

# 2004 Global Security Survey



# Contents

<b>Introduction</b>	Page
Foreword .....	1
Objective of the survey .....	2
How we designed, implemented and evaluated the survey .....	3
Areas covered by the survey .....	5
Who responded .....	6
Regional observations .....	8
Key findings of the survey .....	11
<b>Body of the survey</b>	
Governance .....	16
Investment in security .....	20
Value .....	21
Risk .....	22
Use of security technologies .....	24
Quality of operations .....	25
Privacy .....	27
<b>Conclusion</b>	
Summing up and challenges .....	29

# Foreword

It is particularly gratifying for me to write this foreword to the second annual Deloitte Global Security Survey. When we began the first Global Security Survey last year, we could not have anticipated the



excellent response we received – from financial institutions around the globe and from the media. This response has supported our desire to have this survey become an annual occurrence and not just a “one off” publication. We intend to continue this tradition on an annual basis.

It seems that every year, the importance of information security – particularly for financial institutions – grows more crucial and the challenges on all fronts continue to mount. Chief among these challenges is meeting the various regulatory initiatives and preparing for potential security threats that have not previously materialized. How does an organization keep information secure while, at the same time, allowing customers access to the information to which they are entitled? How does a company keep shareholders happy by returning good value when cutting costs may mean offshoring, a practice that invites consumer concerns? How does an organization protect its information while opening itself up to customers and partners for revenue growth? And how does an organization balance its stakeholder demands while managing the cost of security solutions to prevent IT attacks?

While there are no easy answers to these questions, each one of them is tackled in this Security Survey, some with surprising results. This is a report to which your counterparts, in financial institutions all over the world, have had direct input. Its purpose is to “tell it like it is” – the extent to which it does this directly affects its value as a benchmark. We hope that you will find this information useful and that it helps establish organizational direction for a very complex issue.

We are deeply indebted to the participants, without whom this survey could not exist. To the Chief Security Officers, their designates, and the security management teams from financial services industry organizations around the world, my heartfelt thank you for the time that you invested in this undertaking.

A handwritten signature in black ink that reads "Adel Melek".

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



# Objective of the survey

Response to Deloitte Touche Tohmatsu's inaugural 2003 Global Security Survey was overwhelming. We have come to the realization that, as financial institutions continue to face an unprecedented number of evolving threats, there will always be a need for the type of information contained in these surveys. We are, therefore, very pleased to present our 2004 Global Security Survey for financial institutions. Deloitte's purpose in publishing the results of this survey is to contribute to the protection of the financial services marketplace by sharing current practices and identifying future trends in security and privacy management.

The goal of the 2004 Global Security Survey is to help participants assess the state of information security within their organization relative to other comparable financial institutions around the world, and against themselves year over year, to the extent they respond to the survey annually. 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 data collected

for the 2004 survey, we can begin to determine differences and similarities, identify trends and allow participants to answer more in-depth questions, such as: How is the state of information security changing within my organization? and, Are these changes aligned with the evolution of the rest of the industry?

Where possible, questions that were asked as part of the 2003 Global Security Survey have been repeated, thereby allowing for the collection and analysis of trend data. To ensure that the questions remained 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. Two such areas were Business Continuity Management and Privacy. To help differentiate this survey from any previously existing surveys, Deloitte subject matter experts were approached and their knowledge leveraged to identify the questions with the most impact.

# How we designed, implemented and evaluated the survey

The 2004 Global Security Survey reports on the outcome of focused discussions between Deloitte Touche Tohmatsu 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 that FSIs are gaining from their security investments. To fulfill this objective, senior members of Deloitte's Security Services group designed a questionnaire that probed eight aspects of strategic and operational areas of security and privacy. These eight areas, and their sub areas, are described in the section entitled "*Areas covered by the survey*".

Responses of participants relating to the eight 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 operations in the following geographic regions: North America; Europe, Middle East, Africa (EMEA); Asia Pacific (APAC); and Latin America and the Caribbean (LACRO). To ensure organizational 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 lines of business, including banking, securities, insurance and investment 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 Touche Tohmatsu member firms' Security Services professionals. Questions were selected based on their effectiveness 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 second 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 added to reflect topics being asked about by our clients and topics written in the media.

### **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 attaining answers from the various financial institutions with whom they had a relationship. Most of the data collection process took place through a face-to-face interview with the Chief Security Officer (CSO/CISO) or designate, and in some instances, with the IT security management team.

