

# Deloitte.

---

Global Financial Services Industry

---

## 2005 Global Security Survey

A large, weathered wooden Trojan horse sculpture stands prominently in the foreground. Behind it is a multi-story brick building with several windows. The scene is set against a clear blue sky with a few wispy clouds. A tall, thin evergreen tree is visible on the right side of the frame. The overall image conveys a sense of history and security.

Audit • Tax • Consulting • Financial Advisory •

# Contents

Objective of the survey	4
How we designed, implemented and evaluated the survey	5
Key findings of the survey	13
Governance	19
Investment in security	23
Value	25
Risk	26
Use of security technologies	30
Quality of operations	32
Privacy	34
Global Financial Services Industry Security Outlook	36
Helpful references and links	40

# Foreword

Three years ago, Deloitte Touche Tohmatsu (“Deloitte”) embarked on an ambitious undertaking: to survey global financial services industry organizations to determine the state of their IT security. Back then, we didn’t fully understand the enormity of the task we were taking on – which probably worked in our favour. We’ve learned a lot along the way, enhancing the things that worked and discarding those that didn’t. Conducting this survey brings home to us, again and again, the lesson that nothing stays the same – particularly in the world of IT. For example, when our survey referred to “phishing” a year ago, few organizations outside North America would have known what we were talking about. But, within the space of 12 months, it has become one of the security threats most feared by our survey respondents. What a difference a year makes!

While every year the survey becomes a more challenging undertaking, it also becomes more rewarding – last year’s survey was translated into three languages (French, German and Japanese) and its growing reputation garnered extensive media coverage. In addition to being mentioned on television and in the press, the 2004 Global Security Survey found its way to The White House. The US President’s Information Technology Advisory Committee (PITAC) issued a report, citing one of the Survey’s findings regarding security breaches. Deloitte was the only Big 4 firm mentioned in the report.

With this recognition comes our extreme gratitude – as well as a growing awareness of our responsibility. Going forward, we will do whatever we can to ensure that the Global Security Survey becomes *the* word on the state of information security in the financial services marketplace.

As in other years, the 2005 survey reveals some new “hot” issues and brand new trends. It’s probably quite accurate to say that there is never a dull moment in IT security – I promise you an interesting read along with some eye-opening findings.

As the reputation of Deloitte’s annual survey continues to grow, we find more and more people willing to give their time to the survey and, for that, we are extremely grateful. I cannot express enough my sincere thanks to the Chief Information Security Officers, their designates, and the security management teams from financial services industry organizations around the world, for the time they have spent and the candid and forthcoming manner in which they continue to keep this survey “real”.

The global co-operation that is so clearly evident from this survey underscores the fact that, despite geographic, social and cultural differences, we all have a common goal: to protect the information that is the lifeblood of our businesses.



**Adel Melek**, Partner, Global Leader  
IT Risk Management & Security Services  
Global Financial Services Industry  
Deloitte Touche Tohmatsu



# Objective of the survey

The response and the media attention that the 2003 and 2004 Global Security Surveys have received has been gratifying. Participation in this year's survey has increased more than 20% over last year. Results from the Deloitte surveys have been quoted in media ranging from North American and international newspapers to the President of the United States' IT Advisory Committee Report on Cyber Security.

We are thrilled by the following that the Survey has inspired and are pleased to continue that momentum with the 2005 Global Security Survey. Deloitte's purpose in publishing the survey is to continue to contribute to the protection of the financial services marketplace by sharing current practices and by identifying future trends in security and privacy management.

The goal of the 2005 Global Security Survey is to help respondents assess the state of information security within their organization relative to other comparable financial institutions around the world. Overall, the survey attempts to answer the question: **How does the information security of my organization compare to that of my counterparts?** By comparing the 2005 data with that collected for the 2003 and 2004 surveys, we can begin to determine differences and similarities, identify trends and introduce more in-depth questions, such as: **How is the state of information security changing within my organization?** and **Are the changes aligned with the evolution of the rest of the industry?**

Where possible, questions that were asked as part of the 2003 and 2004 Global Security Surveys have remained constant, thereby allowing for the collection and analysis of trend data. So that questions remain relevant and timely with regard to environmental conditions, certain areas were re-examined and expanded to incorporate the "hot" issues being addressed by financial institutions at a global level. Deloitte subject matter specialists were enlisted and their knowledge leveraged to identify questions with the most impact.

# How we designed, implemented and evaluated the survey

The 2005 Global Security Survey reports on the outcome of focused discussions between Deloitte Touche Tohmatsu (DTT) and DTT member firms' Security Services professionals and Information Technology (IT) executives of top global financial services institutions (FSIs).

Discussions with representatives of these organizations were designed to identify, record, and present the state of the practice of information security in the financial services industry, with a particular emphasis on identifying levels of perceived risks, the types of risks with which FSIs are concerned and the resources being used to mitigate these risks. The survey also identifies which technologies are being implemented to improve security and the value FSIs are gaining from their security investments. To fulfill this objective, senior members of Deloitte's Security Services Group designed a questionnaire that probed seven aspects of strategic and operational areas of security and privacy. These seven areas, and their sub areas, are described on page six in the section entitled **Areas Covered by the Survey**.

Anonymous responses of participants relating to the seven areas of the questionnaire were subsequently analyzed, consolidated and presented herein in both qualitative and quantitative formats.

## Survey scope

The scope of the survey was global, and, as such, encompassed financial institutions with worldwide presence and head office operations in one of the following geographic regions: North America; Europe, Middle East, Africa (EMEA); Asia Pacific (APAC); and Latin America and the Caribbean (LACRO). To promote consistency, and to preserve the value of the answers, the majority of financial institutions were interviewed in their country of headquarters. The strategic focus of financial institutions spanned a variety of sectors, including, Banking, Securities, Insurance and Asset Management. While industry focus was not deemed a crucial criterion in the participant selection process, attributes such as size, global presence and market share were taken into consideration. Due to the diverse focus of institutions surveyed and the qualitative format of our research, the results reported herein may not be representative of each identified region.

## Drafting of the questionnaire

The questionnaire was comprised of questions composed by the global survey team made up of senior Deloitte security services professionals. Questions were selected based on their potential to reflect the most important operating dimensions of a financial

institution's processes or systems in relation to security and privacy. The questions were each tested against global suitability, timeliness, and degree of value. The purpose of the questions was to identify, record, and present the state of information security and privacy in the financial services industry. As this is the third year for the survey, and acknowledging the importance of trend data, various questions were repeated to determine if, and how quickly, participants were reacting to changes in the market environment and how market variables cascaded around the globe. New questions were also added to reflect topics being asked about by Deloitte's clients and written about in the news.

## The collection process

Once the questionnaire was finalized and agreed upon by the survey team, the questionnaires were distributed to the participating regions electronically. Data collection involved gathering both quantitative and qualitative data related to the identified areas. Each participating region assigned responsibility to senior members of their security services practice who were held accountable for obtaining answers from the various financial institutions with whom they had a relationship. Most of the data collection process took place through face-to-face interviews with the Chief Information Security Officer/Chief Security Officer (CISO/CSO) or designate, and in some instances, with the security management team. For the first time, Deloitte offered pre-selected financial institutions the ability to submit answers online using an online questionnaire managed by DeloitteDEX Advisory Services.

## Results analysis and validation

The DeloitteDEX team is responsible for analyzing and validating the data from the survey. DeloitteDEX is a family of proprietary products and processes for diagnostic benchmarking applications. DeloitteDEX Advisory Services, part of the DeloitteDEX team, use a variety of research tools and information databases to provide benchmarking analyses measuring financial and/or operational performance. Deloitte's clients' performance can be measured against that of their peer group(s). The process identifies competitive performance gaps and enables management to learn how to improve the performance of business processes by identifying and adopting leading practices on a company, industry, national or global basis, as appropriate.

Once the DeloitteDEX team received the data, it was arranged by geographic origin of respondents. Some basic measures of dispersion were calculated from the data sets. Some answers to specific questions were not used in calculations to keep the analysis simple and straightforward.

#### **The value of benchmarking**

Financial services providers, now more than ever, recognize the importance of performance measurements and benchmarks in helping them to manage complex systems and processes. The Global Security Survey is intended to enable benchmarking against comparable organizations. Benchmarking can aid in identifying best practices to enhance organizational performance when adapted and implemented in their organization. Benchmarking can often result in recommendations for performance improvements from the benchmarking findings.

**Financial services providers, now more than ever, recognize the importance of performance measurements and benchmarks in helping them manage complex systems and processes.**

#### **Areas covered by the survey**

It is possible that an organization may excel in some areas related to information security, e.g. investment and responsiveness, and fall short in other areas, e.g. value and risk. In order to be able to pinpoint the specific areas that require attention, we chose to group the questions by the following seven aspects of a typical financial services organization's operations and culture:

1. Governance.
  - Compliance, Policy, Accountability, Management Support, Measurement.
2. Investment.
  - Budgeting, Staffing, Management.
3. Value.
  - Management's View, Applications/Uses, Security Infrastructure, Success Measurement, Feedback, Compliance.
4. Risk.
  - Industry Averages, Spending, Intentions, Competition, Public Networks, Controls, Encryption, Software Licensing.
5. Use of security technologies.
  - Technology, Knowledge Base, Trends.
6. Quality of operations.
  - Business Continuity Management, Benchmarking, Administration, Detection, Response, Privileged Users, Authentication, Controls.
7. Privacy.
  - Compliance, Ethics, Data Collection Policies, Communication Techniques, Safeguards, Personal Information Protection.

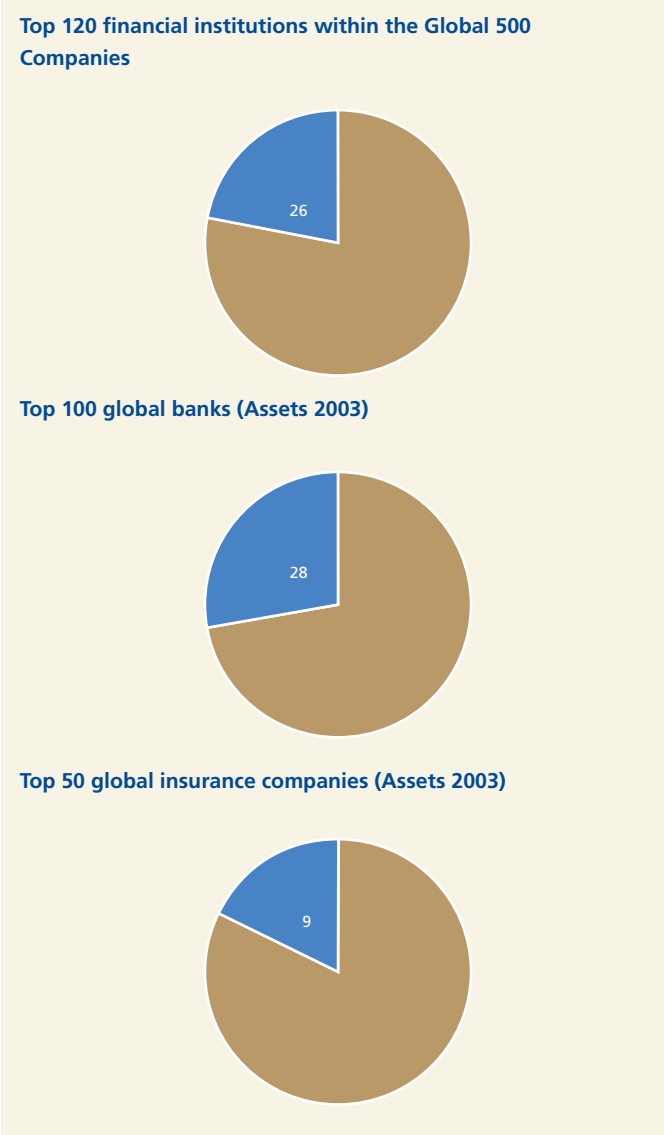
# Who responded

The 2005 Global Security Survey respondent data reflect current trends in security and privacy at a number of major global financial institutions. The final survey sample reflects all major financial sectors (banking, insurance, securities, payments and processors and diversified financial institutions). We agreed to preserve the anonymity of the participants by not identifying their organizations.

However, we can state that, overall, the participants represent:

- 26 of the 120 financial institutions listed within the Global 500 Companies;
- 28 of the top 100 global banks ranked by 2003 tier-1 capital; and
- 9 of the top 50 global insurers ranked by 2003 assets.

**This year’s survey indicates that there are, on average, six IT security professionals for every 1,000 employees.**



**Geographic region**

The survey's pool of respondents provides an excellent cross-section from 26 countries around the world, with a breakdown as follows:

- Europe, the Middle East and Africa: 40%.
- Asia/Pacific: 24%.
- Latin America: 3%.
- North America: 33%.

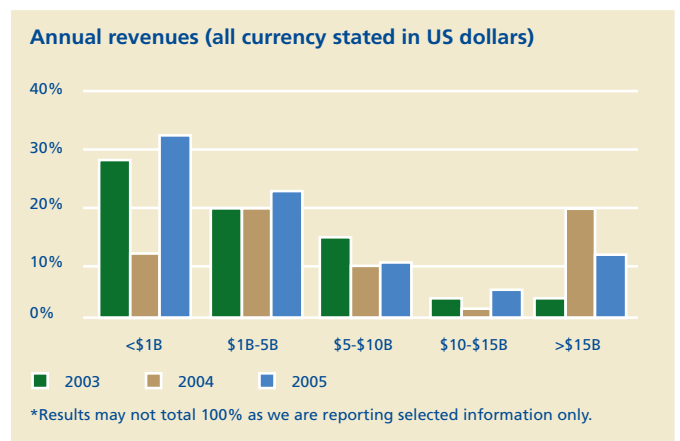
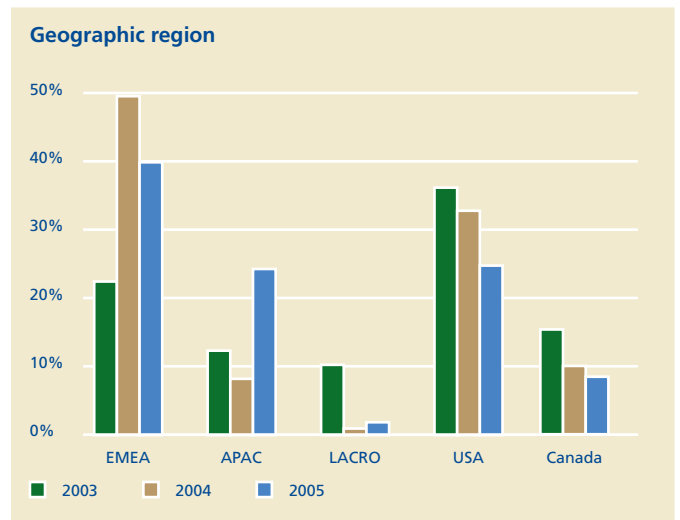
**Industry breakdown**

- Banking: 70%.
- Insurance: 16%.
- Securities: 5%.
- Payment and processors: 3%.
- Other: 6%.

