



ASSURANCE AND ADVISORY
BUSINESS SERVICES

SUB SERVICE INFORMATION
PRIORITY INDUSTRY TERM
OR DATE AND/OR ISSUE

! @ #

Global Information Security Survey 2003

Issues at a glance

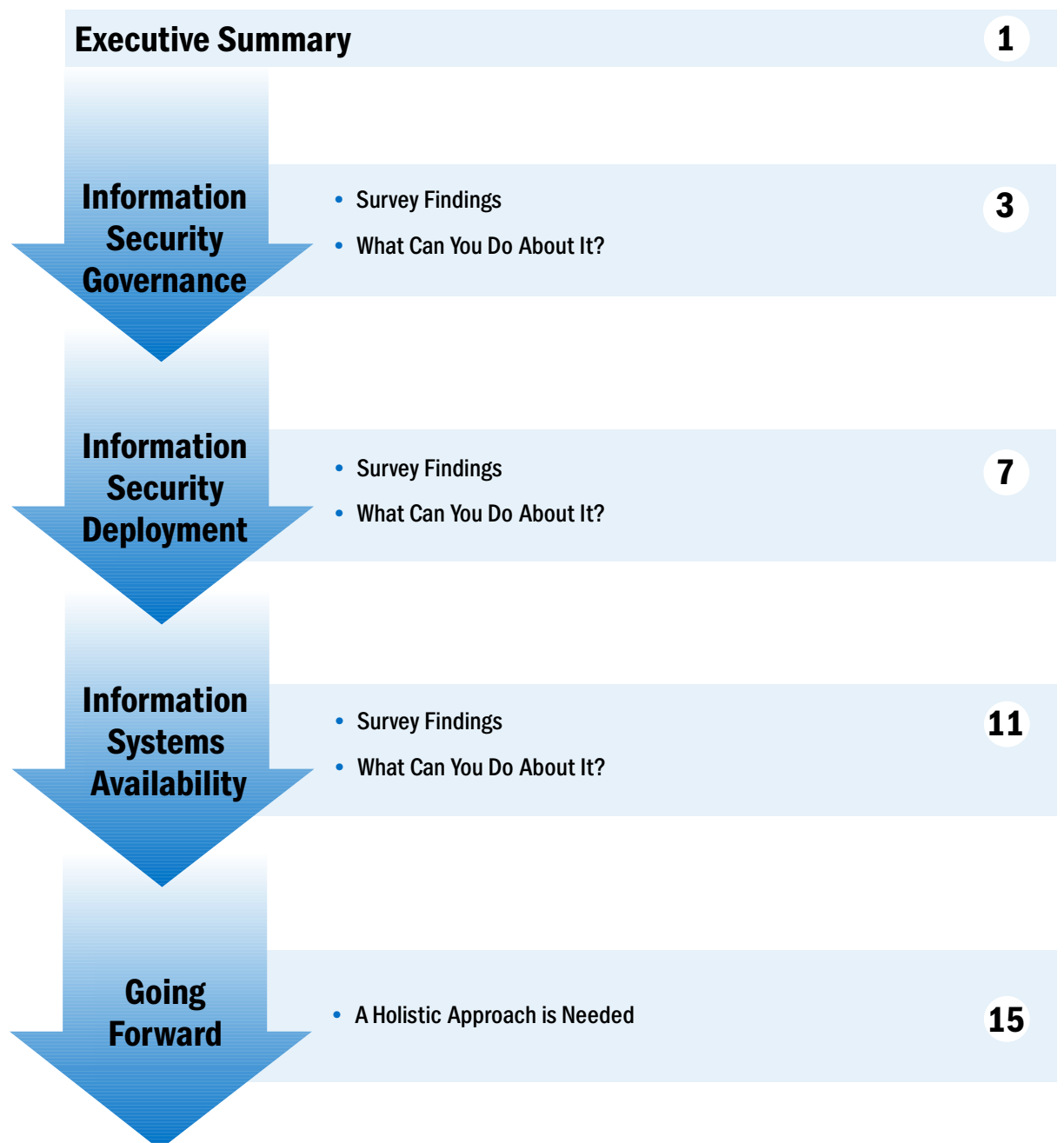
- **Ninety percent** of organizations say information security is of high importance for achieving their overall objectives.
- **Seventy-eight percent** of organizations identify risk reduction as their top influencer for information security spending.

However...

- More than **34%** of organizations rate themselves as less than adequate in their ability to determine whether their systems are currently under attack.
- More than **33%** of organizations say they are inadequate in their ability to respond to incidents.
- Only **34%** of organizations claim to be compliant with applicable security-driven regulations.
- **Fifty-six percent** of organizations cite insufficient budget as the number one obstacle to an effective information security posture.
- Nearly **60%** of organizations say they rarely or never calculate ROI for information security spending.
- Only **29%** of organizations list employee awareness and training as a top area of information security spending, compared with **83%** of organizations that list technology as their top information security spending area.
- Only **35%** of organizations say they have continuous education and awareness programs.



Survey Route Map



Executive Summary

The results of Ernst & Young's 2003 Global Information Security Survey were gleaned from the assistance of more than 1,400 organizations whose executives completed the questionnaire over a two-month period early in 2003. This was the sixth year in which we conducted the survey—to take a snapshot of information security and explore its implications for a broad spectrum of business and industry.

The respondents, from 66 countries, were in a variety of senior management positions, but the majority (60%) were chief information officers, chief information security officers, and other information technology executives. We found that the response profiles of the individual countries were remarkably similar to one another.

The survey asked 40 questions on all aspects of information security. Question topics dealt with how information security is situated and directed within the organization.