### **Results analysis and validation**

The DeloitteDEX team helped with extracting 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 analysis measuring financial and/or operational performance. 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 best 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 manage complex systems and processes. The Global Security Survey is intended to enable benchmarking against comparable organizations. Benchmarking can aid in searching for best practices that produce superior performance when adapted and implemented. Benchmarking can often result in recommendations for performance improvements from the benchmarking findings.

# Areas covered by the survey

It is possible that your organization may excel in some areas related to information security, e.g. investment and responsiveness, and yet fall short in other areas, e.g. value and risk. In order to be able to pinpoint the specific areas

that require your attention, we chose to group the questions by the following eight areas of a typical financial services organization's operations and culture:

## Governance

- Compliance
- Policy, accountability
- Management support
- Measurement

## Investment

- Budgeting
- Staffing
- Management

## Value

- Management's view
- Applications/uses
- Security infrastructure
- Success measurement
- Feedback
- Compliance

## Risk

- Industry averages
- Spending
- Intentions
- Competition
- Public networks
- Controls
- Encryption
- Software licensing

## Responsiveness

- Application development
- Technology change
- Innovation

## Use of security technologies

- Technology
- Knowledge base
- Other

## Quality of operations

- Business continuity management
- Benchmarking
- Administration
- Detection
- Response
- Privileged users
- Authentication
- Controls

## Privacy

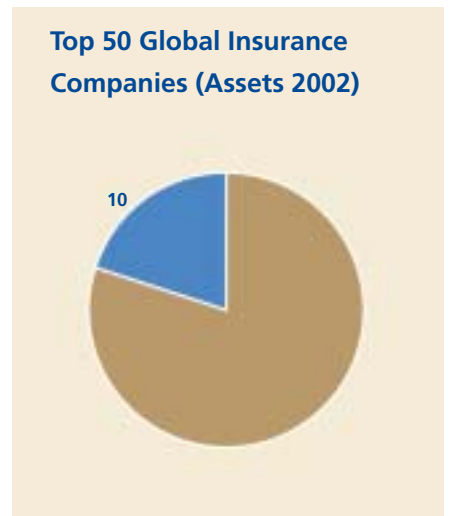
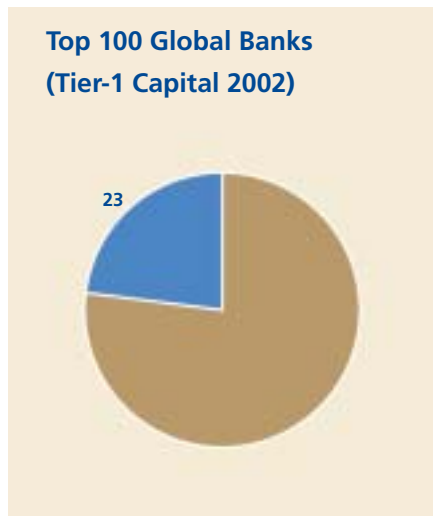
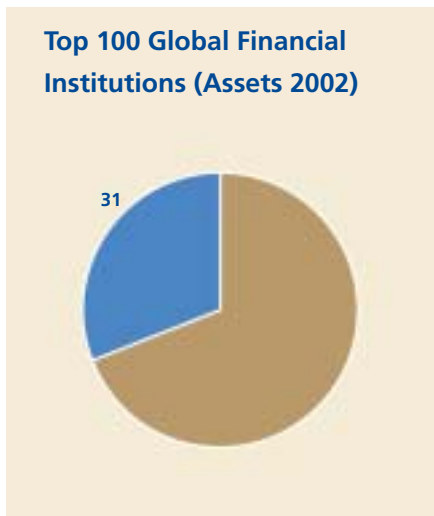
- Compliance
- Ethics
- Data collection policies
- Communication techniques
- Safeguards
- Personal information protection

# Who responded

The 2004 Global Security Survey respondent data reflects current trends in security and privacy throughout major global financial institutions. The final survey sample reflects all major financial sectors (banking, insurance, investment management, securities, payments and processors and diversified financial institutions).

In order to ensure that the answers we received to our survey questions were as honest and candid as possible, we agreed to preserve the anonymity of the participants and their organizations. Overall, the participants represent:

- 31 of the top 100 global financial services institutions ranked by 2002 assets;
- 23 of the top 100 global banks ranked by 2002 tier-1 capital;
- 10 of the top 50 global insurers ranked by 2002 assets.