**Annual revenue**

By annual revenue, the participating financial institutions present a broad spectrum:

- <\$1B in annual revenue: 33%.
- \$1B-\$5B in annual revenue: 23%.
- \$5B-\$10B in annual revenue: 11%.
- \$10B-\$15B in annual revenue: 6%.
- >\$15B in annual revenue: 12%.



# Geographic region and industry segmentation observations

Regional highlight	EMEA	APAC	LACRO	Canada	USA
FSIs who feel that security has risen to the C suite or board as a critical area of business	36%	42%	29%	20%	41%
FSIs possessing a security strategy	89%	70%	29%	70%	83%
FSIs whose information security strategy is led and embraced by line and functional business leaders	66%	83%	50%	67%	57%
FSIs who feel they have both the commitment and funding to address regulatory requirements	62%	56%	67%	78%	83%
FSIs who feel that government driven security regulations are effective in improving security posture in their industry	62%	89%	40%	56%	62%
FSIs with a security staff of less than 40 employees	77%	83%	71%	50%	52%
FSIs who have security linked to their IT security employee's appraisals	43%	48%	50%	70%	52%
FSIs who feel they presently have both the required skills and competencies to respond effectively and efficiently	52%	31%	29%	50%	32%
FSIs who have adopted ISO 17799:2000 or achieved BS7799-2:2002 certification	83%	65%	60%	60%	65%
FSIs whose employees have received at least one training and awareness session on security and privacy in the last twelve months	36%	77%	57%	67%	76%
FSIs who have been compromised in the last 12 months	36%	16%	0%	50%	26%

■ Best in class    ■ Worst in class

## Europe, Middle East, and Africa (EMEA)

EMEA is a short acronym for a large, complex section of the globe, home to many of the world's cultures and languages. EMEA likely deals with the bulk of the world's security issues, with North Africa, the Caucasus, the Balkans and the Middle East all in close proximity to one another and all impacting each other's direction, decisions and security measures. In this year's survey – as in the previous two – EMEA has the highest number of financial institutions who have undergone the process of formulating an information security strategy (89%), 6% higher than the US and roughly 30% above all other regions.

A security strategy is only as good as it is perceived to be by stakeholders. Only 66% of respondents who had an information security strategy feel that it is getting the buy-in required. This may help to explain why, for the last two years, EMEA falls near the middle of the pack when it comes to those who feel that

information security is getting the respect it deserves. Thirty six percent of this year's EMEA respondents feel that security has risen to the C suite or board as a critical component to their business, while 50% feel that the responsibility falls primarily within the IT function. As well, further analysis of the survey indicates that executive management is not being briefed in the right areas around compliance and security.

With corporate governance coming to the forefront around the world, EMEA has its work cut out for it. Although the European Union is striving to find a way to standardize corporate governance through formal standards and regulations, many countries are establishing their own, contributing to potential overlap and confusion. Wide-ranging regulation, originating from the international community, is further adding to this confusion, with little evidence of a strategic shift in thinking towards regulation from compliance to business critical issues.

Many organizations in this region accept that either adequate regulation does not exist or that they are not effective in improving the security posture in the industry (62%). This fact may help explain why EMEA has the highest rate of adoption (83%) of security standards (i.e. ISO 17799) and process frameworks (ITIL). However, respondents need to have the right structure in place to do this effectively. The evidence from the survey suggests that many EMEA respondents are well prepared for implementing the continuing flow of regulations. Presently, EMEA respondents have one of the highest levels of skilled, security-savvy professionals, with 52% of respondents citing that they have both the required skills and competencies to respond effectively and efficiently today. However, countries such as South Africa, Slovenia, Spain and Greece indicate that gaps exist in both competencies and skills, leaving them less likely to respond effectively.

### Asia Pacific (APAC)

Asia Pacific is gaining more and more attention due to the size of China's economy and the corporate governance issues arising from the changing of the state-owned commercial banks into joint-stock companies. Estimates of the investment required in corporate risk-management and governance systems within China's major financial institutions are in excess of \$1.2 billion over the next three to five years. This estimate helps to explain why Chinese respondents indicate that governance and regulatory compliance are the top security initiatives for 2005.

As China aggressively targets the lucrative global sourcing software business currently led by India, and as India responds to the growing opportunity and threat from China, interesting outcomes are on the horizon. However, concerns over privacy and security have kept many FSIs from moving data containing sensitive customer information offshore. Distress over the lack of intellectual property laws and high piracy rates in those countries have led businesses to hesitate due to the fact that increased scrutiny of the legal compliance of their information security measures extends to information that is under the control of and processed by a third party outsource provider.

Respondents from the APAC region had the highest number of respondents who indicate that security has risen to the C suite or board and is critical to their business (42%) and 83% indicate that the strategy is led and embraced by line and functional business leaders. This may support the finding that the majority of respondents feel that senior management is well informed with regard to information security threats and performance goals and that metrics were in place to help measure program effectiveness.

Those APAC respondents who have chosen not to outsource their security function find themselves with staff missing the appropriate skills to be effective in their role. This finding may explain why the APAC region, for the second year, was ahead of rest of the world (77%) in having their employees receive awareness and training on security and privacy issues and statutory compliance.

### Country highlight

#### Japan

Respondents in Japan made up a large proportion of this year's APAC population of respondents. It was interesting to compare their responses, both against the rest of the APAC population or among themselves. In Japan, the Chief Information Security Officer (CISO) reports to the highest levels of the organization, with the Board of Directors being the most cited response. This was particularly interesting in view of a response that indicates that Boards are only "somewhat informed" with regard to information security risks and that the majority of reports on information security are generated on an *ad hoc* basis. With privacy compliance being a major driving force for Japanese respondents and heavily impacting their industry, the majority indicate that their CISO is well informed and heavily involved in the compliance process. In terms of skills and competencies, the majority feel that while gaps exist, they are doing what they can to help close them quickly, demonstrated by the fact that over 83% of respondents have conducted a training session in the last 12 months.

Japan is one of the most technologically advanced countries in the world. With the highest adoption and pilot rates of technologies such as biometrics, smart cards and wireless solutions, respondents in Japan still feel that they are not "ground breakers", preferring instead to consider themselves effective and efficient users of demonstrated technology. Further evidence of their advancements are revealed in their adoption rates of security best practices. According to the ISMS International User Group Website ([www.xisec.com](http://www.xisec.com)) they account for 49% of the global number of BS7799-2:2002 registered organizations as of May 2005.

#### Latin America and the Caribbean (LACRO)

LACRO respondents came from Argentina, Brazil, and Bermuda. LACRO supports the theory that smaller financial institutions are less targeted than the ones who draw more attention to themselves. LACRO respondents had the highest percentage of those who feel that management identifies security as an IT risk exercise and there is little value in taking the time to develop a security strategy. For those who have undertaken efforts to formulate one, they still lag well behind in having the strategy accepted and embraced by

line and functional business leaders. LACRO was the only region that experienced no breaches in information security a response that likely does not tell the whole story. With close to 100% never having performed an inventory of personal information and with only 57% tracking loss of data, it would be difficult for any organization to know if a breach has occurred or not, let alone to report on it.

Privacy in the LACRO region appears to be of little concern. A whopping 86% of LACRO respondents have not implemented a program for managing privacy compliance and only 67% have established a written privacy, fair information and data collection policy. Unfortunately, the light at the end of the privacy tunnel is not very bright for the LACRO region, as the majority of organizations intend to spend less than \$50,000 on privacy initiatives for the year.

## North America

### Canada

With former employees trading confidential messages over BlackBerry™ wireless devices and glitches from routine programming updates causing substantial downtime for key systems, Canadian financial institutions did not have a stellar year when it came to adequately protecting their information. In this year's survey, 50% of the respondents acknowledge that they have experienced some form of information security breach and 100% of those experienced at least one internally (arising from malicious employee activities or non-malicious employee errors). In 2004, 60% of respondents felt that their security staff was made up of the right skills sets and competencies, a number which may have been more wishful thinking than fact, given the number of breaches. This year, that number slipped to 50%. It is interesting to note that, even with all the press coverage of Canadian financial industry institutions, the majority of respondents feel that their Boards and CEOs are, at best, "somewhat informed" regarding information security risks.

But it is not all bad news for Canadian financial institutions. They remain in the middle of the pack when it comes to possessing an information security strategy (70%); however, only 67% feel that it has been embraced by line and functional business leaders. With Privacy and Sarbanes Oxley (SOX) compliance being key regulatory initiatives, it is comforting to know that the majority of respondents (78%) have both the commitment and funding required to address them accordingly.

A full 100% of respondents indicate that having a risk management strategy in place is either "very important" or "extremely important". Canadian CISOs need to continue to face the challenge of directing technology, policies, procedures and people toward a common security posture while ensuring that the needs of the organization are being met.

### United States of America

With some of the largest financial institutions and security staff in the world, it was not surprising that the US had a strong showing in many categories for the second year in a row. Over half of the US respondents felt that security provided their organization with a competitive advantage, 41% felt that security has surfaced to the C suite or board as a critical area of business and 83% had undertaken the process to formulate an information security strategy. Over a quarter of respondents have chosen to outsource a component of their security function while 32% of those who have not feel they have the right skills and competencies to perform those functions effectively.

With integrity, risk management, and regulatory compliance bringing added pressures, US financial institutions have named governance and compliance as their strategic areas of focus for 2005. Corporate scandals and resulting legislation have tightened the focus of management on regulatory compliance and corporate governance. Regulations such as Sarbanes-Oxley, and Gramm Leach Bliley have affected processes around accountability, disclosure, protection of personal privacy information and integrity of reported information. One tangible impact of the renewed visibility of risk governance is the increased involvement of the board in risk oversight. Ninety three per cent of respondents feel that their Boards of Directors are "somewhat informed" and 97% feel that their CEOs are "somewhat informed" about information security risks affecting the organization.

The US financial institutions suffered their share of media coverage surrounding security breaches. Several security breaches involving the loss or disclosure of personal and confidential information were reported over the last twelve months. Class action lawsuits have been brought against a large North American financial institution, whose computer data tapes containing information about 1.2 million federal employees were lost, and an organization that was deceived into granting access, by 50 fictitious businesses, to 145,000 consumer data profiles. These high-profile breaches have resulted in strong pressure for enhanced corporate legal obligations to ensure appropriate information security measures.



# Key findings of the survey

## 1. Managing compliance now relies on input from multiple stakeholders including technology and security

Financial institutions today face the challenge of ever-increasing regulation. While regulation rarely deals directly with an enterprise's use of IT, regulation does increasingly affect IT systems. In some areas, particularly privacy and finance, regulation significantly impacts the use of IT. As a result, the security staff will need to work with the general counsel to identify how the organization can best comply with regulation. For this collaboration to be effective, understanding and leveragability are crucial. In many instances, similar mechanisms and controls are required in order to meet different regulations and standards of good practice. However, because each area may have its own individual requirements for auditing and reporting, a strong understanding of the regulation by all stakeholders is key.

Of the respondents interviewed, only 17% overall deem government security-driven regulations as "very effective" and 50% "effective" in improving their organization's security position or in reducing data protection risks. Only 37% feel that such activities are leading to a sustainable and effective solution.

Responsibility for managing compliance is moving away from being the sole responsibility of the legal department to being shared among the various functions, such as IT and finance.

The objective of compliance should be to meet the requirements of regulation in as effective a manner as possible. This often requires an understanding of how one regulatory requirement may relate to another and how best to meet differing and often inconsistent regulatory requirements around the world.

Compliance is a time-consuming and ongoing exercise that, given the times in which we live, shows no signs of retreating. Organizations that embrace the elements and essence of compliance may be able to re-energize themselves and provide reassurance to their investors.

## 2. Organizations need to be prepared for the changing nature of threats

Survey respondents today must be prepared for a range of risks, previously unheard of. Natural disasters, such as the tsunami in December of 2004, political risks, de-globalization, counterfeiting, pharming, and the spread of infectious diseases are but a small selection of the external risks that have to be considered by survey respondents in all parts of the world today. Poor new-hire screening processes, lackadaisical subcontractor controls, security-ignorant employees and deficient management processes are all examples of internal vulnerabilities that allow many of today's security breaches to occur. Internal or external, by themselves or together, these risks have the potential to bring down the largest and strongest of companies by wreaking havoc on shareholder value. These risks have prompted new legislation, new regulations, and a whole new set of business and customer requirements.

Respondents to this year's survey point to a host of continuing challenges to their business. Chief among them are the increasing sophistication of threats (63%) and the lack of employee awareness and training (48%), both of which may create an environment of exploitable vulnerabilities and weak operational practices. It is clear why executives consistently cite risk management as the most important reason for investing in security.

Although the majority of organizations are confident that they have adequately protected themselves from internal and external attacks, many of their investments in technology are undermined by process flaws. Examples abound throughout the survey results: 33% of respondents acknowledge that they have done nothing to protect themselves from internal wireless communication exposures, and only 38% run scans to identify rogue wireless networks. Of the 74% of respondents who have chosen to outsource at least one function, only 73% have conducted regular assessments of the security outsourcer's compliance with the respondent's information security requirements. With identity theft spinning out of control, and so many respondents concerned with the lack of employee awareness, it is troubling that only 65% of organizations have trained their employees on how to identify and report suspicious activity.

Respondents rate their top perceived threats over the next 12 months to be worms, viruses, spam attacks, spyware and financial fraud (i.e. phishing and pharming). Phishing attacks have sky rocketed and outfoxed the “good guys” as they become more mature and harder to detect.

Pharming attacks, which do not rely on a legitimate looking email to lure users to illegitimate websites, are on the increase. Pharming techniques plant malicious code on vulnerable systems, and then modify the PC’s host files to point to fraudulent rather than legitimate sites.

In order for an organization to be in a position to provide effective information security, it must first have a clear focus on what it is seeking to protect and the corresponding threats. An understanding of these threats will dictate the processes and security technologies that will adequately protect, and be flexible enough to change with, the respondent’s operating environment.

It is clear from examining the responses regarding technologies deployed that many respondents appear to be responding at a tactical level: anti-virus protections (98%); VPNs (79%) and IDS (69%) – providing a “layered” defense. However, the fragmentation of security products and their lack of interoperability are proving to be additional security challenges. Integrating a layered defense is difficult, as vendors’ products do not always live up to their claims and respondents’ environments do not necessarily mimic those of the vendors’ design labs. Some organizations look at developing an information security program or leveraging better practice frameworks, such as ISO 17799. Such practices allow the organization to transition from perimeter security to in-depth defence. Organizations are also being forced to build security into all aspects of their business (hiring processes, physical security, applications, governance, etc.) to help the organization properly manage risk and allow it to be resilient and adaptable in the face of ever-changing threat.

Organizations, and their CISOs, need to do a better job of communicating the objectives and the value of their security program to the organization. They need to clearly understand the threats and vulnerabilities of their environment, not only to mitigate damage but to take advantage of the business opportunities that may be presented.