Issues and Implications

Among the major implications from the survey data:

- Insufficient budget is the number one cited obstacle to effective information security, followed closely by resource priorities—not surprising, in view of the tight economic picture that prevailed in most nations during the survey period.
- Return on investment (ROI) is not valued as a measure of information security spending effectiveness. This was evidenced by the nearly 60% of organizations that said they rarely or never calculate ROI for information security spending.
- Information security managers are harder pressed than ever to formulate and present a good business case because of their inability to explain the relevance of information security to the broad, overall business strategy.
- Despite the widely held views about how critically important risk assessment is, only 27% of our survey respondents placed “addressing information security assessment findings” among the top three influential factors when their organizations consider adopting new information security solutions.
- Few organizations are influenced by a broad spectrum of factors—which include opportunities, threats, and benefits—when addressing information security. Mostly, they take a one-dimensional, reactive, and risk-averse approach rather than a proactive and holistic one.
- There is a disconnect between the very high level of importance assigned to information security and the relatively low self-assessment among organizations; barely half say they align their spending well with their key business objectives.
- Technology is the strongest magnet for funds within organizations—a degree of spending that seems disproportionately high and suggests that a greater benefit might be derived from investing more heavily in the surrounding human capital issues instead of in hardware.
- Viruses and worms are the leading information security concerns and continue to generate the most media and public attention. But CIOs and other IT executives are increasingly recognizing the significance of internal threats such as employee misconduct involving information systems.

What Organizations Need To Do

During the period in which the survey results were taken this year, we sense that CIOs were hoping that competitive pressures and changing business needs would materialize, providing them with a business case for receiving more funds. This has not happened, and we believe that the growth projections being cited by major research organizations are several times greater than what will actually materialize over the next two or three years. Finding a credible alternative to conventional ROI approaches will be necessary to obtain funding for the information security function.

Information security issues are no longer solely the domain of the “computer gurus.” There is an intense and immediate need for them to capture the attention of senior management and their boards. Therefore, it will be critical for CIOs to communicate the issues in terms that are meaningful to these stakeholders. In order to have an effective information security posture, organizations need to align their information security with their business objectives. To do this, they must eliminate the hierarchical layers between the C-suite and the functional managers, who have historically viewed information security as a technology issue and not a business issue. Having the active involvement of senior management in security-related decisions is crucial in establishing this alignment.

Organizations need to back up their talk about the importance of protecting their digital assets by investing in information security. All too often it requires a security breach, a competitor being attacked, or a regulatory mandate for organizations to take action. Then, the core business objectives are ignored and a temporary “fix” is applied to the problem. Measured, proactive spending is less costly in the long run than reactive spending, which is often overspending in response to an incident.

Many senior executives still tend to focus on the more publicized security events, such as virus outbreaks and malicious hackers. They should focus more on the less-obvious and less publicized threats, such as disgruntled

employees and ex-employees, network links to business partners who don't have proven trustworthy systems, the theft of laptop and handheld computers, and insecure wireless access points set up by their employees. These can be the things that may not only cause serious damage, but can tarnish an organization's “brand.”

Internal Security Breaches Are Expensive

External attacks, when they are revealed, generally get more attention in the news media. However, hard experience points out that external attacks have not been historically as expensive as thought. A 2002 report by Vista Research estimates that 70% of security breaches that involve losses of more than \$100,000 are perpetrated internally, often by disgruntled employees. And inside attacks are potentially more costly.¹ A study conducted jointly by the Computer Security Institute and the FBI determined from a small sample of respondents that an insider attack against a large company caused an average of \$2.7 million in damages, where the average outside attack cost \$57,000. This bolsters the argument that security is to a large extent a people issue. Good human resource practices and adequate division of responsibilities are imperative, so that no one “runs everything.”

The foregoing comparison isn't to downplay the attention that should be paid to external threats, which can be substantial. A research firm, Computer Economics Inc., estimates that hackers, worms, and other high-tech interference caused \$11.1 billion in damages last year, more than a twenty-fold increase from 1995.²

Another leading issue connected with information security is the motivating power to mitigate risk. More than a third of organizations that responded regard risk mitigation as the most important influencer when they are considering expenditures for information security solutions. Indeed, one of the core realities of information security is that you must know your organization's critical information and identify what risks exist in regard to that information.

1. Cited in *The Economist*, October 24, 2002, “The Weakest Link.”

2. Cited in *The Orange County Register*, April 9, 2003, “Hacker Trackers.”

Information Security Governance

Security governance focuses on strategic alignment, delivering value while managing risk, and measuring overall performance. In an environment where IT is both strategic and operationally critical to many organizations, what are the current information security priorities—and is this view reflected in the investments that organizations make?

Survey Findings

Alignment of security with the business – Fifty-one percent of respondents said their information security spending was either completely or closely aligned with business objectives, while 37% rated themselves as somewhat aligned and 9% responded with “poorly aligned.” Based on our observations and experience, the 9% assessing themselves as poorly aligned is surprisingly low. With barely half the respondents rating themselves as at least closely aligned with their business objectives, it is clear that many organizations have much ground to cover in achieving a truly effective information security program.

Alignment is also manifested in how regularly meetings take place between individuals responsible for information security and business unit leaders, to gain an understanding of business objectives and information security needs. Only 25% of the survey respondents held such meetings at least

monthly. Twenty percent said they met only quarterly. Over 55% said they met less frequently, if at all. Comparing these responses with those to the other question about the degree of successful alignment of information security spending with business objectives, we sense a bit of incongruity. We believe that the infrequency of meetings between security people and business unit people suggests over optimism by the 51% of survey participants who characterize their alignment of information security spending with their business objectives as “closely” or “completely” aligned.