## Geographic region

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

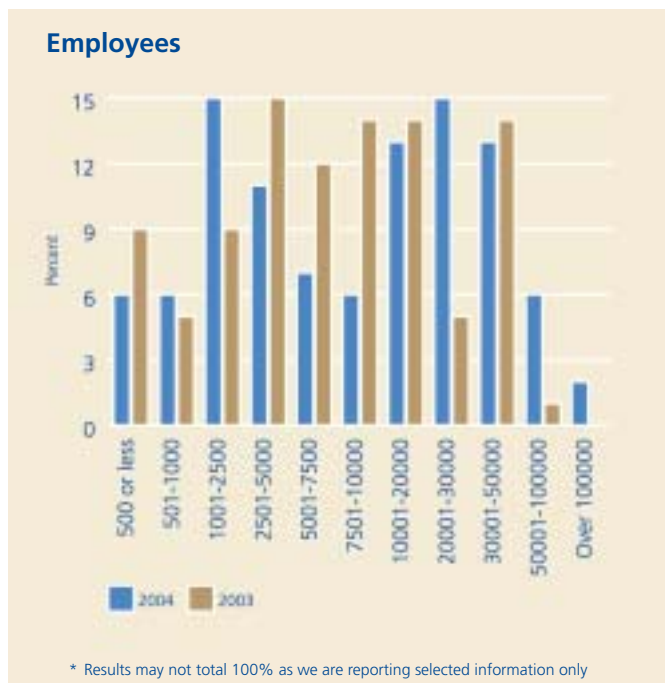
- United States: 32%
- Canada: 10%
- Europe, the Middle East and Africa: 49%
- Asia/Pacific: 7%
- Latin America: 2%



### Ownership and size

Because the level of scrutiny to which public and private organizations are held differs greatly, we wanted to ensure that our survey included both types. Of the organizations that responded, 48% were public, 42% were private and the other 10% comprised not-for-profit, public sector or private subsidiaries of publicly held organizations.

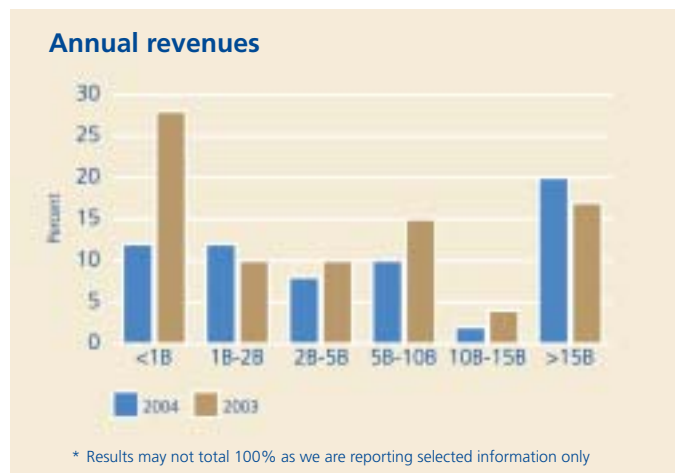
- 500 to 20K employees: 64%
- 20K to 30K employees: 15%
- 30K to 50K employees: 13%
- 50k to over 100k employees: 8%



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

- <1B in annual revenue: 19%
- \$1B-\$2B in annual revenue: 19%
- \$2B-\$5B in annual revenue: 12%
- \$5B-\$10B in annual revenue: 16%
- \$10B-\$15B in annual revenue: 3%
- >\$15B in annual revenue: 31%

All currency stated in US dollars



# Observations regarding similarities and contrasts by geographic region

## Europe, Middle East and Africa (EMEA)

Once again, EMEA respondents are ahead of the pack when it comes to policy setting, security standards, privacy compliance and having a formalized security strategy. Legal and industry regulations, reputation and brand were among the most identified drivers in ensuring compliance. Not surprisingly, given the number of countries and diversity of languages, EMEA ranked second highest behind Canada in commitment and funding to address regulatory requirements.

EMEA ranked in the mid-range when it came to recognizing the value of security and its tie to enabling business operations. They had a mid-range ranking when it came to having the right key performance indicators (KPIs) and the required skills and competencies to address security. Of all respondents, EMEA ranked the lowest in reporting and tracking security successes. The security functions in EMEA rank highest in employing the greatest number of security staff, which in turn, could be directly related to them having the lowest percentage of FSIs who experienced a flat budget growth.