### **3. While the number of overall security breaches is down, geography and stature of the organization play a key role in whether an organization’s security will be breached**

In 2004, 83% of respondents acknowledged that their systems had been compromised in some way over the last year. This year, the number was closer to 30%, with 35% occurring from inside and 39% occurring from both inside and outside. Although the total number of respondents who experienced a security breach over the last twelve months fell significantly, geography and size appear to have a strong influence on findings. For example, successful external security breaches were less likely in small organizations – less than 5,000 employees – a fact that supports the theory that larger organizations are the targets of choice due to the wealth of personal information and monetary assets under their control. In the past, security attacks were more common on smaller, less protected institutions but as attacks begin to focus more on weak operational practices rather than on technology, the larger institutions are far more attractive to hackers in terms of the ultimate rewards.

Geography also appears to play a role in the number of security breaches an organization experiences. Respondents in LACRO and in Japan shared the least number of successful breaches. However, the fact that a security breach is not known to have occurred or has not been reported does not establish the effectiveness of a respondent’s security program. Past surveys have shown that organizations may not have been aware of a breach and, therefore, cannot report it. In addition, an organization may choose not to disclose security breaches for fear of tarnishing its reputation.

In North America, the incidents of security breaches increased or stayed relatively the same as last year. In Canada, breaches increased by 6% to 50% of respondents, while the US stayed relatively consistent with a 1% increase to 25%.

It is clear that many security breaches are the result of human error or negligence resulting from weak operational practices. As any experienced hacker – ethical or criminal – will attest, it is more effective to focus on people errors and poor security practices than it is to try to crack today’s sophisticated technology solutions. With deliberate and widespread attacks in the form of phishing, pharming and fraudulent web sites, it is clear why CISOs are attempting to create a security-aware organization, rather than relying solely on the security function and technology to do the job.

#### 4. There is a trend toward having the Chief Information Security Officer (CISO) report to the highest levels within the organization

For the 81% of organizations who employ a CISO, 86% indicate that this function reports directly to the board or to the C suite level. Deloitte's analysis shows that a respondent's appetite for risk, as well as culture and geography, influence the job description of the CISO. The CISO's activities and responsibilities vary greatly among respondents. A high proportion of respondents indicate that the majority of the CISO's time is spent in security strategy and management. The remainder of respondents indicate that the CISO is involved in less strategic work, with a focus in the areas of security administration and corporate implementation.

Obviously, the decision as to where the CISO position falls within the organizational structure has a strong impact on that person's perceived authority and control. Therefore, there is a direct correlation between the importance an organization places on its protection of information and the stature of the CISO role within the organizational hierarchy.

Based on the survey results, it is evident that no matter where the CISO role fits in the hierarchy or who it reports to or how big or how small the information security function is in terms of resources, the CISO participates in a vast number of groups or committees covering a diverse array of functions made up of various stakeholders (i.e. IT Committee, Risk Committee, and Privacy Committee). However, the majority (59%) of respondents feel that management still views information security as purely a risk management exercise and not an area essential to the business. With so many functions beginning to worry about the protection of their information, there is a need to integrate this protection across the organization, an undertaking that requires a high degree of coordination and control.

What these results appear to indicate is that, although progress has been made, the role of the CISO is still evolving. It is clear that further development is required to help dispel the myth that security is purely a technology problem and to demonstrate that security can be aligned with business objectives, if a connection exists between the different viewpoints of IT and the business.

The degree to which an organization is considered secure often hinges upon the effectiveness of collaboration between interested stakeholders. In today's operating environment, good information security requires a multifaceted approach, supported by a culture

that is proactive in terms of understanding and responding to business requirements. The job description of the CISO is evolving into a complex and challenging role. It now requires effective decision-making concerning risk. It requires the ability to understand and co-ordinate the different requirements of the affected parties, a task that grows more complex as the number of parties grows to include the CEO, COO, heads of business units, the CFO, internal and external auditors, affected internal functions (HR, legal etc.), physical security, IT and employees themselves. The increasingly challenging mandate of the CISO requires that person to expand his or her horizons beyond the traditional. As organizations continue to look to the CISO as a champion of information security, the CISO will need to thoroughly understand the business and technical issues involved. Only then will the CISO be in a position to demonstrate his or her influence on the organization by making effective decisions around technology implementations, policies and processes, and people.

#### 5. The board's interest in security is no longer optional; it is a requirement

The trend is clear and its implications for the financial services industry are significant: if organizations do not take action to adequately protect their customers' information, the result will be lack of trust, tarnished reputation, decreasing shareholder value, financial retribution and, possibly, criminal charges, such as imprisonment for senior executives. Regulators will further react – with the introduction of tighter regulation and compliance efforts.

Security of information is a major concern for all corporate stakeholders. There is an increasing understanding by boards that taking the appropriate steps to ensure security of information is a requirement. Boards of directors need to understand whether management has plans in place – and is delivering on those plans – to secure the organization's people, facilities, and information in the event of an incident. As corporate scandals and security breaches lead to increased legislation and regulation, boards continue to focus their attention on regulatory compliance, corporate governance and behaving ethically. One of the benefits of this environment is the renewed focus on risk governance and the increasing involvement of the board in risk oversight. A full 86% of respondents indicate that the board of directors has knowledge of the risks associated with the organization. Today's boards should be taken through a regular exercise to inform them of the organization's key assets, the risks associated with those assets, and the benefits and criticality of ensuring those assets are secured.

It is clear that the days of the executive team sitting passively by while the IT people deal with security are gone.

#### **6. The most effective way to cost justify the security function is to assess the value and impact delivered to the business**

Although only 30% of respondents indicate that their security projects fail “some of the time”, the biggest cause of these failures is lack of buy-in from the business owners. These results support the fact that 54% of respondents feel that strategic and technological alignment in relation to security is only “somewhat aligned”, if at all. Security funding needs to be directed to projects that support the needs of the business. In North America, this money needs to go to further protecting and educating people within organizations. One way to address proper alignment is to have the CISO act as a liaison between IT and the business units so that business requirements can be effectively assessed.

Although the majority of respondents are still doing poorly at measuring performance – if they are attempting it at all – the ones that do measure performance appear to be focusing more on cost and returns as opposed to the value the security provides the organization. Evaluating security projects in terms of the value and impact delivered to the business and identifying a language that both security and IT people can talk, will not only help the security function achieve greater recognition but will also result in projects that will become more aligned with the needs of the business.

New legislation, regulations and lawsuits have all led to a rise in security spending over the last few years, primarily in the areas of compliance and technological investments. New technology purchases and implementation, higher insurance premiums, the reconfiguration of procedures, the addition of people, and an increase in the purchase of professional services – the costs are enormous. As a result, respondents have smaller budgets, time and resources for new investments and emerging technologies, evident by the small number of new technologies being deployed or piloted.

#### **7. Identity and vulnerability management: The role of these solutions in the compliance world is increasing**

For the second year, spending on identity management and vulnerability management solutions is on the rise. In today's environment, compliance with regulations such as SOX and various country-specific privacy legislation are a top priority for respondents, who demand improved controls over users' access and management. Identity management entails a combination of services from provisioning of user I.D.s, access control authorization, and authentication controls linked to offer a robust solution to help provide simplified, automated and auditable controls over users' identities.

While identity management is not the single solution for compliance, it does play a major role in helping an organization with their compliance efforts. As much of the new regulation involves the protection of personal, customer and financial information and their respective internal controls, organizations turn to IT in their internal control efforts. An identity management solution which includes provisioning and access services helps an organization enforce access management and integrity over information and automates the processes for the creation, management and dissemination of such information. In terms of privacy legislation, the 80-20 rule appears to apply: 80% of all privacy legislation requires the same kinds of controls while the other 20% require further modification to help meet local privacy requirements. Therefore, by implementing an identity management solution where business processes are in line with stated business requirements, an organization will be in a better and more sustainable position to comply with control objectives and privacy compliance.

For the second consecutive year, respondents are worried by the increase in the number of worms, viruses, Trojan horses and malicious code that they need to deal with on a daily basis. Such threats exploit organizational vulnerabilities caused by weak

processes and/or technologies as many of the risks associated with such threats arise from the misalignment of technology, people and processes, as well as the lack of end-to-end enterprise-wide co-ordinated processes and procedures to effectively respond to an incident with the appropriate resolution process, one that guides the security operations team through the process of containing and eliminating threats and addressing the issue. With the majority of respondents indicating that security is a vital component of their risk management strategy, many are attempting to develop a vulnerability management process that will help protect them from the internal and external threats to which they are subjected while, at the same time, achieving compliance with applicable laws and regulations.

The process of effectively managing vulnerabilities will take into account (1) the people, processes and technologies required to establish and maintain a security configuration baseline, (2) the logging, monitoring and reporting of events required to perform the consolidated and correlative analysis to proactively monitor for policy violations, (3) a process to notify the right people when serious violations occur, and (4) a process to identify and prioritize attack activity and possible exposures. Such a vulnerability management process will help the organization extract intelligent, actionable information out of disparate security and application logs from the various information systems. By doing so, it will provide the organization with valuable insight into security events and allow it to generate reports that normalize and detail the events and associated vulnerabilities for compliance and auditing activities, helping security specialists isolate security events that could cause the organization to be non-compliant.

### **8. Training and awareness are crucial – yet underutilized – contributors to employee vigilance surrounding an organization's security function**

Human performance is a function of ability, motivation and environment. Only 65% of organizations have trained their employees on how to identify and report suspicious activity. Many (64%) are slowly increasing security training and awareness programs, with methods ranging from classroom settings (32%) to posters (20%) to information on web sites (42%) to Lunch & Learns (18%). Regardless, these programs are only effective if people feel motivated by the overall security objective.

Organizations must introduce and maintain “motivators” to help their people be ever-vigilant about the security function. Motivators can be both positive and negative – recognition programs as well as penalties and dismissals. The CISO or the functions responsible for security awareness and training must develop a good understanding of their people and culture.

Only 6% of respondents provide any education or awareness as part of the new hire orientation. For many, the only awareness they get is assimilated over time on the job but by that time, bad habits may have become ingrained. An organization must develop an environment suitable and conducive to improving awareness and changing bad habits. This requires needs assessments, developing the required awareness programs and supporting messages with consistent policies, procedures and technical infrastructure.

As the CISO becomes more adept at working with the different functions within the organization to understand their business requirements, he or she can then establish the right mix of security, developing and implementing strong business processes and effective technologies to help mitigate the effects of security breaches.



# Governance

The position of the Chief Information Security Officer (CISO) continues to gain importance – both in terms of the number of institutions who have established the position as well as its status within the respondents’ hierarchy.

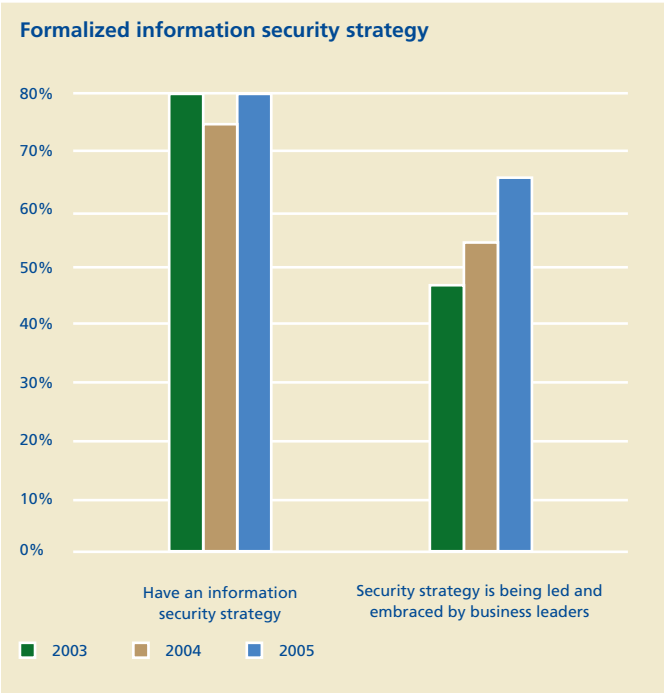
This year, 81% of the institutions surveyed have established the role of the CISO and tenure still sits within the three to five year range (43%). Eighty six per cent of respondents with a CISO indicate that the CISO reports directly to the board of directors or the C suite, with the highest proportion (28%) reporting directly to the CIO. The reason for this increase over last year’s results may be due, in part, to the need for CISOs to continue to expand their responsibilities and work more closely with the infrastructure and business lines to help them understand the importance of aligning security projects with business requirements.

**Tenure of CISOs:**

- 28% have a tenure up to two years.
- 43% have a tenure from 3-5 years.
- 13% have a tenure from 6-10 years.
- 16% have a tenure greater than 11 years.

Even in organizations where the role of the CISO is established and where the CISO reports to either the board or the C suite, security remains largely a function of IT (42%). Only about one third of the organizations interviewed feel that security has risen to the C suite and board levels as a critical area of the business.

What these results may indicate is that although there has been some change in the thinking, the role of the CISO is still in its infancy. Clearly, further development is needed to help dispel the myth that security is purely a technology problem and to demonstrate that security can be aligned with business objectives.



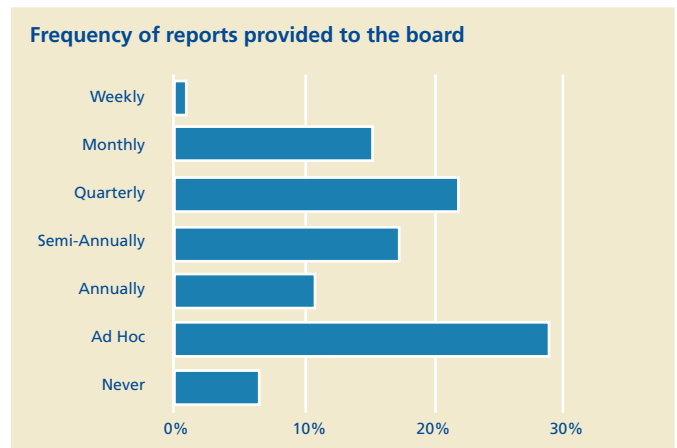
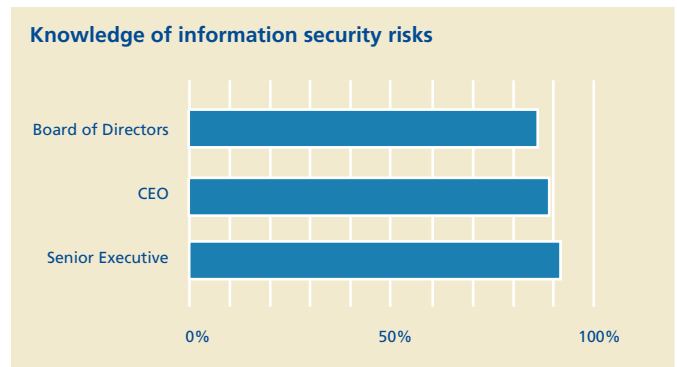
The number of financial institutions who are formulating information security strategies continues to rise – this year, 80% acknowledge that they have undergone the process. However, without involving the right parties in the process, the security strategy will likely miss the mark and leave the organization’s assets prone to risk. As advancements are made in the areas of the role of the CISO and communication between business areas and IT, the numbers continue to improve – 66% of respondents feel that their strategy was led and embraced by its functional and line managers compared to 47% in 2003 and 54% in 2004.