We also found that the great majority of organizations surveyed review their information security policies and procedures for consistency with business objectives and with current business processes annually or less, if at all. Reviews for consistency with business objectives are done by 33% on an annual basis, 25% do them less often, and 13% never perform such reviews. Only 5% conduct them monthly or more often and 25% do them quarterly or semi-annually. Survey results for the frequency of reviews for consistency with current business processes were very similar, with 31% saying they perform these reviews annually, 25% say less often, and 11% reply that they never conduct such reviews. Only 6% say they conduct these reviews monthly or more often, and 27% do them quarterly or semi-annually.

Organization and reporting relationships – Nearly one-third (31%) said their chief information officer was the person primarily responsible for information security. Fourteen percent named the information technology executive, and 13% named the chief information security officer. Chief Executive Officers were named by 5%.

“The alignment of information security spending with an organization’s business objectives is only possible when information security is viewed as an organizational issue, not just an IT issue.”

John Cieslak, CIO
Toronto Stock
Exchange

The number of respondents who said their organizations provide their top governing body with reports about information security status or security incidents quarterly, monthly, or more often surprised us, particularly the 15% who declared they make monthly or more-frequent reports. This seems high, in our estimation. If true, it is encouraging. Twenty-one percent reported quarterly frequency.

However, there is another side to the story. There was heavy response at the low end of the scale, as well, with 19% acknowledging they made reports only on an annual basis, another 19% reporting less often than that, and those who never make such reports (14%). This is not a good sign and reflects a great deal of work needed to transform information security into an issue that gets equal status in the boardroom with other major business concerns.

Perceived importance – Ninety percent of those surveyed categorized the importance of information security as very important or somewhat important to their organizations’ overall objectives. However, we take a cautious view of this finding in light of the alignment gap we noted earlier, between information security and business objectives. Those entrusted with information security need to respond in a much more substantive way to the high importance they say they attach to this vital business issue.

Low priority of human capital – As part of security governance, human resource spending associated with information security does not enjoy the high priority that would seem to be justified, in light of what organizations identify as the chief obstacles they see to effective information security. The urgency is felt, but somehow not acted upon. When asked what their organizations’ top three areas of spending were, just one-third mentioned staff. On the security spending hierarchy, expenditures for staff were ranked fifth behind consultants, process improvement, business continuity planning, and technology. It is therefore no surprise that 32% of survey respondents ranked “a lack of availability of skilled staff” among their top three impediments to effective information security within their organizations.

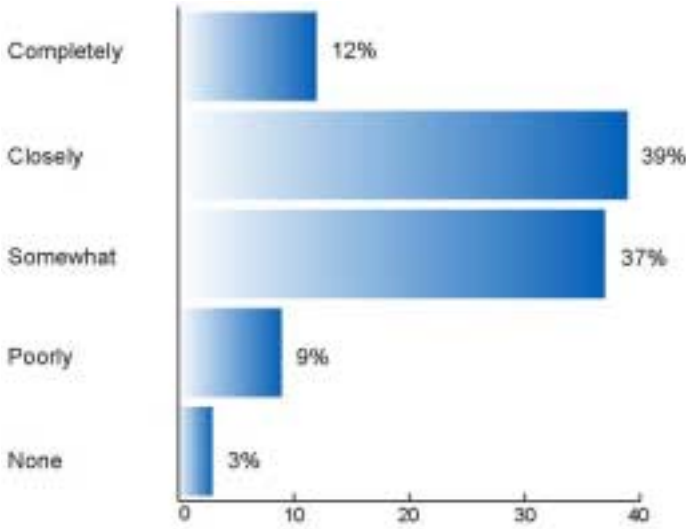
“To be truly effective, security procedures should be reviewed for consistency with business processes and objectives on an ongoing basis and as part of the lessons learned from incidents.”

**Mostafa Mehrabani,
Executive Vice President & CIO,
McGraw-Hill**

Other people-related investments were low on the spending agenda, as well. Employee awareness brought a response from only 16% (ranked sixth) and training received just 13% (ranked seventh). We believe that relegating human resource concerns to such a low priority may be seriously shortsighted, in view of the potential threat and costs cited in our Executive Summary, as well as the growing number of vulnerabilities that are appearing on the horizon.

Regulatory compliance – Not surprisingly, a heavy proportion of our survey respondents said that government security-driven regulations are having an impact on their industries and their organizations. Thirty-eight percent cited a major impact and 37% acknowledged a minor impact. Interestingly, a significant 11% did not acknowledge any impact. This response may reflect the not-for-profit constituency that participated in the survey.

Thirty-four percent of the respondents said their organizations are compliant with security-driven government regulations, while 32% said they are partially compliant. Thirteen percent responded “no” and 21% claimed that no compliance was needed—perhaps representing the views of non-profit organizations.



Question 9:
How well is the organization's information security spending aligned with its business objectives?