Outsourcing security staff is gaining popularity as the option of choice in Europe and the Middle East but African respondents indicated that they had not outsourced any of their security staffing needs.

## Asia Pacific (APAC)

APAC was far ahead of any other part of the world in its view of security as a key business enabler, which was interesting as they then went on to report that secured solutions were not critical to their business solution or to helping them achieve any form of competitive advantage. Of the respondents who identified a high turnover rate of security staff, APAC had the highest. APAC also had the least of the required skills and competencies to meet the security demands of their operating environment. This staff statistic is in line with the region also having the highest number of security staff being outsourced, and may, in the short term, help to explain why they are among the top regions in having experienced the most number of security breaches.

APAC was far ahead of the rest of the world in having their employees receive awareness and training on security and privacy issues and statutory compliance. APAC respondents had the highest number of policies that were described as *ad hoc* or “best efforts”. The lack of direction and clarity within these policies may be a contributing factor as to why only about 34% of the respondents were reporting on the right KPIs, or did any sort of measuring and tracking at all. If APAC continues to improve its accountability and governance structure, it would not take much effort to put them ahead in many of the areas that allow for a more secure organization. With the highest number of security staff being outsourced in relation to other parts of the world, it is no surprise that APAC also felt that they were investing less in security.

**“One of the questions most frequently asked by executive management and members of the Board is, how is their organization doing compared to other organizations in the sector. The Deloitte survey provides an excellent means of providing the benchmark information that executive management and the Board want to see.”**

Global Security Survey Respondent

### Latin America and the Caribbean (LACRO)

LACRO demonstrated that they were ahead of most, and tied with Africa, when it came to holding their security staff responsible for a secure organization. All respondents acknowledged that they had defined and documented job roles and responsibilities for their security staff, yet went on to say that no LACRO financial institutions were doing any form of reporting on KPIs. This finding may be partly explained by the fact that LACRO was also the region that had the least required skills, leading organizations to hire the most specialized staff, requiring them to give more direction, resulting in less autonomy. This finding correlates with the response to the number of applications having an identified owner, where they shared the top spot with Africa. Although responsibilities may be defined, it is almost impossible to measure whether they are being acted on accordingly, as only 20% of the respondents stated that they have clearly outlined senior management goals and that performance goals and metrics are used. Only 20% seek feedback in relation to the success of their security programs. In dealing with regulatory and legal requirements, 50% of LACRO respondents felt that not only did they have the required commitment from their organizations but that senior management funded them accordingly. Similar to last year, LACRO respondents were highly driven in terms of regulations and doing what they were required to do – “you tell me what I need to do and I will accomplish it” was the prevailing attitude. Over three quarters of the respondents felt that legal and industry regulations were the most influential drivers in ensuring privacy compliance.

### North America

#### Canada

Similar to last year, Canada was very competitive and compliance-focused, in that their decisions and activities were driven by what their competitors did, and they felt that their spending was in line with that of their competitors. This finding is partly due to the number of large banks in Canada and their experience of working together on industry-wide initiatives. Canada had the highest rate in terms of executive management commitment and funding when it came to security projects needed to address regulatory or legal requirements. Canada led the world when it came to understanding the link between security and business strategy. This finding may help to explain why Canada also had one of the highest percentages of reporting on the appropriate KPIs. Despite this finding, 30% of financial institutions still fail to use KPIs. Canada was the leader when it came to tracking and communicating security successes, both inside and outside the institution. Similar to other parts of the world, with the exception of the US, Canadian respondents felt somewhat concerned about the security/privacy paradox.

Canadian respondents were in second place of all respondents in having job roles and responsibilities for their security staffing; they were also tied for first place in the number of respondents who increased their security staff over the last twelve months. Less than half of Canadian respondents feel that they currently have the right mix of skills and competencies to adequately prepare themselves for the risks they are encountering. The other 40% feel that key skills are missing but they have a plan in place to quickly close the gap. When it comes to measuring accountability, all parts of the world fared poorly with Canada being no exception. Less than half of all respondents had an identified owner for all their applications, and less than a third had performance measures in place or took the initiative to seek out feedback in regard to the security programs success.