The level of understanding of security risks is permeating higher and higher levels within the organizational structure. Last year, middle level to senior management ranks had the preponderance of understanding of security risks; this year, outside of the IT function, the greater knowledge is attributed to senior management and the board. No longer can the executive team wait passively for evidence that security is insufficient. Now they demand to be more involved of the process of risk identification and to receive continuous feedback on security program performance. For example:

- 86% of respondents indicate that the board of directors have knowledge of security risks.
- 89% of respondents indicate that the CEO has knowledge of security risks.
- 92% of respondents indicate that the senior executive team has knowledge of security risks.

As information security becomes more mainstream and makes its way into the media, the impact of security breaches piques the attention of boards. Of respondents whose CISO reports directly to the board or to the C suite, 82% reported that their boards have a clear view of the organization’s major security investments from a risk and return point of view. Only 18% of respondents whose CISO reports lower than the C suite feel that their boards share this same understanding.

The frequency with which boards are provided a report of the status of information security risks and incidents, however, is still poorly defined. Only 38% of respondents provide such reports either quarterly or semi-annually and 34% of organizations indicate these reports are non-existent or *ad hoc* at best.



Security staff practices have shown some improvement over the last year as 89% of respondents indicate that job roles and responsibilities have been documented and communicated to their IT security staff.

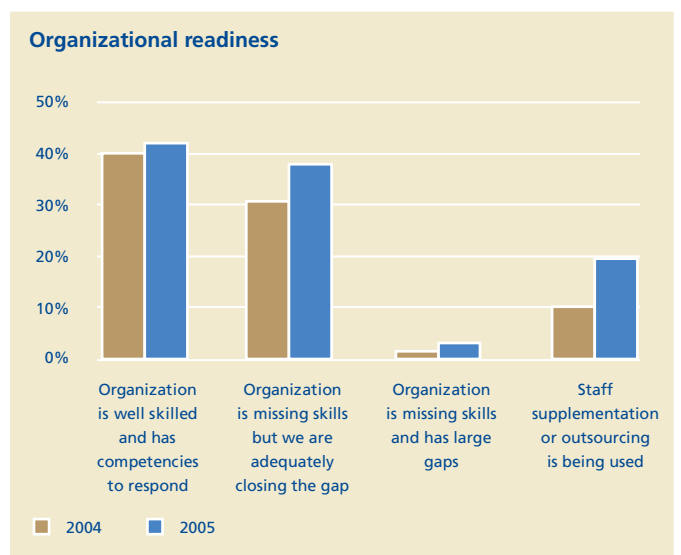
When it comes to security linked to the appraisals of IT security staff:

- Security is linked to IT/Security staff: 50% compared to last year's 28%.
- Security is not linked to IT/Security staff: 50% compared to last year's 72%.

Metrics and measurements are an important part of the security program as they provide a means to measure the effectiveness of the program. Performance measurement of information security still remains relatively low – 35% of organizations indicate they do not currently track and measure the success of their security investments and only 34% acknowledge that they measure them consistently. Of those who track and measure investments, 33% feel that, based on the feedback they receive, the security function is effective in meeting the needs of the business, while 53% feel that they are at least "somewhat effective". The "somewhat effective" response may be explained by the fact that 46% still feel that they identify and measure the wrong indicators of performance. Therefore, metrics must be developed to measure progress toward the goals of the organization with regard to security and feedback mechanisms established to allow for continual assessment and readjustment.

Sufficient and security-savvy resources must be available to an organization so that staff do not become overloaded and less effective. Although technology purchases may be on the rise, technology does not always replace man power and it cannot replace thinking and experience. As with last year, the majority (78%) of the organizations surveyed still feel that they either have, or are quickly closing the gap on, the right set of skilled and competent security professionals. This finding is consistent with the high confidence levels of respondents when asked about their ability to protect themselves from internal and external attacks.

As corporate governance continues to be front page news, and the need for a security strategy aligned with IT's goals and corporate objectives continues to be discussed, the majority (67%) of respondents indicate that senior management continues to commit the required funding and support to appropriately address regulatory and legal requirements.

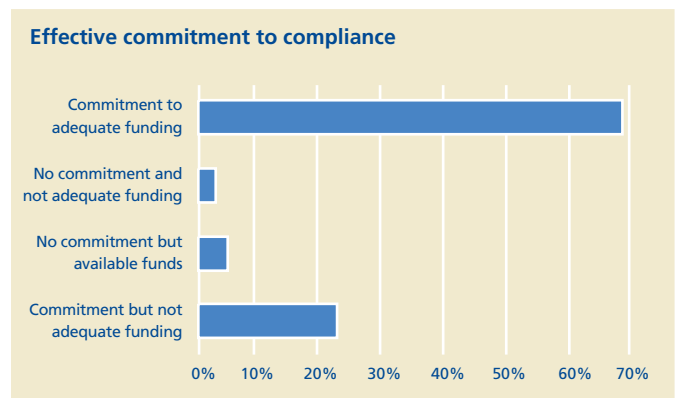
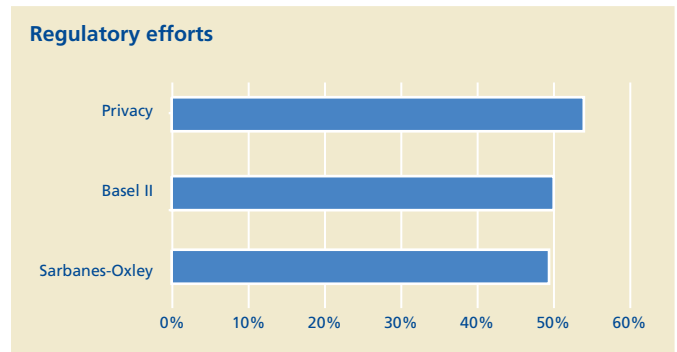


However, the purpose of governance is to enable the organization to meet and exceed regulatory, social and ethical requirements to ultimately enhance shareholder value – a goal that is more easily attained if a security strategy is aligned with the goals of the organization.

Respondents are continually challenged by regulatory compliance. Ninety percent of respondents indicate that government security-driven regulations are either “somewhat” or “considerably” impacting their industry and organization. Privacy and Basel II (46% and 42% respectively) were the most-cited regulatory initiatives impacting the industry with SOX close behind at 41%. By region, the most cited regulatory initiatives are:

- LACRO – SOX, 80%.
- EMEA – Basel II, 73%.
- APAC – Privacy, 45%.
- USA – SOX, 83%.
- Canada – Privacy, 70%.

The size of respondents’ organizations (number of employees) did not seem to have a significant impact on the estimated amount of time spent on information security-related regulatory matters. Although a full 80% of organizations felt that this time would increase over the next twelve months, only 37% of respondents felt that time spent is leading to sustainable and effective solutions within their organization. Seventy-one percent of respondents indicate that they either have no tools or only partially implemented tools to help monitor and measure the effectiveness of their compliance program.



**“The BS7799 certification not only demonstrated our operational security capabilities, it also enabled us to effectively manage security policy and practice in a sustainable environment”.**

– Survey Respondent

# Investment in security

Forty-seven percent of respondents indicate that IT security spending for 2005 hovers around 3% of the total IT budget – a finding that mirrors last year's. Twenty-nine percent of respondents indicate that this number is in the 4%-6% range, while 23% indicate that it is 7% or greater. When respondents were asked what percentage they feel would be optimal to protect the organization, the number was closer to 6%. Due possibly to the increase of awareness by the board, security budgets increased over those of last year, with the majority (43%) increasing by up to 5%. Nineteen percent of respondents indicate an increase of greater than 20% over 2004.

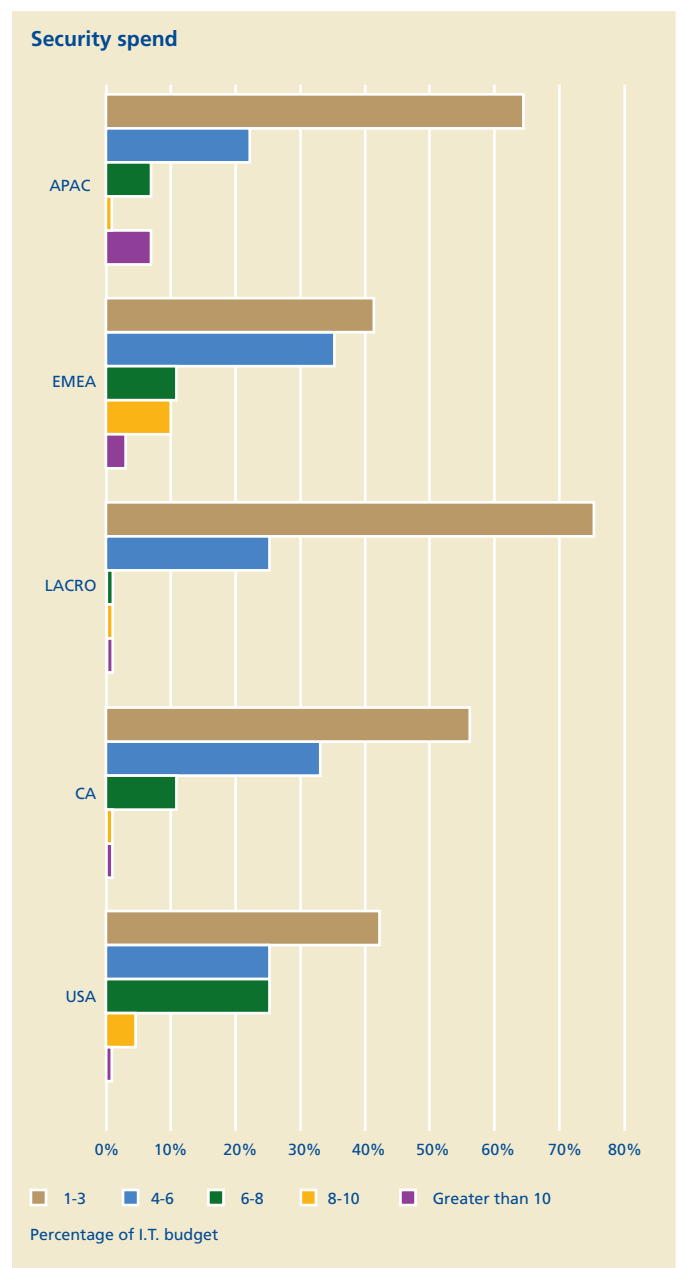
Last year, the majority of respondents indicate that they would characterize their spending on information security as being "in line" with comparable organizations. This year, respondents appear to have less of an idea of what other organizations are spending, as wider variations exist between them.

With increased internal awareness and more organizations attempting to measure security investments, 55% of respondents indicate that security projects do not often fail to deliver what they promise. However, 30% still feel that they fail to deliver "very often" to "somewhat often" with the most common reasons being: lack of buy-in from the business owners (34%); integration problems due to poor up-front design and architecture (48%); or unrealistic timelines and budgets (56%).

However, even with these challenges, 46% of respondents feel that the average overrun is still under 10% of the security operational budget.

What comprises the majority of respondent's security budgets for 2005? The following were identified:

- Logical access control products – 72%.
- Infrastructure protection devices – 67%.
- Security consultants – 64%.
- Hardware and infrastructure – 55%.
- Audit or certification costs – 46%.
- Physical Access Control devices – 31%.



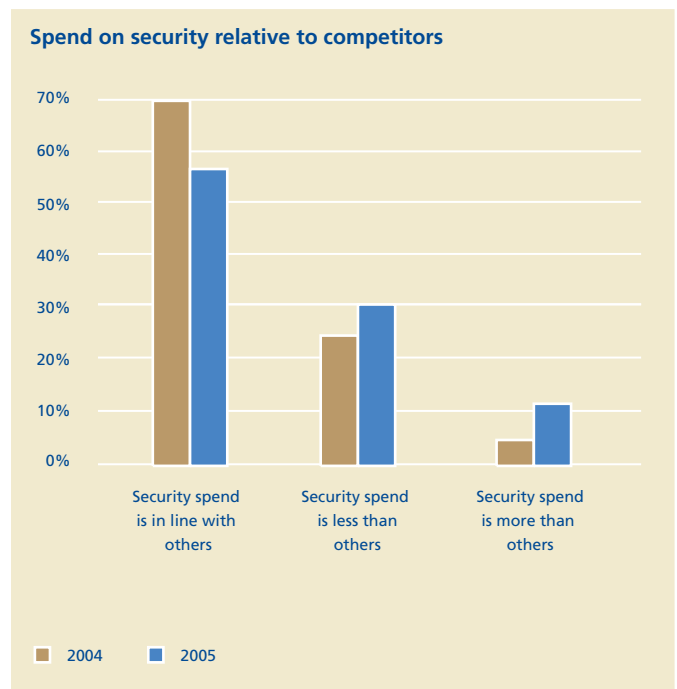
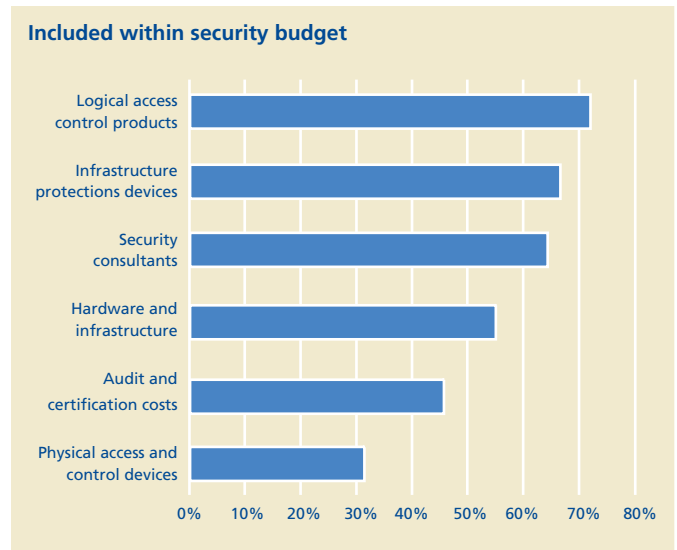
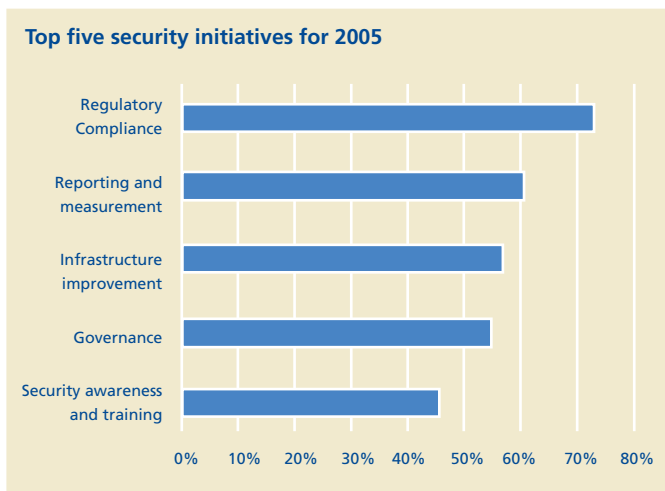
To gain a better understanding of how purchasing decisions are made, respondents indicate that cost and service were the primary influencers when it came time to select a product:

- Total cost of ownership – 98%.
- Service and support – 77%.
- Product build architecture – 26%.