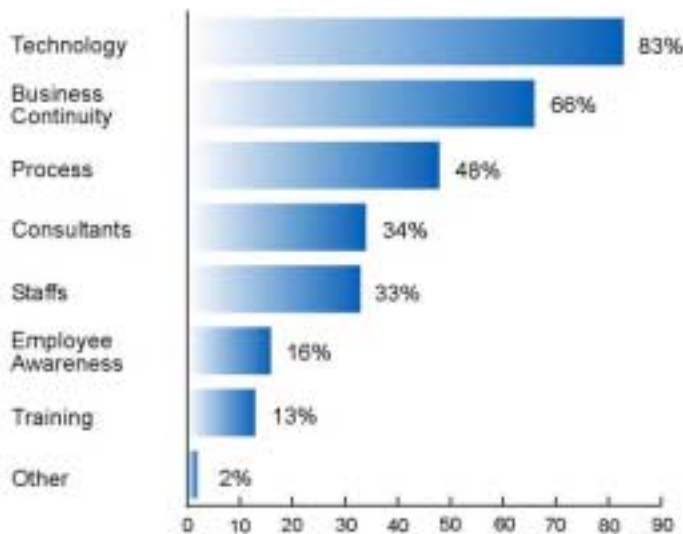
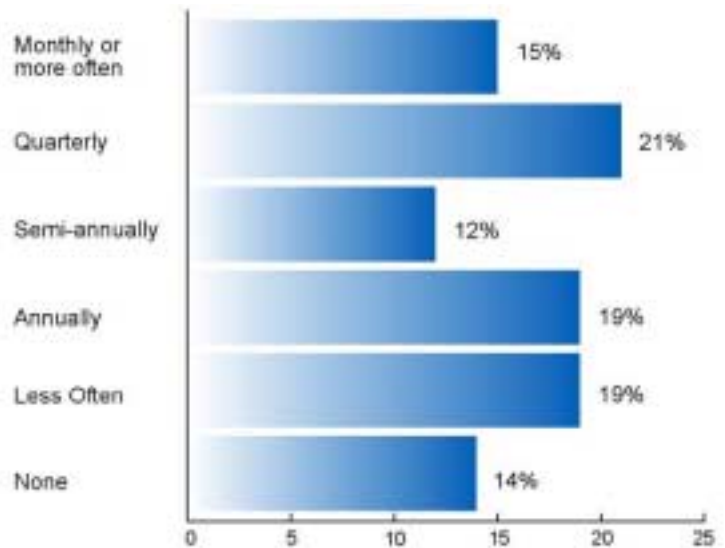
Fifty-one percent characterize their information security spending as completely or closely aligned with business objectives.

Percentage of 1418 Respondents

Question 13:
How often does your organization provide its boards of directors or equivalent with a report about the organization's information security status or security incidents?

Thirty-eight percent of respondents said their information security function makes reports about information security status or security incidents to their top governing body on an annual basis or less often. An additional 14% never makes such reports.

Percentage of 1419 Respondents



Question 10:
What are your organization's top three areas of information security spending?

Spending on people and related investments ranked fifth or lower, behind technology, business continuity, process, and consultants.

Percentage of 1425 Respondents

What Can You Do About It?

The “What you can do about it?” tables are unchanged from last year. Feedback indicates that our readers found them helpful, and the suggestions they contain are still relevant.

If you believe you have an information security strategy, challenge whether it is business risk-based or just technologically rationalized. Ask whether it is truly understood and implemented. Ensure that you are getting objective assurance that it is effective. If you don't have a strategy, now is the time to act.

1. Whether challenging an existing information security strategy or developing a new one from the start, make sure the final strategy creates a positive response to the questions at the right.

- Does it consider the organization's wider business strategy, maturity, and culture?
- Is it consistent with the organization's overall IT and business security strategies?
- Does it provide a framework for establishing security awareness, sourcing strategies, funding, priorities, resourcing, technologies, and tools?
- Does it provide direction for decisions on key third-parties, such as service providers and other stakeholders such as suppliers or customers?
- Is there an articulated and agreed-upon set of threats and critical assets that is prioritized and reviewed regularly?

2. Once you have the strategy, look at IT security plans and budgets across the organization.

- Do you have a framework within which you can make investment decisions and determine the impact of cutting expenditure or curtailing projects?
- Do you know how much you are spending and on what?
- How do you measure your return on investment?

3. If IT security is not on the board's agenda, make sure it is, and not just when there is a problem. Information is an asset and information security is too important to be left to IT alone. An organization's capability and appetite for risk management comes from the top and effective IT security can create competitive advantage.

- Do you have visible and measurable board support?
- Is the organization clear where it sees itself in its approach to security and risk?
- Is information security importance reflected in investment and programs?
- How do you ensure that technology, people, and process activities related to information security are linked?

4. Ensure that accountability for information security is clear and recognized.

- Do you have performance goals and metrics to measure effectiveness?
- Are there mechanisms to achieve independent assurance that information security is effectively managed?
- Is there organization-wide recognition of security accountability and responsibility?

Information Security Deployment

In this section, we attempt to identify our survey respondents' key concerns and challenges in achieving the required level of information security. Where do they perceive the real threats to be, based on their own experience, and what steps have been taken to address concerns?

Relative Intensity of Threats over the next 12 months?	Mean				
	Low 1	2	Mod. 3	4	High 5
Major virus or worms			•		
Employee misconduct involving information systems			•		
Distributed Denial of Service (DDoS) attack			•		
Loss of customer data privacy/confidentiality			•		
Amateur hackers or "Script Kiddies"			•		
Theft of proprietary information or intellectual property			•		
Consultants/vendors who have access to info systems			•		
Former employee misconduct involving info systems			•		
Natural disasters			•		
Business partner(s) misconduct involving info systems			•		
Competitor espionage			•		
Political "hactivism" or cyber protest			•		
Cyber-terrorism—foreign-based			•		
Cyber-terrorism—domestic-based			•		
Non-nuclear terrorist attack			•		
Cyber War			•		
Foreign government espionage			•		

Survey Findings

Relative intensity of threats – We asked respondents to assign a numerical value to the intensity of the threat they felt was posed by each of 17 adverse events that could befall their organization. The survey used a one-through-five scale, with one equaling lowest threat intensity and five equaling highest intensity.

We found that 57% of the respondents rated employee misconduct with information systems as moderate to very high, while 31% rated former employee conduct within this range. These percentages contrasted with the much higher 77% who believed major viruses or worms have the highest threat intensity. While viruses and worms are indeed serious threats, people with insider status—employees, former employees, and trusted business partners—pose a far greater threat to organizations in terms of potential cost

per occurrence and total potential cost than attacks mounted from outside. The fact that only 5% of survey respondents attributed unexpected or unscheduled outages of critical business systems in the past year to employee misconduct and just 1% blamed misconduct of a former employee does not minimize the threat of internal security breaches. It may be a reflection of good luck, good people practices, or an expression of natural hesitancy on the part of employers to reveal internal breaches out of concern for damage to their organizations' reputation. In addition, in certain cultures, employee misconduct is not openly discussed. In defense of managers, it is natural for them to have their attention swayed toward external threats because they are already inundated with information about hackers and worms.

