29%	11%
Single sign-on	28%	23%
Cyber-certifications (e.g., WebTrust)	23%	9%
Wireless security products	32%	26%
Digital identity management software	15%	21%
Biometric systems	11%	15%

Transportation	Yes	Maybe in 2004
Managed security services	47%	11%
Policy development	39%	32%
Vulnerability management services	44%	40%
Spam filtering services	38%	33%
Cyber-risk insurance	4%	9%
Anti-virus desktop/server software	100%	0%
Virtual private network	75%	18%
Spam filtering software	48%	30%
Intrusion detection systems	50%	32%
Information security audit tools	44%	23%
Public key infrastructure	32%	14%
Smart cards	20%	5%
Single sign-on	18%	23%
Cyber-certifications (e.g., WebTrust)	25%	9%
Wireless security products	34%	27%
Digital identity management software	25%	16%
Biometric systems	11%	5%

Moving Forward



**You are only as
secure as the weakest
link in the ever-
lengthening chain.**

We believe that the people who are “doing information security right” are those that have adopted a holistic view of their extended enterprise—all those entities that work together to produce economic value. A well-developed and ruthlessly executed information security policy will go a long way to protect the value a business creates. Senior management has an ever-strengthening mandate from the shareholders to regard information security as a fundamental responsibility. Unfortunately, the very things that ease entry and facilitate the extended enterprise open up multiple new points of vulnerability.

In this environment, respondents are all saying the right things. But, by and large, they are still taking information security on faith. This is a risky business. Any number of risks or failures can accumulate to put them at risk of a major business disruption and both financial and reputational losses. What seems to be more typical, unfortunately, is that, left to their own devices, decision makers will usually take the low-cost course of action. The accumulation of these substandard measures may serve as a perverse incentive for others in the extended enterprise not to invest in controls because the costs of failure likely fall on others.

On the other hand, an organization that is taking a holistic view honestly addresses the full array of security threats, both external and internal. Managers who emphasize effective security controls know that they can’t predicate their efforts upon “keeping the bad guys out.” Although public attention is quickly focused on viruses and incidents of hacking, it is the people who work for an organization and those who are already legitimate users of its network who are capable of doing the most damage.

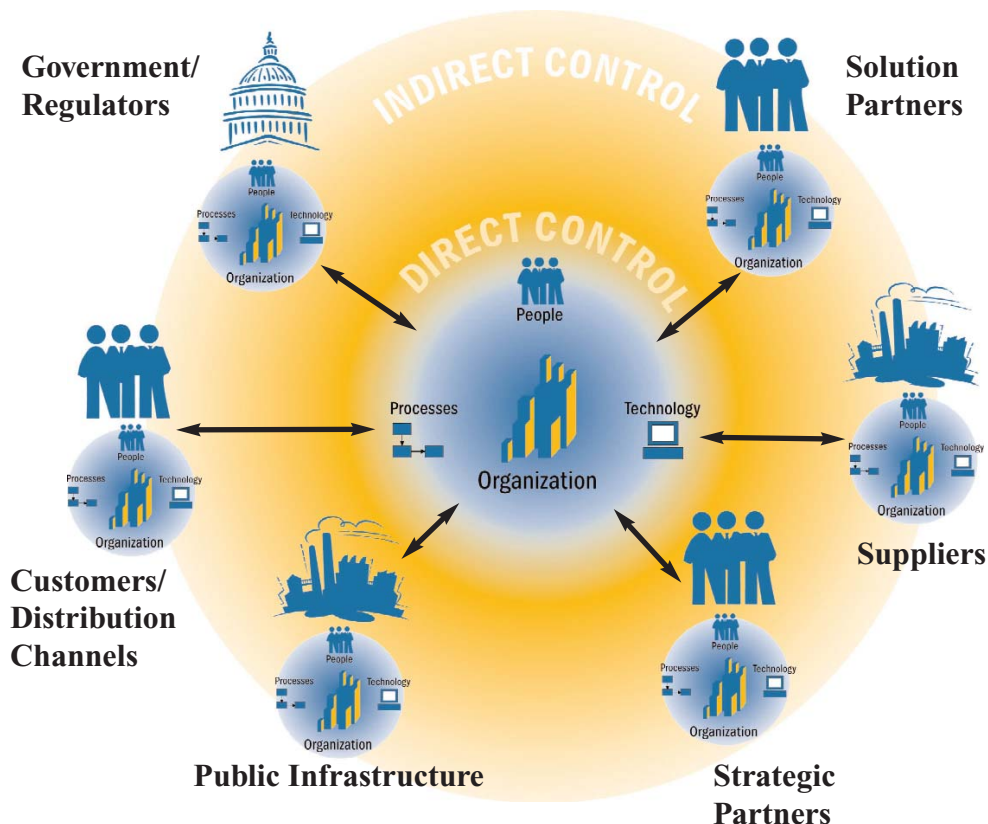
With a greater emphasis on a management-based approach to security that includes increasing employee security awareness, we believe that closer scrutiny of employees and business partners is necessary and inevitable. There is a certain irony with people. Collectively, they are the largest single risk, but if properly supported, they can also be the strongest layer in an organization’s defense.

Finally, the “tone at the top” is crucial. Executive attitude and motivation can make an exceptionally large difference. For example, for a CEO to view information security as a necessary cost of doing business is a basic expectation. However, looking at security as a business enabler, as a way to gain competitive advantage and a means to preserve shareholder value, raises the topic to a whole new level of awareness, urgency, and importance. As the world continues to get more complicated, the need for information security can only increase. We are bullish that organizations and senior management will rise to the challenge.

How Secure Is Your Extended Enterprise?

Realities that need responses:

- Faster growth in your organizational complexity than in your ability to understand and protect it
- Greater reliance on common software platforms, which extends the exposure of the entire network to common vulnerabilities
- Greater dependence between you and business partners to create value
- Lack of adequate incentives among many in the extended enterprise to address countermeasures that could benefit all members
- Shortfalls in the monitoring and enforcement mechanisms of government regulations
- Creation of risks by the behavior of others in the network



In the typical organization, according to survey results:

People

- Lack of user awareness named as the top obstacle to effective information security
- Roughly 70% failed to list “raising employee training/awareness” as a top initiative
- More than half fail to provide employees with ongoing training in security and controls
- Only 20% feel strongly that their organizations view information security as a CEO-level priority

Process

- More than 70% fail to regularly assess foreign-based third-party provider’s compliance with information security regulatory requirements
- More than 60% fail to regularly assess this vendor’s compliance with their organization’s security policy
- Some 40% fail to provide their employees with instruction on classifying data, e.g., confidential

Technology

- Almost 100% deployed anti-virus technology to protect themselves
- Less than 64% have vulnerability and penetration assessments conducted on a regular basis
- Less than 50% agreed that they could continue business operations in the event of a serious disruption

ERNST & YOUNG

www.ey.com

© 2004 EYGM Limited.
All Rights Reserved.

EYG No. FF0231