Topping the list of security initiatives for 2005 was regulatory compliance followed closely by improving processes and mechanisms for reporting and measurement. Respondents also place importance on improving and consolidating their IT infrastructures.

Investments are aligned with the top security initiatives for the year. The greatest investments are in the following areas:

- Security tools – 64%.
- Process improvement – 29%.
- Consulting – 28%.
- Employee awareness and training – 15%.

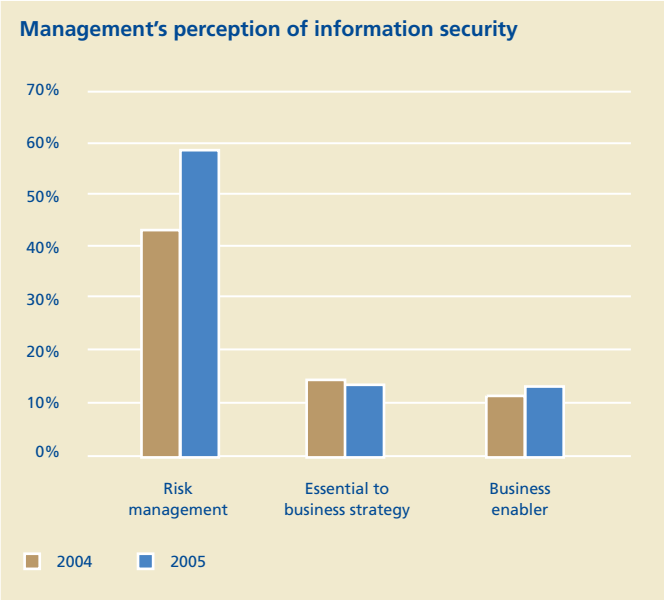


# Value

Although in most organizations, management still views information security as a risk management exercise (59%) there was a slight increase in the number who view it as a “business enabler” (13%).

Appreciation by the business unit leaders regarding information security was in between “somewhat appreciated” (82%) and “highly appreciated” (18%). Of respondents who feel they are effective in terms of meeting the needs of the business based on internal measures, 73% acknowledge that their board remains highly informed regarding their decisions and the state of information security risks. Through greater communication between the various parties, business requirements for security are focused on delivering appropriate – not excessive – security.

**Forty-nine percent of respondents acknowledged that a secure IT environment gives them a competitive advantage over the competition.**



# Risk

In 2003, 39% of respondents indicated that they had experienced some form of security breach within the last 12 months. In 2004, this number increased to 83%, with the majority of breaches occurring from the outside. This year, the number drops to 28% of respondents, with the majority of attacks taking place inside the walls of respondents' organizations.

The huge difference between the last two years begged further analysis. We identified the following:

- Almost 70% of respondents that claim not to have experienced a security breach have less than 5000 employees.
- Similarly, 65% of the companies that claim not to have experienced a security breach have less than 20 IT security professionals.
- The average number of IT security professionals in respondents who indicate they have not been breached is 4.8 Full-Time Equivalents (FTEs); the same average number of IT security professionals for respondents who have been breached is closer to 50 FTEs.

This further analysis indicates one of two factors or a combination of these factors: small organizations are not being targeted as frequently as larger organizations; or the ability of small organizations to identify and cope with the incidents is questionable.

Regional differences exist as well. Further analysis indicates that:

- The number of Canadian respondents who experienced a breach actually increased by 6% to 50%.
- US respondents experienced a slight increase of 1% – 25% of respondents questioned experienced some form of breach.
- Respondents located within EMEA who indicate they have been breached decreased to 35%.

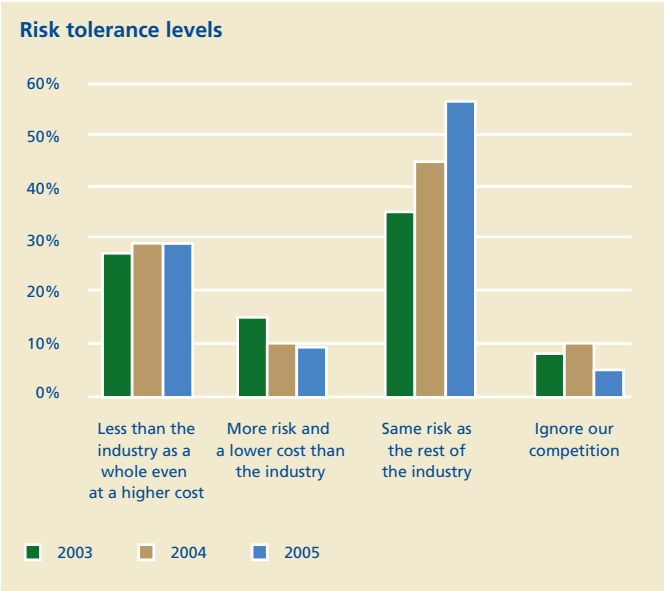
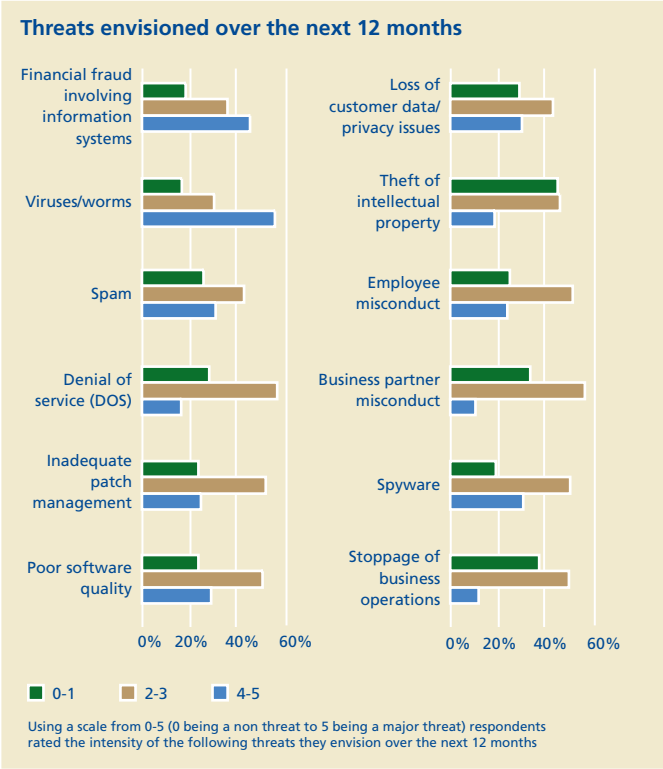
- The respondents who indicate that they did not experience a breach were the highest in the LACRO region with 100% (compared to 50% last year) and the Asia Pacific region 84% (compared to last year's 71%).

In addition to these findings, respondents who experienced a breach had a higher-than-expected response to threats compared to organizations that did not experience a breach over the last twelve months. This finding indicates that respondents who reported no breach actually underestimated their exposure to security risk.

Other interesting facts include:

- 26% report attacks from an external source, compared to 2004 (23%) and 2003 (16%).
- 35% report attacks from an internal source, compared to 2004 (14%) and 2003 (10%).
- 39% report attacks from both sources, compared to 2004 (51%) and 2003 (13%).
- 80% of those who experienced a breach incurred a financial loss of less than \$1 million USD.
- 38% of respondents who did not experience a breach claim that their organization is equipped with the right skills and that they have all the required competencies to respond effectively and efficiently, compared to the 50% who were breached.

An increasing number of respondents who are seeking high performance capabilities depend on their information systems for high value business outcomes; however, these systems are now under unprecedented attack.



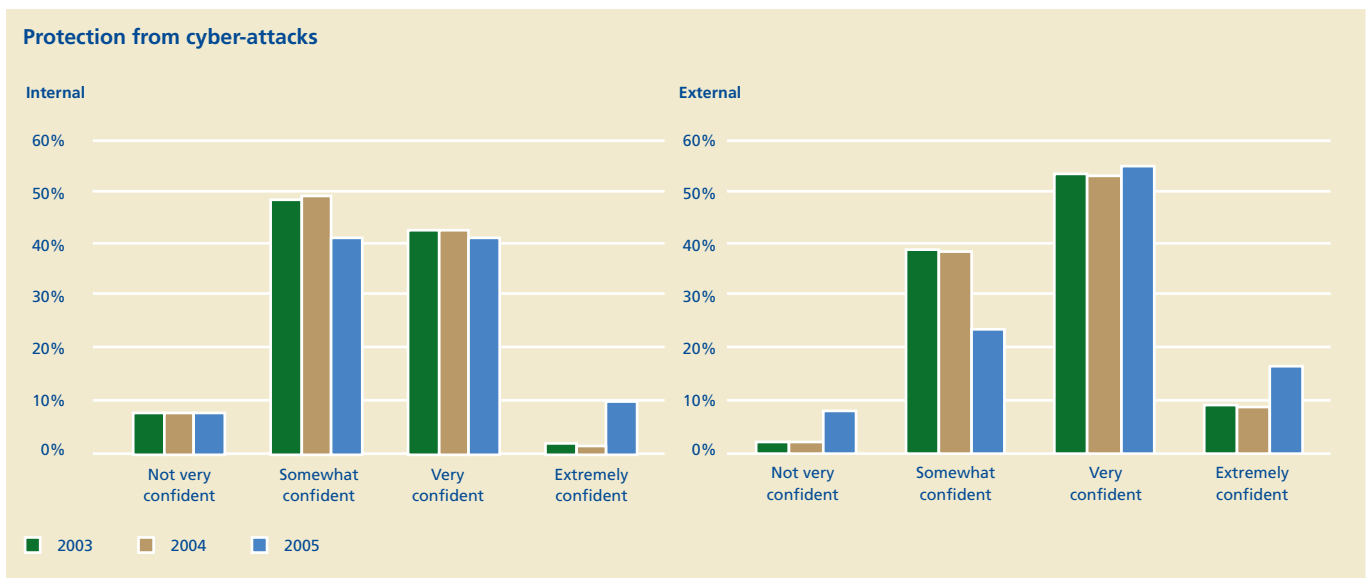
For the third consecutive year, respondents rely on the risk tolerance levels of their competitors. However, this year's respondents are willing to forgo protection and comfort for cost as those who once ignored the competition are starting to look over their shoulder to see what their neighbors are up to.

Respondents can proactively address risk by embedding risk management in processes and taking a pragmatic view of the overall infrastructure. Similar to last year, 91% of respondents indicate that having a risk management process within their organization was either "very important" or "extremely important" and 77% indicate that risk management is part of their strategic planning exercise.

Only 7% of respondents indicate that they do not use a formal risk assessment methodology, with the majority of organizations indicating that they rely on qualitative measures (74%) and measures conducted annually (26%).

Supporting this finding:

- 57% take the same risk as the industry, compared to 45% last year and 35% in 2003.
- 9% take more risk and have a lower cost than the industry, compared to 10% last year and 15% in 2003.
- 29% take less risk than the industry as a whole, even at a higher cost, compared to 29% last year and 27% in 2003.
- 5% ignore the competition, compared to 10% last year and 8% in 2003.



Similar to the responses of the last two years, 82% of respondents are either “very confident” or “somewhat confident” in their networks being protected from internal attacks. This finding is interesting considering that the majority of breaches occurring in 2005 stemmed from inside the organization. However, when it comes to confidence levels relating to external attacks, the number and the attitudes change. This year, 53% of respondents indicate that they are “very confident” in the protection of their systems and 16% are “extremely confident”. What this may show is that organizations need to start to increase their spending in efforts to improve the protection inside the walls of their organization.

Institutions are increasingly re-examining their overall security postures and re-evaluating their level of risk tolerance. With regulation deadlines constantly looming and pressure to protect the organization’s assets, 66% of respondents indicate they have conducted, or are in the process of conducting, a full physical audit of their assets, both hardware and software. Before a security strategy can be developed, organizations need to know their assets, their value and where they are located. Of those who have identified their assets, 66% have classified their critical IT business assets in terms of value to risk and 91% feel that their organization’s IT assets have been appropriately protected.

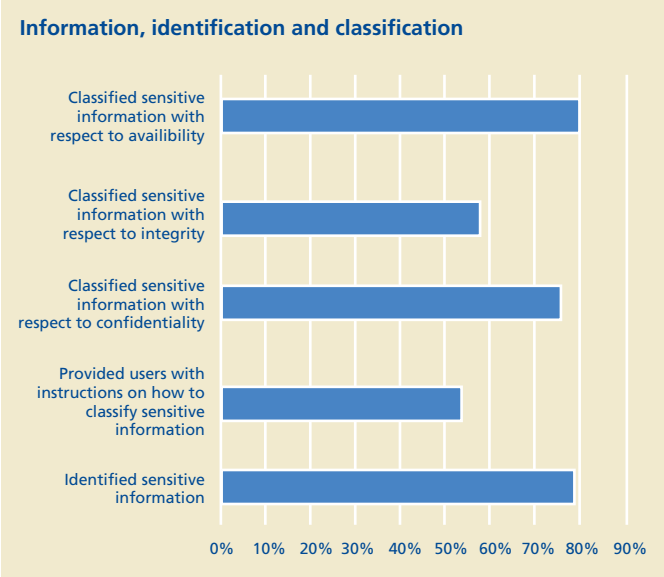
Classification of assets should take into account the information and the capabilities associated with the assets. With respect to information classification for this year’s survey, the breakdown is as follows:

- 79% have identified their sensitive and confidential information.
- Of those who have identified their sensitive information, 75% have classified their information assets with respect to confidentiality and privacy.
- 52% have classified them according to integrity.
- 78% have classified them according to availability.

Forty-seven per cent of respondents prefer to use three data classification categories. In just over half, or 57%, of respondents, users are provided with instructions, reference materials and the required training to help identify and classify their information assets.

Unlike 2003, where the number of respondents who could acknowledge that they maintained an accurate inventory count of software installations by application barely hit 10%, this year shows an increase to 81%. Although 93% of respondents indicate that they are either "somewhat confident" to "extremely confident" that they could produce the necessary records to demonstrate software license compliance, it is Deloitte's experience from working with many of the largest software publishers in the area of third-party licensing compliance, that this number is inflated due to the complexity of software's licensing terms and conditions and poor asset management practices.