### United States

With the largest security staff and the greatest number of financial institutions with security strategies, it is not surprising that the US reported that they were likely spending more on security than any other part of the world, given the events of the last few years. They also felt that they were prepared to take higher risks and be the leaders in adopting new forms of technology. This is a similar finding to last year, when US respondents felt that their competitors had no relevance to the way they operated or spent their money. Of all the respondents, the US was least likely to have job roles and responsibilities documented for their security staff and, just over a third had an identified owner for applications. Although the US was least likely to have documented job roles and responsibilities, they were the most likely to have security linked to their employee appraisals, which raises the question of how effective this is if employees do not have clear guidelines and well defined roles in terms of what

they are to accomplish. Although the US was one of the areas that had security job loss, they did come in second for the number of security jobs being supplemented or outsourced. Only slightly more than half of the financial institutions felt that they had adequate skills and competencies to respond to the increasing number of threats. Even with increasing regulation and corporate scandals, over half of the respondents in the US acknowledged that their employees had received no awareness or training in relation to security, privacy and statutory compliance issues in the last 12 months. The US dominated other parts of the world when it came to dealing with the privacy/security paradox. US respondents felt more concerned – 18% more than in any other part of the world – about the conflicts between security and privacy regulations. This may partly explain their drive to pursue new technologies and undertake new customer-focused initiatives.

### Regional Highlights

	EMEA	APAC	LACRO	Canada	US
Financial institutions possessing a security strategy	89%	71%	50%	70%	82%
Financial institutions who perceive security to be a key part of their solution	63%	29%	50%	50%	64%
Financial institutions who are reporting on the right KPIs	44%	34%	0%	40%	52%
Financial institutions with a security staff of less than 40 employees	68%	86%	100%	70%	62%
Financial institutions who feel they presently have the necessary required skills and competencies	58%	14%	0%	40%	54%
Financial institutions who feel they have both the commitment and funding to address regulatory requirements	83%	66%	50%	88%	69%
Financial institutions who experienced flat budget growth	28%	40%	0%	50%	29%
Financial institutions who experienced a budget growth	56%	60%	50%	50%	64%
Financial institutions who report that security success is tracked and measured	29%	50%	50%	80%	46%
Financial institutions who have been compromised in the last 12 months	47%	71%	50%	44%	24%

# Key findings of the survey

The following points summarize the highlights of our research:

**1** **Size does matter.** When comparing the responses of the larger financial institutions (over 5B in revenue annually) to that of a smaller revenue base (under 5B in revenue), the results were not surprising. In most cases, the larger the organization, the more mature its security programs. Perception of security and its importance to the business was consistent across organizations of all sizes – most saw it as a risk management exercise that is key to the business. Executing on this perception is where they diverged, as 12% more of the larger organizations had a security strategy in place and over 16% more of the smaller financial institutions were doing very little in their attempts to measure the security programs success. Though smaller financial institutions did attempt to identify and report on KPIs, large financial institutions were close to 100% more likely to be reporting on the right ones. Larger financial institutions demonstrated a greater maturity in security programs as a whole. Whereas 28% of the larger organizations had a security staff of over 100 personnel, 42% of the smaller organizations had a staff of less than 10.

The outsourcing of security functions was more likely to occur in larger financial institutions as was having the required skills within the organization to meet current demands. The smaller financial institutions struggled to find and attract staff with the adequate skills and competencies required to protect the organization from perceived threats. Budgets are a likely factor, although the majority of budgets of large and small financial institutions remained relatively flat: 15% of the larger financial institutions saw any form of budget increase, and over 23% of financial institutions saw an increase over 20%. These increases contributed to the fact that larger financial institutions felt that their management was doing a better job when addressing personnel compliance issues – both in terms of commitment and

funding. As with last year, most respondents anticipated either meeting or exceeding the old rule of thumb; one information security professional per 1000 users. From last year's study, we concluded that this metric is no longer valid or meaningful. However, for the sake of measuring this metric, it appears that this ratio is currently at 1:650.