Level of information protection – Seventy percent of the survey respondents rated their level of protection of critical business information as either world class or adequate. When we correlated the self-assessments about the ability to protect critical business information with the responses about how information security policy was structured, the organizations that reported having centralized policies felt that they had the clear edge. Among those that gave themselves either the highest rating or an adequate rating in level of protection, nearly 80% had centralized policy structures, compared with 68% who had decentralized information security policy structures.

The same pattern materialized when we compared organizations' ability to protect critical information with how often their information security functions reported concerns, issues, or incidents to top management. Eighty percent of the highest self-rated organizations in terms of ability to protect critical information made reports to their board or similar governing body on a monthly or more-frequent basis, while only 63% of such organizations were among those who made reports less than once a year.

Perceived obstacles – In the previous survey for 2002, the speed of change, and the increasing sophistication of threats, was the leading factor cited that inhibited effective information security. Also in the 2002 survey, lack of sufficient budget was in fourth place. In the 2003 survey, the shortage of available funds migrated to the top as the leading inhibitor, named by 56%. This is not startling in view of stock market turmoil and poor general economic conditions that prevailed in most countries.

Risk mitigation the chief motivator – Two of our questions explored the quest for security solutions from the viewpoint of what factors are most influential in driving information security spending, and what aspects of security are the strongest magnets for these expenditures. Results showed that organizations worldwide are clearly being driven by risk reduction, which was named by 78% of those responding. Legislative and regulatory compliance (48%) and reputation and trust (47%) were in second and third place.

Risk management is certainly not a misplaced rationale for making information security investments: witness the large loss figures connected with damage estimates. A digital risk management firm based in the UK, mi2g Ltd., says that there could be more than 180,000 attacks—amounting to \$80 billion to \$100 billion worth of damage during 2003. With the number of vulnerabilities doubling since 1998, according to Carnegie Mellon University’s CERT Coordination Center, it’s no wonder that risk management is a leading motivator.

What are the spending magnets? – The aspect of information security that is getting the most money is technology tools, software and hardware, which were named by 83% of those responding. Spending on business continuity (named by 66%) and process improvement (48%) were the runners up. As noted earlier, employee awareness and training, combined, captured only 29% of the response — the lowest-

“Only in the high end of security investment aimed at managing risks over and above basic controls should specific security ROI be used. In all other cases, investment evaluation for security should be included in the total IT proposition.”

Dr. Paul Dorey, Director
Digital Security, BP

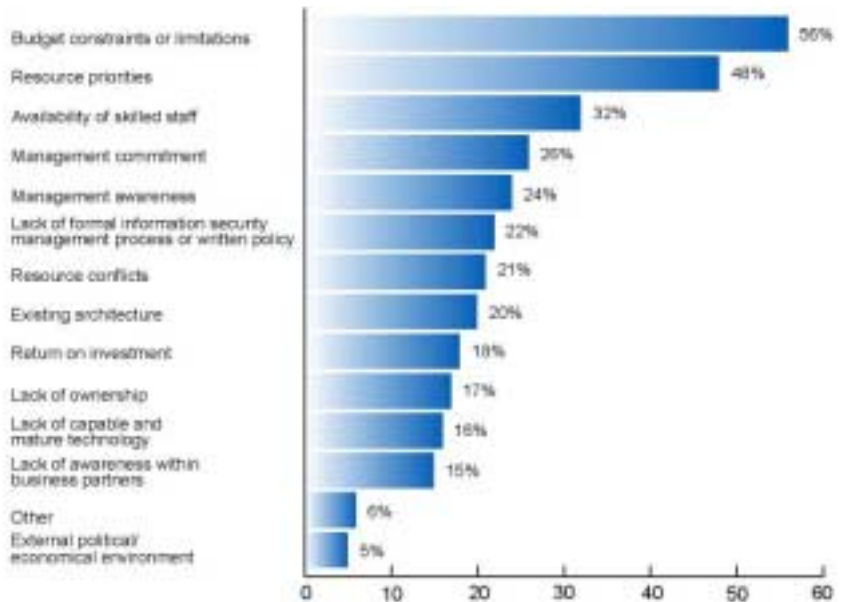
ranked two factors on the list. There is ample evidence, in our opinion, that the money spent on technology tools may in fact be at the expense of organizational and people issues. We regard the human capital part of the equation as very important in addressing information security and deserving of far more consideration that it is apparently receiving.

More than half don’t consider ROI – Although the number one obstacle to effective information security is insufficient budget—according to 56% of those surveyed—59% of the sample says they rarely or never make an ROI calculation for information security spending. It appears that ROI has fallen out of favor as a measure of spending effectiveness for information security. Many information security managers are now harder pressed than ever to formulate and present a good business case for greater security budgets. Work that has been done in developing the credibility of Return on Security Investment (ROSI) is encouraging, but quantifying important variables such as loss of confidence and employee productivity is difficult at best.