**Unlike 2003, where the number of respondents who could acknowledge that they maintained an accurate inventory count of software installations by application barely hit 10%, this year shows an increase to 81%.**



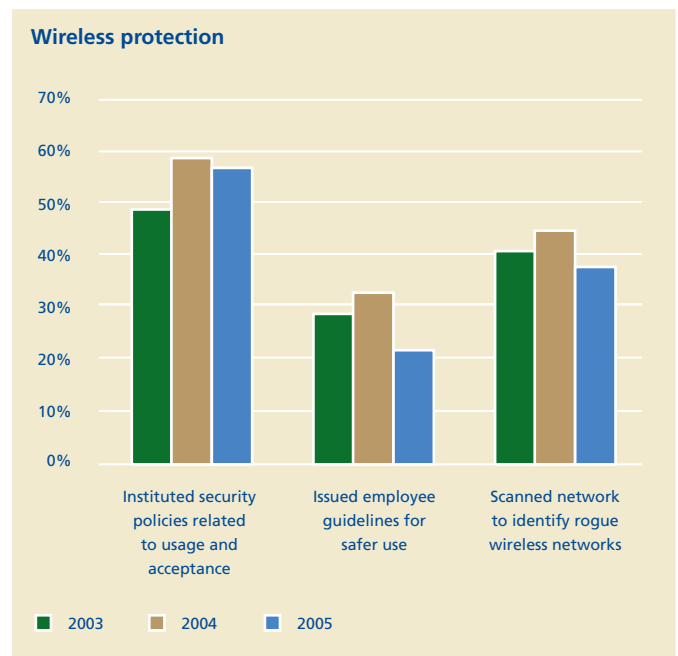
# Use of security technologies

Consistent with findings of the last two years, responses are in line with the cautious attitude exhibited around risk, as respondents identify themselves for the third year in a row as “effective users of demonstrated technology” (60%). Only 6% are willing to take the risk associated with being an early adopter, which again may help explain the high confidence respondents have in relation to prevention from attacks.

Practices around handling emerging technologies, such as wireless networks, are still immature in that little is being done to proactively protect organizations from internal wireless communication exposures. Most respondents rely upon policies for compliance with little enforcement or testing to measure effectiveness. Supporting this finding:

- 38% have scanned the network to identify rogue wireless networks compared to 45% in 2004 and 41% in 2003.
- 22% have issued employee guidelines for the safer use of WiFi, compared to 33% last year and 29% in 2003.
- 57% have instituted security policies related to organizational wireless usage and acceptance compared to 59% last year and 49% in 2003.
- 33% acknowledge they have done nothing to protect themselves from internal wireless communication exposures.

As with the majority of emerging technologies, they need to be designed and deployed in a way that meets the needs of their employees, allowing the organization to capitalize on opportunities while still providing the appropriate levels of security.

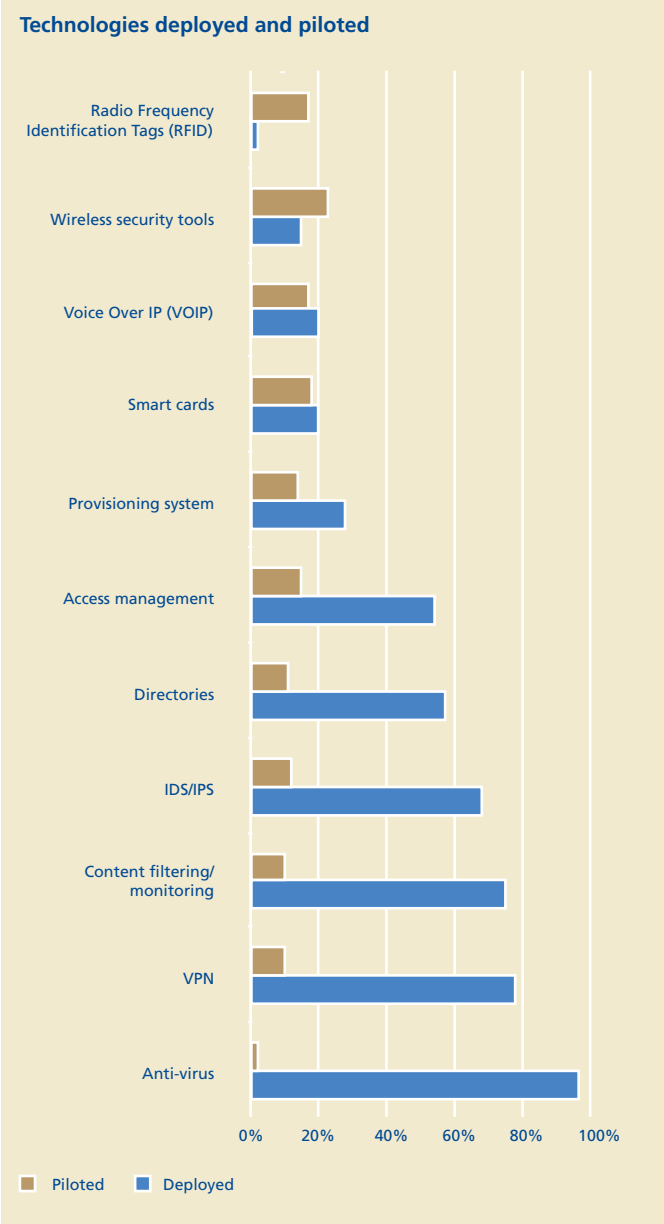


Technologies which have been fully deployed are consistent with those of the last two years. This year the following technology is either deployed or piloted:

- Antivirus – 98% and 2% piloting.
- VPNs – 79% and 10% piloting.
- Content filtering/monitoring – 76% and 10% piloting.
- IDS/IPS – 69% and 12% piloting.
- Directories – 58 and 11% piloting.
- Access management – 55% and 15% piloting.
- Provisioning systems – 28% and 14% piloting.
- Smart Cards – 20% and 18% piloting.
- VOIP – 20% and 17% piloting.
- Wireless Security tools – 15% and 23% piloting.
- RFID – 2% and 17% piloting.

In an effort to understand how respondents feel that the landscape is changing, we asked what technologies they would be piloting or deploying over the next 18 months. Responses included:

- Access management – 23%.
- Wireless security tools – 20%.
- Smart cards – 19%.
- VOIP – 15%.



# Quality of operations

Breaches due to internal attack are on the rise. For the first time in the Global Security Survey, the number of organizations who have experienced internal attacks is higher than the number who have experienced them externally. It is interesting to note that security training and awareness dollars have decreased over the last year, even though 86% of respondents indicate they are concerned about employee misconduct involving information systems.

When it comes to training and awareness sessions on security and privacy issues and statutory compliance in the last 12 months:

- Only 59% of respondents who feel “extremely confident” in the protection of their networks internally have put on a training and awareness program for their employees over the last 12 months.
- Of those organizations concerned about employee misconduct, only 64% have put on a training and awareness program for their employees over the last 12 months.

Continual education should be a mainstay within the business and employees should be indoctrinated into the security system. For this reason, education should fall evenly within the domains of awareness and technical education. The goal is to establish and maintain an organizational culture where information security is second nature to all employees within the organization. In an era when comparing oneself to the competition is crucial, it is interesting to note that 80% of respondents leverage and disseminate known successes and innovations in security.

Strategic and technological alignment in relation to security initiatives is getting closer to hitting a reasonable level. Thirty seven per cent of respondents feel that they are “aligned” and 54% feel that they are “somewhat aligned”. This finding is an improvement over last year, where only 26% of respondents felt that there was strategic and technological alignment.

Security measures implemented or maintained over the last 12 months appear to have slipped in some organizations:

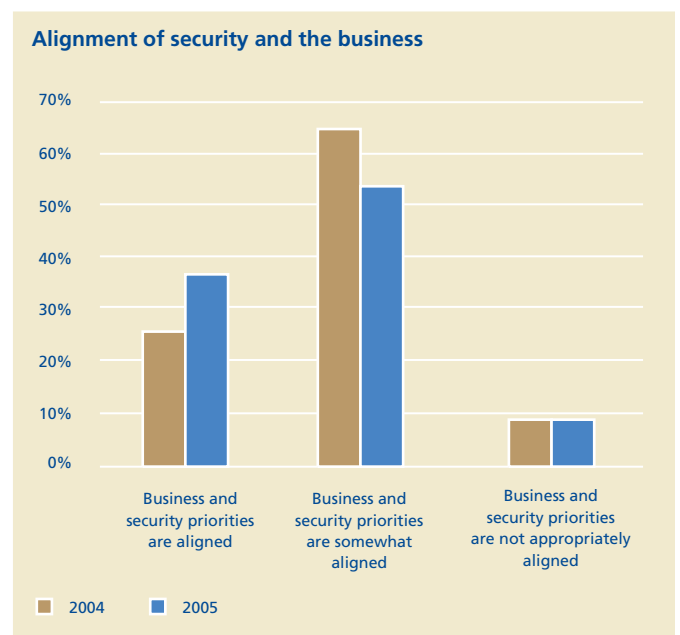
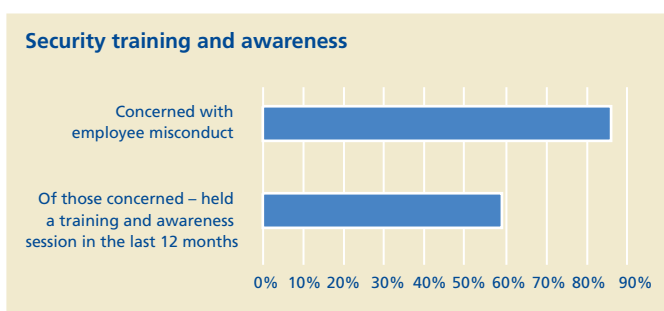
- Security policy – 66% compared to last year (84%).
- Security training and awareness – 65% compared to last year (77%).
- System security tools – 60% compared to last year (75%).
- Business continuity planning – 55% compared to last year (75%).

These findings may possibly be due to an increase in the effort and time spent working on compliance-related activities.

Corporate executives are relatively on par with those of last year in that they are willing to take a direct investment in security preparedness against physical disasters, cyber terrorism and other potential threats.

In terms of respondents who have a comprehensive IT disaster recovery/business continuity plan in place:

- 87% of respondents say they have identified all their critical systems and made the appropriate preparations to operate without them in case of disruption.



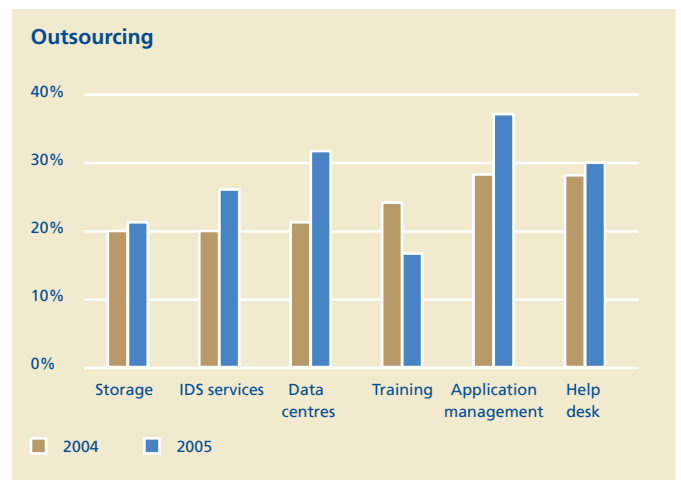
- 54% characterize themselves as “very confident” that their backups are being stored off-site in accordance with policy, compared with 54% for last year and 43% in 2003.
- 86% say their organizations have a recovery/business continuity plan, compared to last year (91%) and 88% in 2003.

Organizations today are finding it difficult to keep up with leading practices in information security, as well as with the appropriate technologies to counter their security threats.

An increasing number of organizations are looking to outsourcing arrangements for their non-core activities to help them accelerate the development of their critical core functions. With an increased number of organizations choosing to outsource, the extended enterprise is no longer the sole owner of the network identities of the users that access its online applications and services.

This survey revealed that organizations that outsource IT-related functions do so in the following areas:

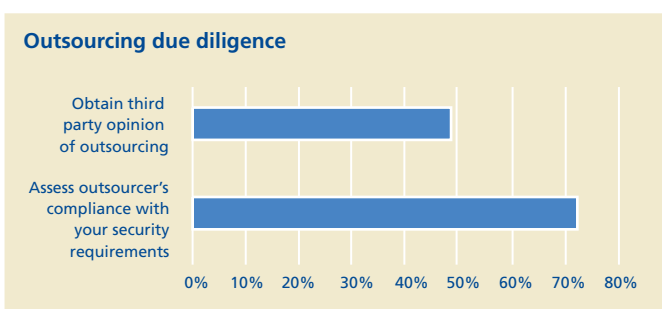
- Application management systems (37%) compared to last year (28%).
- Data centers (32%) compared to last year (21%).
- Help desk (30%) compared to last year (28%).
- IDS services (23%) compared to last year (20%).
- Storage services (21%) compared to last year (20%).
- Training (17%) compared to last year (24%).



Of the 74% of respondents who have chosen to outsource at least one function, the following situations exist:

- 73% have conducted regular assessments of the security outsourcers’ compliance with respondents’ information security requirements.
- Of those 27% who do not conduct regular assessments, 64% are still either “very confident” or “extremely confident” that they have adequately protected their network from an attack.
- 49% currently obtain a third-party opinion (SAS70, Section 5900) from their outsourcer.

Thirty-seven per cent of organizations who chose to outsource would rate their outsourcer’s performance as “very good”. Respondents need to recognize that the increased scrutiny of the compliance of their information security measures also extends to information under the control of, and processed by, third-party outsource providers. Therefore, as a result, respondents will need to do a better job of ensuring that their security measures are strictly upheld by the outsourced providers with whom they contract. Organizations that will prosper in today’s operating environment will have both security and resiliency built into their extended enterprise and greater security compatibility with their partners.



# Privacy

Dealing with privacy compliance issues while trying to design a cost-effective security organization can be difficult to balance. While compliance can be tricky, non-compliance can put the whole organization at risk. Therefore, with privacy the subject area affecting most respondents in terms of regulatory compliance, it is surprising that only 68% of respondents have a program in place for managing privacy compliance within their organization. It is interesting to discover that, given the environment of 2005, still less than half (49%) of respondents have established the role of the Chief Privacy Officer (CPO) although 5% acknowledge that they will have one established by the end of the year.

Reporting structures for CPOs appear to be less defined than those of the CISOs. However, 58% of respondents indicate that they are concerned about conflicts between security and privacy regulations and 38% are cautious but unaware of any conflicts at this time.

Only 57% of respondents currently have a CPO reporting to the C suite or board of directors level, with the highest number reporting to the board itself (19%) or the compliance executive (18%). Privacy reports are not common but 38% of respondents indicate that the board receives them and 33% indicate that the IT committee receives them. However, in the case of 33% of respondents, no privacy reports are distributed.

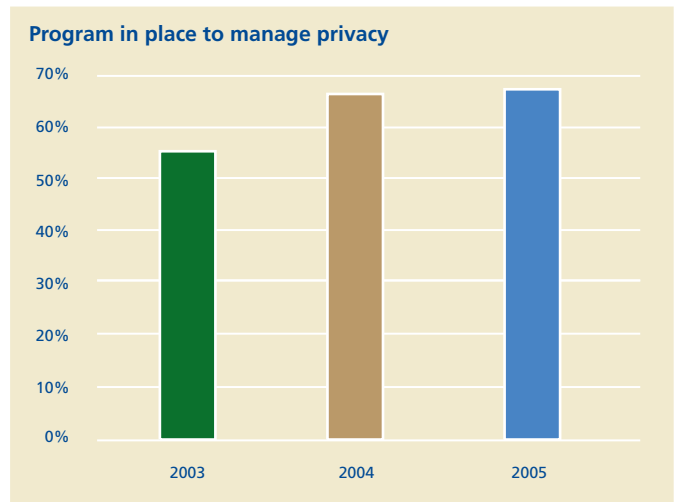
Currently, the majority (61%) of respondents have chosen a centralized model managed from a central corporate group rather than 39% who have chosen a distributive model, whereby responsibility is placed within the business units or entities.

Responsibilities of the privacy executive included the following:

- Customer privacy policies – 59%.
- Privacy strategy – 52%.
- Employee privacy policies and procedures – 48%.
- Analyzing regulations – 46%.
- Reporting to management – 36%.
- Performing privacy risk assessments and data inventories – 25%.

From a reputation perspective, respondents have identified regulations, reputation and brand as the most influential from a privacy perspective.

- Regulations – 83%.
- Reputation and brand – 75%.
- Potential liability – 45%.
- Competition – 45%.



For the second consecutive year, and to a much higher degree than last year, respondents are most concerned with unauthorized access to personal information, and aligning their operational practices with that of their policies from a privacy perspective. Supporting this finding:

- Unauthorized access to personal information – 83% compared to 62% in 2004.
- Managing third-party information sharing – 33% compared to 45% in 2004.
- Aligning operational practices with policies – 30% compared to 19% in 2004.

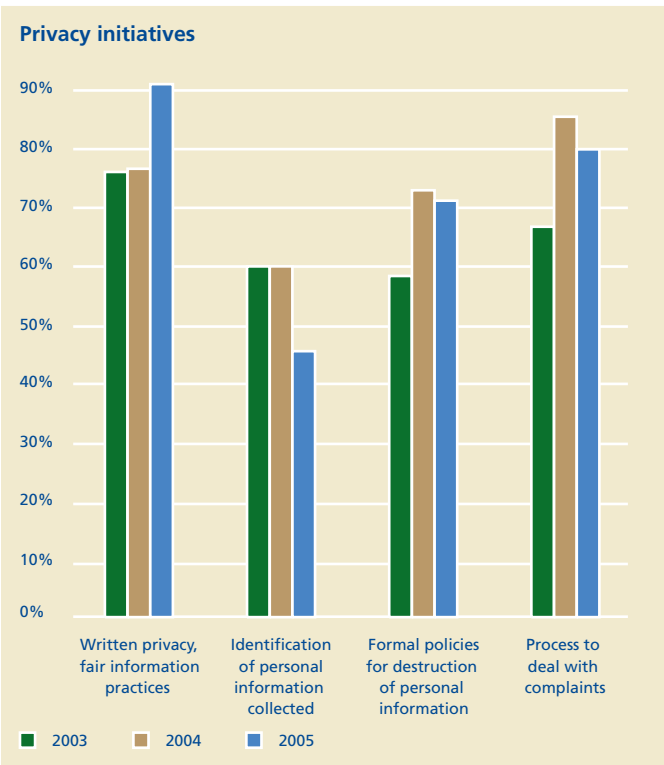
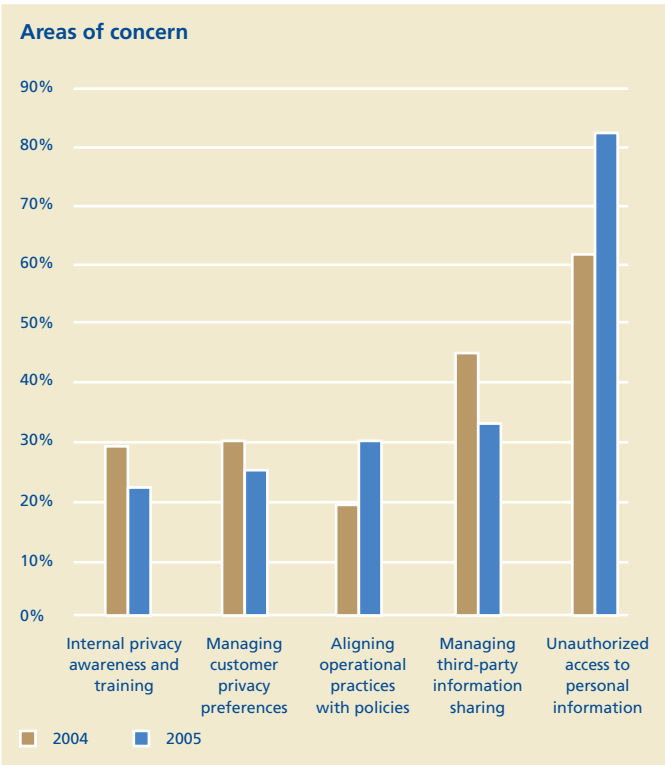
- Managing customer privacy preferences – 25% compared to 30% in 2004.
- Internal privacy awareness and training – 22% compared to 29% in 2004.

Other areas related to privacy remain relatively consistent:

- Written privacy, fair information practices or data collection policies in place – 77% compared to 91% in 2004 and 76% in 2003.
- Formal processes in place to deal with complaints about personal information management practices or policies – 80% compared to 85% in 2004 and 67% in 2003.
- Identification of the types of personal information that is collected and classified according to sensitivity – 46% compared to 60% in 2004 and 2003.

- Formal policies in place with respect to the destruction of personal information – 71% compared to 73% in 2004 and 59% in 2003.

**Although risk is inherent in an organization’s existence, it can either paralyze a potentially successful growth strategy or, if managed properly, it can set the stage for profitable growth.**



# Global Financial Services Industry Security Outlook

## Regulation is here to stay with more to come

"The value of Sarbanes Oxley is not for the current generation but for the next." This quote, from US Federal Reserve Chairman Alan Greenspan, underscores his view that Sarbanes Oxley legislation will affect the way organizations conduct business for years to come. Although SOX is relevant only for US companies and foreign organizations whose shares are listed on US stock exchanges, it continues to set a standard for countries looking to improve their corporate governance.

As a global firm, Deloitte has been engaged by numerous organizations who are adopting SOX, even some who are voluntarily adopting SOX as a "best practice" rather than a requirement. The impact of SOX is shaping how other countries deal with governance and its associated regulations worldwide. The implementation of these regulations and standards will produce fundamental changes in the way financial institutions operate and will help shape their business/risk management strategies.

Although a large number of respondents outside APAC feel that the emerging government-driven security regulations are ineffective in improving security in their industry, those who fail to respond face reputational damage, increased regulation and loss of enterprise value. For those who use these initiatives to drive change, the story will be very different: they have the potential to successfully link strategy formulation to a fully informed analysis of the implications of these changes, bringing with it an opportunity to strengthen corporate governance. Adopting best practices can allow FSIs to strengthen their brand and distinguish themselves in the current environment of intense scrutiny and skepticism of corporate behavior.

## The growing threat of identity theft

Identity theft is the practice of assuming another person's identity in order to commit a crime. In the past, most people have associated identity theft with credit card fraud. However, with more people online and new and emerging forms of theft, identity theft has become the fastest growing white collar crime in the US. It accounts for 42% of all fraud complaints to the US Federal Trade Commission (FTC). The Credit Industry Fraud Avoidance Scheme (CIFAS) reported that identity theft cost the UK nearly \$1 billion in 2003. The most common identity theft complaints to the FTC involved credit card fraud, bank fraud and loan fraud.

Over the last year, attacks on financial institutions have been on the rise. Financial services institutions are targets because they hold people's money and have copious amounts of personal data. Many global financial institutions have been subject to phishing attacks over the last year. Other organizations have experienced attacks of even greater severity and of a different nature including a shift in approach whereby attackers are targeting third parties and related entities as the weakest link.

A large North American financial institution became a statistic when workstations containing sensitive information were stolen from its premises, providing the thieves access to valuable information required to steal customers' identities.

In February of 2005, a large North American financial institution lost computer data tapes containing the personal information of 1.2 million federal employees, including some members of the U.S. Senate. The lost data included Social Security numbers and account information that had the potential to make customers of a federal government charge card program vulnerable to identity theft. The bank later allayed people's fears somewhat by announcing that accessing the data would require "special software".

As a result of California Civil Code 1798, an organization was obligated to disclose to their California customers that the company had lost their information. However, the breach turned out to be far worse than expected when the organization revealed that it had lost information on a total of 145,000 US citizens. In India, employees of a call center were arrested for defrauding customers of account information and \$350,000 from another large global financial institution.

Once considered stalwart and impenetrable, financial institutions are now besieged and the results are tarnished brands and loss of customers, with the accompanying financial losses.

Governments all over the world have reacted. In the US, the federal government has enacted laws such as the Theft and Assumption Deterrence Act (ITADA) and ID Theft Penalty Enhancement Act of 2004. The US has also established regulations on industries such as the Health Insurance Portability and Accountability Act (HIPPA) for health care providers and Gramm Leach Bliley Act (GLBA) for financial institutions. Outside the US, provisions for identity theft are part of Canada's Personal Information Protection and Electronics Document Act (PIPEDA). In Europe, the EU Data Protection Directive is aimed at protecting individual information for reasons of consumer privacy and identity theft prevention.

Identity theft is evolving quickly. In the past, the majority of attacks were on unlocked and unguarded mail boxes and through social engineering or customer impersonation. Today, methods include spyware, SQL injection, hardware theft, hacking, phishing and pharming, and, most frightening, insider fraud. This year's survey indicates that the majority of respondents who experienced some form of breach experienced it from within the walls of their organization. In many instances, employees have unlimited access to customers' vital data, including government issued numbers (e.g. Social Insurance and Social Security Numbers) and account number information.

Increased regulation is only one variable in helping prevent future fraud attempts. Another measure is technology enhancements. Many financial institutions are looking to existing technologies to help prevent future identity theft attacks. Smart and Chip cards, encryption, web site and email validation solutions are all technology solutions that financial institutions are targeting to help prevent further attack attempts. However, technologies are not silver bullets. Financial institutions need to create and enforce security measures, like policies and procedures for data access, running background checks for new hires and making third-party service providers follow the organization's security requirements such as monitoring for compliance and limiting employees' access to vital information. All these measures need to be further reinforced through company-wide training and awareness sessions and by the creation of motivators to help influence people's behaviors.

**A security program needs to be driven by the requirements of the business and then continually monitored, measured and adapted to the business's changing operating environment**

Respondents indicate that supporting changes in corporate governance is a key priority for 2005. Although the majority of organizations have an information security strategy, most are in the early stages of implementation. Many require revisiting with a careful appraisal of all potential dangers.

A comprehensive information security program provides the framework and processes required to help an organization proactively identify its threats and vulnerabilities and assess their impact on information systems and the information they protect. However, tying an effectively executed governance structure into the information security program is a highly complex undertaking.

Many respondents have a defined IT security governance framework in place (69%) or are in the process of drafting one (18%). Information security is an essential component of IT governance, helping to define the objectives, structure, roles and responsibilities and to provide a process for decision making driven by data. In a complimentary finding, 81% of respondents have aligned their information security strategy with one of the industry-accepted security standards, such as ISO 17799: 2000, an internationally recognized, structured list of better practices dedicated to information security (67%); ITIL, a framework for mature processes for IT services management (39%); and BS7799-2:2002 certification (17%). The ideal governance structure will aid an organization in helping to set the right priorities and fund the highest value initiatives.

A good security program assists an organization in finding the balance between understanding security risks, being in a position to take advantage of business opportunities and continually increasing shareholder value. A security program needs to be driven by the needs of the business and then continually monitored, measured and adapted to the business's changing operating environment. A systematic, comprehensive approach is required to identify all the components that need to be addressed and their interdependencies to one another and to the business.

A key component of BS7799-2:2002 and ISO 17799:2000 is that the thinking behind them is very similar to the thinking used in security program development. This thinking provides a framework for seeing beyond the pieces of an organization to the whole. It allows for the management of risk either in silos or across the entire organization, enabling management to minimize change and volatility at an operational level while exploiting it at a strategic level. A management system establishes policy and objectives and, if done correctly, helps the organization to achieve its organizational objectives. Therefore, an Information Security Management System (ISMS) is the framework that must be created to implement, manage, maintain and enforce information security processes. Like a security program, an ISMS is used to develop policies and procedures and put them into effect via targets and objectives in a systematic way.

### **Safeguarding information requires a collaborative approach**

With concerns over privacy and security increasing both from financial institutions and their customers, it is no surprise that governments and private industry are reacting quickly. The requirement for a secure economy is creating a balance between private companies and the public sector, co-operation that didn't always happen easily in the past. Financial institutions are starting to invest more time and resources in helping advance the public and private partnership. FSIs are finding it to their advantage to work with their respective governments to help them develop appropriate security standards and influence laws and regulations. With the private sector owning large pieces of the critical infrastructure (power grids, banking networks, industrial logistics systems, and telecommunications networks) it is in the government's best interests to work with them to help mitigate any potential threats to the country and its people. Given that the majority of large, powerful organizations operate both within and outside the borders of their respective countries the world has an economic interest in helping each other's enterprise fight the threats they may face and share innovative best practices in relation to information security.

Over the last twelve months, there have been several security breaches involving the loss or disclosure of personal information held by financial institutions and other organizations, generating strong pressure for enhanced legal actions, to implement appropriate information security measures to protect personal data. As a result, there have been a mix of responses.

**The attacks of the last year have done a good job at demonstrating not only the importance of technology but also its limitations.**

**Anti-Phishing Working Group (APWG)**

According to the Anti-Phishing Working Group report of March 2005 phishing attacks have experienced a monthly average growth rate of 28% since July 2004. With numbers like these there was a definite need for the private industry to come together. The APWG is made up of a combination of financial service institutions, Internet Service Providers (ISPs), e-commerce providers and vendors of email services and software. The goal of the APWG is to help educate the public on phishing attacks as well as provide the right vision and set of expertise to assist in finding the right solution to phishing attacks.