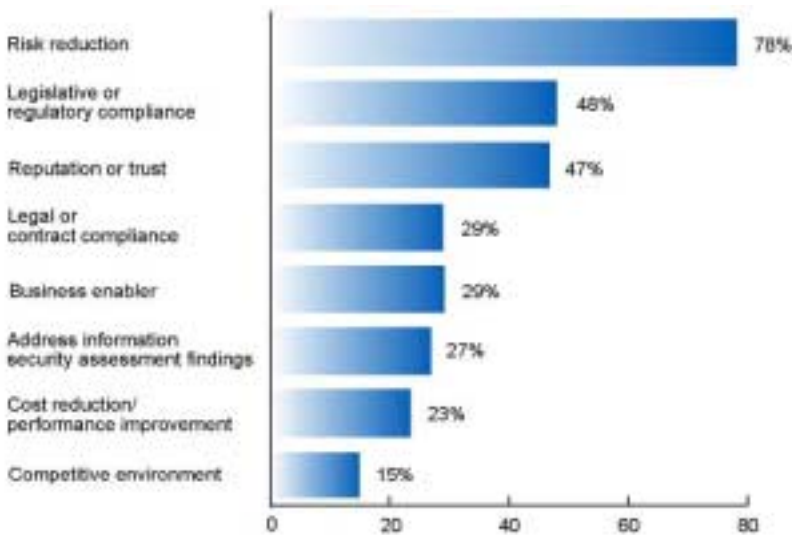
Question 21:
What are some of the most significant obstacles to effective information security within your organization?

(Multiple responses allowed)

The number one obstacle to effective information security is insufficient budget, according to 56% of those surveyed.



Percentage of 1413 Respondents



Question 19:
What top three factors are the most influential when your organization considers adopting new information security solutions?

(Multiple responses allowed)

Organizations worldwide are clearly being driven by risk reduction.

Percentage of 1424 Respondents

What Can You Do About It?

1. Know what is important to your organization. It may be your strategic plan, financial information, product research and pricing information, personnel information, supplier details, etc.

- Have you conducted a proper threat and vulnerability analysis, including an assessment of others' capabilities and incentives to launch attacks?
- Have you assessed your ability to deal with the threats?
- Do you have a process to re-assess threats and vulnerabilities regularly?

2. Agree on the priorities and get the basics in place. People, process, and technology combine to achieve effective security.

- Are you confident that your antivirus technologies and policies, for example, cannot be undermined by inadequate training and awareness activities?
- Is your firewall protection, for example, being undermined by the absence of clear policies and standards to control connectivity in the organization?
- Do you budget and plan for effective and regular assurance activities?

3. Once you have agreed on your priorities, assess your core information security competencies.

- Do you have qualified in-house talent who can provide robust management of security activities across the business, IT, and third parties?
- What is reasonable to do in-house and what might be better done by others, either because they have greater depth and breadth of expertise and experience, or because independence is needed?
- If you are using a third party, have you conducted a rigorous assessment of their skills and capabilities, culture, and their understanding of your business?

4. Ensure you have appropriate management information to enable you to make decisions and manage information security effectively.

- Are you receiving information on a regular basis that allows you to assess the suitability of continued connectivity with third parties?
- How are you measuring and monitoring the staff awareness aspects of your information security framework?
- What was the impact of the latest virus? Did the organization handle it better than previous incidents?
- How recently have you reviewed your approach to detecting and monitoring both internal and external incidents and attacks?

Information Systems Availability

In the 20-plus months since September 11, 2001, the set of probabilities that businesses face in preparing for business interruption has changed significantly. Our survey explored the major causes of system unavailability; whether organizations know and act upon the business impact of systems not being functional; and how organizations are addressing business continuity issues in the event of system outages.

Survey Findings

Experiencing and recognizing causes of system outages – Slightly more than half (52%) of our survey participants said they had experienced an unscheduled or unexpected outage of a critical business system in the past year. The largest segment (34%) attributed hardware failure as the cause, while 31% blamed a telecommunications failure, and 25% cited software.

The most recent experience with combined hardware and software failures tracked very close to the year earlier responses—59% this year compared with 56% in the 2002 survey. Telecommunications failures dropped from nearly half of respondents (49%) recognizing them a year ago to 31% this year.

Major viruses or worms were named by 22%—relatively unchanged from last year's 24% answering the same question. Near the low end of the hierarchy of causes were employee misconduct (cited by 5%) and former employee misconduct (named by 1%).

Operational errors, such as loading the wrong software, have apparently been curbed somewhat, with 15% citing this as the cause of the outage, compared with 25% last year. System capacity issues followed a similar pattern, declining from 26% to 10%. Third party failures also declined—named by 26% last year and 16% this year.

Sense of urgency – Our survey showed there has been little change in organizations' sense of urgency about business continuity and disaster recovery since the level measured in the months immediately following September 11, 2001. Nineteen percent said they had an extremely urgent regard right after the terrorist attacks and 18% responded this way in our 2003 survey. Those characterizing these issues as


urgent amounted to 45% of the sample in our 2002 survey and 47% in this year's survey. Likewise, the percentage claiming these issues were changed little—6% this year, compared with 7% last year.

Business continuity plans of major partners – Just over half—54%—of the respondents replied that they have a process in place to monitor the business continuity plans of their critical relationships so that operational connectivity could be maintained at an acceptable level during a system outage. Thirty-two percent replied in the negative and another 13% said the process was not applicable or they did not know.

Identifying vulnerabilities and detecting attacks – sixty-six percent of respondents rated their effectiveness in identifying information system vulnerabilities as either “world class” or adequate. With just 7% giving themselves the highest assessment, the consensus seems to indicate most

“Business continuity plans are rarely given much thought until well after a business deal has been struck and security needs to be considered as part of establishing any business relationship.”

John Cieslak, CIO
Toronto Stock
Exchange



organizations deem themselves “good enough.” However, the remaining 35% who rated themselves as marginal, inadequate, or not adequate at all is a real cause for concern.

When we shifted the point of emphasis slightly and asked (in a separate question) about ability to detect whether systems were under attack, the response profile was very similar. Sixty-six percent rated their own organizations as world class or adequate and 32% claimed a rating of marginal, inadequate, or not adequate at all.

The similarity of the responses given to identifying vulnerabilities and detecting attacks points out that executives consistently acknowledge they have work to do to ensure they can prepare for and respond to system attacks. It should be noted that the two tasks are different in nature, but have to be considered as part of a holistic picture.

Centralization has benefits – When we correlated the responses about how well an organization could identify system vulnerabilities with the organization’s information security policy structure, we found that “adequacy” was raised significantly (72%) when an organization had centralized policy, from the level of only 63% observed when policy was decentralized. A similar pattern emerged when the survey compared centralized structure and ability to detect if information systems were under attack. Centralized structure had a positive relationship with an adequate rating; more than 5% more organizations with a centralized structure rated themselves as adequate than those who had a decentralized structure.

Frequency of reporting – Our analysis shows that the frequency with which information security executives make reports to the top governing body has a positive relationship with an adequate rating when it comes to identifying system vulnerabilities. When information systems managers make reports less frequently than yearly, an “adequate” rating results among only 57% of respondents. When reports are made more frequently, adequacy rises significantly—to 64% among those reporting yearly—and to 76% among those who report to their top governing body monthly or more often. The same trend applies when one considers ability to detect a system attack.

Assessing recovery and continuity – Two-thirds rated their own ability to continue business operations in the event of a malicious attack or disaster as either world class or adequate, with the largest number (64%) declaring themselves adequate.

When we asked respondents to rate other business entities, the largest segment in each case rated the entity as adequate. Thirty-one percent rated their major competitors’ ability to continue operations as adequate; key suppliers drew an adequate rating from 35%; key outsource vendors drew a 36% response. Twenty-one percent rated key customers as adequate and 28% rated key alliance partners as adequate.

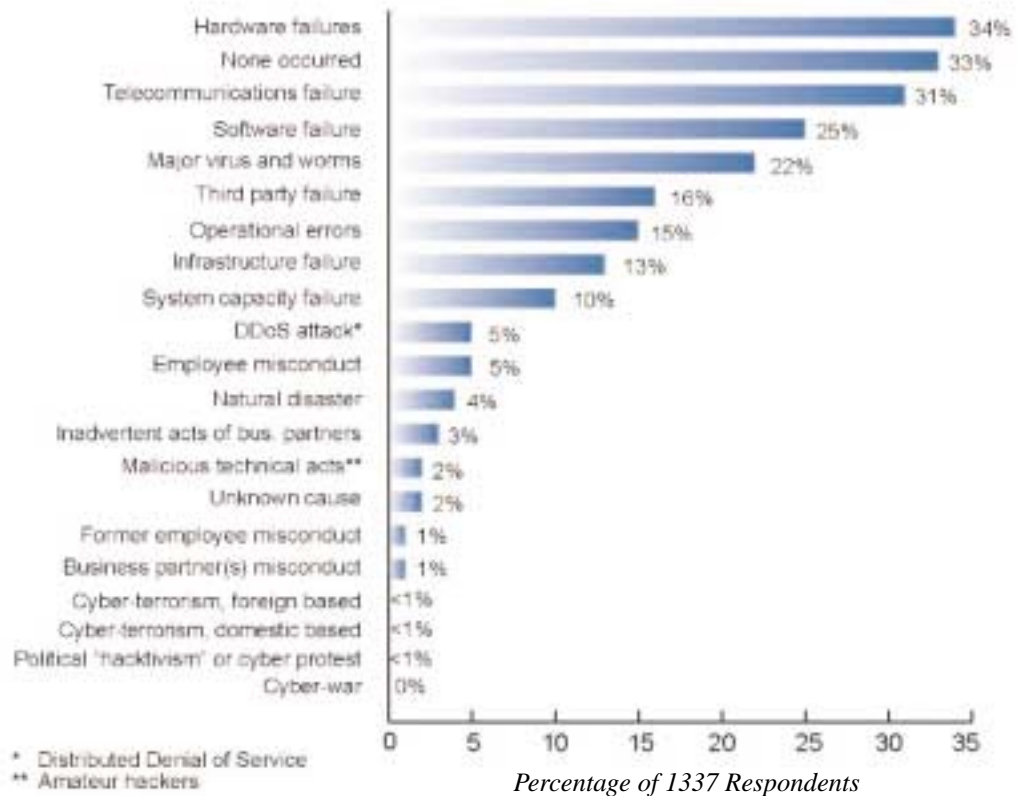
The relatively low number of respondents (54%) who acknowledged they have a process in place to track the effectiveness of the business continuity plans of their major business partners suggests that the prevalent “adequate” assessment they gave their partners—in their ability to identify vulnerabilities and detect attacks—may be simply a convenient “hunch.” This important issue requires a much more fact-based assessment than it appears to be receiving.

Reporting of incidents – Internet service providers were the most often-named entity that our survey respondents (47%) would notify in the event of an information security incident. Business partners and suppliers ranked second (45%) and law enforcement agencies, named by 38%, were in third place. Twenty-nine percent said they would notify customers and 20% would notify a government agency. Twenty-two percent replied that they would not report the occurrence to anyone. In light of the hesitance of many organizations to report security incidents, we found the number who would report to law enforcement surprisingly high. Not surprisingly, in a related question in which we asked the reason if they did not report at all, negative publicity was the leading cause, reported by 26%. Damage to brand or reputation ranked second (21%); internal policy was named by 17%; and competitive vulnerability was identified by 11%. Fourteen percent said they did not know which government agency to contact. A significant 9% were unaware that they could file such reports.

The insurance issue – When we asked our survey respondents if they have insurance coverage for losses due to damages arising from information security breaches, nearly a third (33%) replied that such risks were covered by their general policies and 34% said they did not have insurance. Either way, this is a problematic situation. Such damages are not covered by broad form insurance policies and organizations should have these risks covered. It was also revealing that 22% of the responding sample said they did not know the answer to the question. Seven percent responded that these losses were insured by a specific policy—a response that seems astonishingly low, given the risk environment and the fact that general policies don’t provide such coverage.