**Financial Services Information Sharing and Analysis Center (FS-ISAC)**

Fraud works on the premise of "if it ain't broke don't fix it." Fraudsters will continue using the same scam over and over until they have been thwarted. Knowing this, it comes as little surprise that 80% of respondents indicate that they leverage and disseminate known successes and innovations in security such as best practices. The Financial Services Information Sharing and Analysis Center (FS-ISAC) is just that. The FS-ISAC is a private partnership of banks, brokerages, insurance companies, and utilities which is under the auspices of the President's Commission on Critical Infrastructure Protection. Through FS-ISAC, many of the nation's experts in the financial services sector share and assess threat intelligence provided by its members, enforcement agencies, technology providers, and security associations.

**European Network and Information Security Agency (ENISA)**

In 2004, the EU facilitated the creation of ENISA to fulfill their mission "to assist the community in ensuring particularly high levels of network and information security."

ENISA's tasks include helping the public sector draft legislation around security, raise awareness and educate the masses by promoting information security best practices and track and evaluate global threat agents that may have an impact on the community members.

**Payment Card Industry Standard (PCI)**

With consumers becoming increasingly protective about their privacy and relatively fickle if they feel their respective institutions cannot adequately protect their information, it is no surprise that credit card issuers are taking a proactive stance to ensure that their customers' confidential information remains protected. In March 2005, an association of credit card companies led by MasterCard International announced a new Payment Card Industry (PCI) standard.

The program requires tighter security for merchants that process a high volume of credit card transactions (six million or greater a year) and it standardizes security practices around the world. Now, any merchant that exceeds the threshold of processing six million or greater transactions a year (online or offline) must be certified annually by a third-party firm. The certification which can only be granted by a Qualified Independent Security Assessor (QISA), confirms that the merchant is compliant with 12 security measures, like safeguarding systems and data from viruses to establishing a hiring policy for staff and contractors.

**The essence of Access Management is to enable a safe, secure and trusted business environment through enhanced accountability, auditability and transparency of information assets.**

# Helpful references and links

## Global Information Security Associations

Bank for International Settlements  
[www.bis.org](http://www.bis.org)

Banking Industry Technology Secretariat (BITS)  
[www.bitsinfo.org](http://www.bitsinfo.org)

British Standards Institution (BSI): BS7799-2:2002  
[www.bsi-global.com](http://www.bsi-global.com)

Business Software Alliance (BSA)  
[www.bsa.org](http://www.bsa.org)

Carnegie Mellon University Software Engineering Institute  
[www.sei.cmu.edu](http://www.sei.cmu.edu)

Defense Information Systems Agency (DISA)  
[www.disa.mil](http://www.disa.mil)

Department of Trade and Industry: Information Security  
[www.dti.gov.uk/industries/information\\_security/](http://www.dti.gov.uk/industries/information_security/)

European Commission (EUROPA): Data Protection  
[http://europa.eu.int/comm/internal\\_market/privacy/index\\_en.htm](http://europa.eu.int/comm/internal_market/privacy/index_en.htm)

Federal Trade Commission (FTC)  
[www.ftc.gov](http://www.ftc.gov)

Global Corporate Governance Forum (GCGF)  
[www.ggf.org](http://www.ggf.org)

Information Security Forum (ISF)  
[www.isfsecuritystandard.com](http://www.isfsecuritystandard.com)

Information Systems Audit and Control Association  
[www.isaca.org](http://www.isaca.org)

Information Systems Security Association (ISSA)  
[www.issa.org](http://www.issa.org)

International Federation of Accountants  
[www.ifac.org](http://www.ifac.org)

International Information Systems Security Certification Consortium (ISC)2  
[www.isc2.org](http://www.isc2.org)

International Standards Organization (ISO): ISO 17799-2000  
[www.iso.org](http://www.iso.org)

IT Governance Institute (ITGI)  
[www.itgi.org](http://www.itgi.org)

National Institute of Standards and Technology (NIST) Computer Security Resource Center  
<http://csrc.nist.gov>

National Security Agency (NSA)  
[www.nsa.org](http://www.nsa.org)

OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security  
[www.oecd.org](http://www.oecd.org)

Systems Administration, Audit and Network Security Institute (SANS)  
[www.sans.org](http://www.sans.org)

VISA International Account Information Security (AIS): Payment Card Industry (PCI) Data Security Standard  
[www.visa.com/\\_gds\\_mod/fb/merchants/gds/main.html](http://www.visa.com/_gds_mod/fb/merchants/gds/main.html)

## Industry Responses to Identity Theft

Anti-Phishing Working Group (APWG)  
[www.antiphishing.org](http://www.antiphishing.org)

Financial Services Information Sharing and Analysis Center (FSI/ISAC)  
[www.fsisac.com](http://www.fsisac.com)

Identity Theft Assistance Center (ITAC)  
[www.bitsinfo.org](http://www.bitsinfo.org)

Infragard  
[www.infragard.net](http://www.infragard.net)

**APAC**

Institute of Chartered Accountants in Australia  
<http://icaa.org.au>

Australia's National Computer Emergency Response Team (AusCERT)  
[www.auscert.org.au](http://www.auscert.org.au)

China Education and Research Network Computer Emergency  
 Response Team (CCERT)  
[www.ccert.edu.cn](http://www.ccert.edu.cn)

Corporate Governance Japan  
[www.rieti.go.jp](http://www.rieti.go.jp)

Japan Computer Emergency Response Team Coordination  
 Center (JPCERT)  
[www.jpCERT.or.jp](http://www.jpCERT.or.jp)

**EMEA**

African-Union  
[www.africa-union.org](http://www.africa-union.org)

Austrian Working Group for Corporate Governance  
[www.corporate-governance.at](http://www.corporate-governance.at)

Belgian Directors Institute (BDI)  
[www.ivb-ida.com](http://www.ivb-ida.com)

European Corporate Governance Institute (ECGI)  
[www.ecgi.de/codes](http://www.ecgi.de/codes)

Institute of Chartered Accountants in England and Wales  
[www.icaew.co.uk](http://www.icaew.co.uk)

French Business Confederation (MEDEF)  
[www.medef.fr](http://www.medef.fr)

CERT-Bund (Germany)  
[www.bsi.bund.de/certbund](http://www.bsi.bund.de/certbund)

German Accounting Standards Committee  
[www.standardsetter.de](http://www.standardsetter.de)

Computer Emergency Response Team Italy (CERT-IT)  
<http://security.dsi.unimi.it>

**LACRO**

Ministerio da Ciencia e Tecnologia: Policy for Information Security  
 Management (Brazil)  
[www.mct.gov.br/legis/decretos/3505\\_2000.htm](http://www.mct.gov.br/legis/decretos/3505_2000.htm)

**North America**

North American Electric Reliability Council (NERC)  
[www.nerc.com](http://www.nerc.com)

American Institute of Certified Public Accountants (AICPA): SysTrust/  
 WebTrust  
[www.aicpa.org/trustservices](http://www.aicpa.org/trustservices)

Department of Homeland Security (DHS)  
[www.dhs.gov](http://www.dhs.gov)

Public Company Accounting Oversight Board (PCAOB)  
[www.pcaobus.org](http://www.pcaobus.org)

Canada - Personal Information Protection and Electronic Documents  
 Act (PIPEDA)  
<http://laws.justice.gc.ca/en/p-8.6/93196.html>

Canada's Computer Emergency Response Team (canCERT)  
[www.cancert.ca](http://www.cancert.ca)

Canadian Institute of Chartered Accountants (CICA)  
[www.cica.ca](http://www.cica.ca)  
[http://europa.eu.int/agencies/enisa/index\\_en.htm](http://europa.eu.int/agencies/enisa/index_en.htm)

# Acknowledgements

We wish to thank all of the professionals of the financial institutions who responded to our survey and who allowed us to further correspond with them over the course of this project. Without such participation and commitment, Deloitte Touche Tohmatsu member firms could not produce surveys such as this. We extend our heartfelt thanks for the time and effort that respondents devoted to this project.

## Survey Development Team

### Authors

Adel Melek  
1 (416) 601 6524  
amelek@deloitte.ca

Marc MacKinnon  
1 (416) 601 5993  
mmackinnon@deloitte.ca

### Data Analysis and Editing

Joseph Strantzl  
1 (416) 601 6359  
jstrantzl@deloitte.ca

Clare Galloway  
1 (416) 601 6357  
clgalloway@deloitte.ca

### Methodology and Survey Development

DeloitteDex:  
Olivier Curet  
1 (216) 589 5448  
ocuret@deloitte.com

Cynthia O'Brien  
1 (216) 589 3980  
cobrien@deloitte.com

### Marketing Support

Chris Patterson  
1 (212) 436 2779  
chrpatterson@deloitte.com

Nicolas de Rooij  
1 (416) 601 5932  
nderooij@deloitte.ca

# Contacts

## Jack Ribeiro

Managing Partner  
Global Financial Services Industry Practice  
Deloitte & Touche LLP  
+1 212 436 2573  
jribeiro@deloitte.com

## Leon Bloom

Managing Partner, Service Lines  
Global Financial Services Industry Practice  
Deloitte & Touche  
+1 416 601 6244  
lebloom@deloitte.ca

## Regional leaders

Adel Melek	Toronto, Canada	Deloitte & Touche LLP	+1 416 601 6524	amelek@deloitte.ca
Mike White	Johannesburg, South Africa	Deloitte & Touche	+27 11 806 5899	mikwhite@deloitte.co.za
Kevin Shaw	Melbourne, Australia	Deloitte Touche Tohmatsu	+61 3 9208 7637	kevshaw@deloitte.com.au
Ted DeZabala	New York, U.S.A.	Deloitte & Touche LLP	+1 212 436 2957	tdezabala@deloitte.com
Keiichi Kubo	Tokyo, Japan	Deloitte Touche Tohmatsu	+81 3 6213 1112	keiichi.kubo@tohmatsu.co.jp
Roberto Gejman	Santiago, Chile	Deloitte & Touche	+56 2 270 31 50	rgejman@deloitte.com

## Contacts

Ioannis Tzanos	Athens, Greece	Deloitte Touche Tohmatsu	+30 210 678 1100	itzanos@deloitte.gr
Chris Verdonck	Brussels, Belgium	Deloitte Business Advisory NV	+32 2 800 2420	cverdonck@deloitte.com
Danny Lau	Hong Kong	Deloitte Touche Tohmatsu	+852 2852 1015	danlau@deloitte.com
Juan Miguel Ramos	Madrid, Spain	Deloitte, S.L.	+34 91 514 5000 x2107	juramos@deloitte.es
John Clark	Chicago, U.S.A.	Deloitte & Touche LLP	+1 312 946 3985	johclark@deloitte.com
Bruce Daly	Tokyo, Japan	Deloitte Touche Tohmatsu	+81 3 4218 7284	brdaly@deloitte.com
Rob Stout	Den Haag, Netherlands	Deloitte Holding B.V.	+31 20 582 4040	Rstout@deloitte.nl
Gerry Fitzpatrick	Dublin, Ireland	Deloitte Touche Tohmatsu	+353 1 417 2645	gfitzpatrick@deloitte.com
Stefan Weiss	Frankfurt, Germany	Deloitte & Touche GmbH	+49 711 16554 7322	stweiss@deloitte.de
Simon Owen	London, U.K.	Deloitte & Touche LLP U.K.	+44 20 7007 8105	sdwown@deloitte.co.uk
Alfonso Mur	Madrid, Spain	Deloitte, S.L.	+34 91 514 5000 x2103	amur@deloitte.es
Marcel Labelle	Montreal, Canada	Deloitte & Touche LLP	+1 514 393 5472	marlabelle@deloitte.ca
Abhay Gupte	Mumbai, India	Deloitte Haskins & Sells	+91 22 282 4399	agupte@deloitte.com
Francois Renault	Neuilly, France	Deloitte & Touche FR	+33 1 55 61 61 22	frenault@deloitte.fr
Henry Ristuccia	New York, U.S.A.	Deloitte & Touche LLP	+1 212 436 4244	hristuccia@deloitte.com
Valerie Flament	Paris, France	Deloitte & Touche FR	+33 1 40 88 2464	vflament@deloitte.fr
Kenneth DeJarnette	San Francisco, U.S.A.	Deloitte & Touche LLP	+1 415 783 4315	kdejarnette@deloitte.com
Ricardo Balkins	São Paulo, Brazil	Deloitte Touche Tohmatsu	+55 11 5186 1559	rbalkins@deloitte.com
Tommy Viljoen	Sydney, Australia	Deloitte Touche Tohmatsu	+61 3 9208 7140	tfviljoen@deloitte.com.au
Donald McColl	Toronto, Canada	Deloitte & Touche LLP	+1 416 601 6373	dmccoll@deloitte.ca
David A. Old	Wellington, New Zealand	Deloitte Touche Tohmatsu	+64 4 470 3614	dold@deloitte.co.nz
David J. Pike	Zurich, Switzerland	Deloitte & Touche AG	+41 44 421 6401	djpike@deloitte.com

The scope of this survey was global, and, as such, encompassed financial institutions with worldwide presence with head office operations in one of the following geographic regions: North America; Europe, Middle East, Africa (EMEA); Asia Pacific (APAC); and Latin America and the Caribbean (LACRO). Attributes such as size, global presence, and market share were taken into consideration. Due to the global nature of the survey, the results are representative of each identified region.

Survey users should be aware that Deloitte Touche Tohmatsu has made no attempt to verify the reliability of such information. Additionally, the survey results are limited in nature, and do not comprehend all matters relating to security and privacy that might be pertinent to your organization.

Deloitte Touche Tohmatsu makes no representation as to the sufficiency of these survey results for your purposes. Reported survey findings should not be viewed as a substitute for other forms of analysis that management should conduct.

Prior to making decisions or taking action that might affect your business; you should consult a qualified professional advisor. Your use of these survey results and information contained herein is at your own risk.

Deloitte Touche Tohmatsu will not be liable for any damages, including, without limitation, negligence) or other consequences that may result from the use of the information contained in this report are provided "as is," and Deloitte Touche Tohmatsu makes no express or implied representations or warranties regarding the results or the information.

For more information on the Global Security Survey, please contact your local Deloitte Touche Tohmatsu professional listed above.

Deloitte Touche Tohmatsu is a Swiss Verein (association), and, as such, neither Deloitte Touche Tohmatsu nor any of its member firms has any liability for each other's acts or omissions. Each member firm is a separate and independent legal entity operating under the names "Deloitte," "Deloitte & Touche," "Deloitte Touche Tohmatsu," or other, related names. The services described herein are provided by the member firms and not by the Deloitte Touche Tohmatsu Verein.

Deloitte Touche Tohmatsu is an organization of member firms devoted to excellence in providing professional services and advice. We are focused on client service through a global strategy executed locally in nearly 150 countries. With access to the deep intellectual capital of 120,000 people worldwide, our member firms, including their affiliates, deliver services in four professional areas: audit, tax, consulting, and financial advisory. Our member firms serve more than one-half of the world's largest companies, as well as large national enterprises, public institutions, locally important clients, and successful, fast-growing global companies. For regulatory and other reasons, certain member firms do not provide services in all four professional areas.

Designed and produced by The Creative Studio at Deloitte, London. AP #5071