In the past, when connectivity was not so prevalent as it is now, computer risks were included in general insurance policies. But as the year 2000 and its perceived threats approached, insurers specifically excluded these risks. Insurers can provide coverage against a range of risks, such as data theft, malicious attacks, or loss of income due to security breaches or network failures. But these risks are not covered by general business policies. To obtain this coverage, your organization will have to quantify and demonstrate the risks it wants to insure against—a job that is difficult and takes time and research.

Question 36:
What was the cause of your organization’s unexpected or unscheduled outage of critical business systems within the last 12 months?
 (Multiple responses allowed)



Hardware failure was still the most-often-cited cause of failure, little changed from last year. Operational errors, system capacity issues, and third-party failures were lower in 2002.

What Can You Do About It?

Efforts to prevent disasters should have equal footing with what you will do after the disaster occurs.

1. Know what is important to your business and the threats it might face. This is key to achieving a consistent understanding of business priorities.

- Do you know what would be the impact on the organization of a serious security incident or loss of availability in terms of reputation, revenue, legal, operational performance, and investor confidence?
- Have you identified and assessed the major threats to your business?

2. Ensure you have good operational procedures supporting your critical IT services.

- Do you know what has been the cause and impact to date of systems operational failures?
- How robust are your procedures for making changes to operational software?
- How confident are you that data backups work and are genuinely being taken off site in accordance with agreed cycles?

3. Review your approach to business continuity planning (including consideration of third parties).

- Have you followed a formal approach to develop your recovery plans?
- Have you done enough to identify and minimize the risks to your business operations?
- Have you considered the full end-to-end business process? Was the business involved in assessing what is needed for recovery and agreeing recovery timescales?
- Are the plans robust enough to deal with a range of disasters?
- Have you challenged assumptions used in developing plans?
- Are your plans over-reliant on key individuals to manage the crisis?
- Will you be able to access both your recovery and offsite data storage locations following a disaster?
- Are you confident you know what your service providers will supply if you need to call on them?

4. Test regularly, and update arrangements accordingly.

- How will you communicate, test, and review business continuity plans regularly? Consider using a range of disaster scenarios in the testing of the plans (for example, inability to access a key building, a supplier failure, or enterprisewide virus attack). Review and update plans accordingly—following tests.

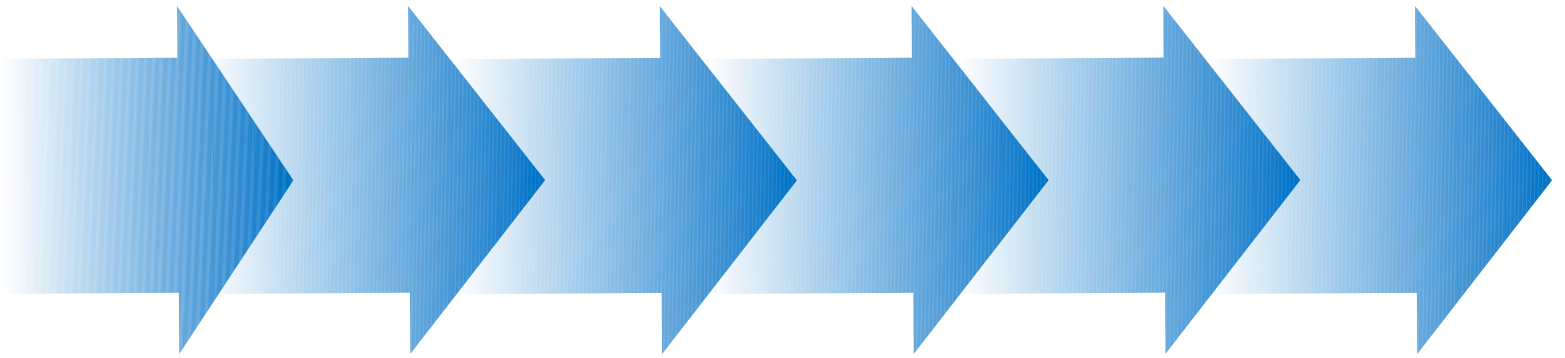
Going Forward

A Holistic Approach Is Needed

Senior management and boards of directors are under greater scrutiny for risk management oversight. Yet, the overall responses we gathered in this year's survey seem to suggest that many organizations are continuing to take a piecemeal approach to information security. As we saw in the survey, most organizations continue to have major gaps in risk coverage, while the impact of information security failures on market value has grown exponentially.

Information security, availability and confidentiality only address some of the components of an organization's digital risk. Therefore, we are moving beyond the concept of just information security. For organizations to successfully manage their digital risk in the future, they need to develop an enterprisewide Digital Risk Framework, which addresses:

- IT and project integrity, and effectiveness
- Effective and efficient control environment
- Security and availability of digital information
- System privileges and access controls
- Disruption from intrusions or viruses
- Threats to business continuity



To be sustainable, the Digital Risk Framework must evolve with the organization's business objectives and strategies, and encompass the following key points:

- ☑ It must be flexible to deal with the growing complexity and scale of information security threats to the organization
- ☑ It needs to ensure that the supporting information security policy is sound and enforceable
- ☑ It must recognize that people and process are critical, and that technology is just a small part of an overall Digital Risk framework
- ☑ It has to evolve with the changing regulatory requirements, threats, and controls
- ☑ It must be vigilant to be able to react to or anticipate new threats, trends, and opportunities for improvement

Enterprisewide Digital Risk Framework



ERNST & YOUNG LLP

www.ey.com

© 2003 Ernst & Young LLP.
All Rights Reserved.
Ernst & Young is
a registered trademark.

SCORE Retrieval File
No.FF0224