**2** **Amid the onslaught of regulatory requirements – many of them, open to interpretation – global financial institutions are doing their best to adopt better practices and security standards.** The survey highlighted that most financial institutions are attempting to demonstrate how the controls they have implemented to achieve security align with relevant regulations and the demands of their customers. Respondents' answers reflected the importance to them of company brand, data protection and customer loyalty. To inspire stakeholder confidence in their security governance, global financial institutions are approaching security in a comprehensive manner, with the adoption of industry standards such as COBIT, ITIL and ISO 17799. Although Sarbanes-Oxley directly affects SEC registrants, organizations around the world are using the Act's requirements as a baseline for the development of security programs. Other regulations such as the European Data Protection Directive and the Gramm-Leach-Bliley Act of 1999, require specific actions. Financial institutions are adopting principles such as those within the ISO 17799 standard for the initiation, implementation, and maintenance of their information security program. The ISO 17799 standard functions as an international benchmark that financial institutions can use to determine whether they or their business partners have adequately addressed the policies, plans and procedures to create a comprehensive information security management system.

**3** Creating an effective security awareness program for employees aids in the identification and protection of the organization. Raising employee awareness of data protection and security issues is a necessary component of an organization's compliance with legislation and regulatory requirements. Even though the majority of respondents perceived security and privacy as a risk management exercise driven by regulatory requirements and country legislation, the perception has resulted in an increase in training and awareness programs in many financial institutions. Specific regulations such as the US Bank Secrecy Act (BSA) and the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (US PATRIOT ACT), as examples, require all US-based financial institutions to conduct ongoing, updated training for their personnel around the issues of anti-money laundering. Programs of this nature are taking place at a global level as well; as the Organization for Economic Cooperation and Development's Financial Action Task Force on Money Laundering have similar requirements in their report "40 Recommendations". Other proactive financial institutions are using training and awareness programs in various locations worldwide to uphold consistent ethical standards and security practices. Developing an effective information security awareness program is a key component of any successful information security strategy, as it provides a financial institution with a more knowledgeable workforce and it allows financial institutions to improve in other areas where they are currently lacking. The majority of respondents did not have security linked to performance appraisals, making it difficult to hold people accountable for protecting data. As high-quality, low-cost, web-based training becomes more widely accepted, financial institutions will be able to measure the effectiveness of their security programs and, at the same time, communicate to their employees their responsibility to protect sensitive information as well as to proactively identify potential threats.

**4** Responding to new legislation and regulations along with the goal of reducing costs, the value of IT assets is a strategic priority within many financial institutions. Financial institutions are paying much closer attention to what they own as they seek out industry best practices, on how to manage and account for assets. A year ago, the majority of our respondents had difficulty answering questions related to the management of their intangible assets such as software and software licensing. Now, new regulations are holding financial institutions accountable for exactly what assets they own, what information they may contain, who is accessing them, where they are located and whether the true value equals that stated on the balance sheet. These requirements have defined the need for effective asset management practices, as financial institutions that cannot answer these questions cannot demonstrate that they have secured their data appropriately and met their fiduciary responsibilities. Although such regulations are dependent on whether the financial institution is public or private and the geographies in which it operates, benefits associated with effective asset management extend the scope of compliance and risk mitigation. Effective asset management practices are being aligned with business strategies in the creation of market competitive offerings and increasing productivity. Enterprise asset management is proving to be a strategic approach to reducing costs and generating more efficient operations.

**5** Moving business processes to locations with lower labor and real estate costs is not new but security and privacy have not caught up yet. There has been a surge, over the past 12-18 months, in outsourcing (offshoring) systems development, application development, management and call centers to remote locations, in an attempt by FSIs to increase their profit margins. Canada, China, India, other far east countries, and the UK are emerging markets to which financial institutions are looking to offshore their operations. It is estimated that the financial services industry employs over 13 million

**“Privacy concerns lie at the heart of the institution's ability to adequately protect the confidentiality of personal data that is no longer within the physical boundaries of a company.”**

Global Security Survey Respondent

people worldwide and Deloitte estimates that 15% of this headcount is moving offshore to help financial institutions achieve dramatic cost reductions. Although job loss is the primary criticism of offshoring, equally important is the concern around consumer privacy. Survey results indicate that although financial institutions may be willing to outsource a wide range of business processes, including IT, the majority of them are not prepared to outsource critical security functions. As the number and sophistication of security threats continue to increase, smaller financial institutions find it difficult to justify keeping all functions in-house. One way to meet security requirements is to increase the pool of expertise and hire more security staff. The survey demonstrates that the majority of respondents are already facing difficulty in finding and hiring staff with the required skills and competencies. As well, the majority of their perceived threats revolve around non-core functional areas, like patch management and viruses. By outsourcing non-strategic security functions, financial institutions may be in a better position to concentrate on their core business while working with their outsourced service providers to enhance their security infrastructure and support their growth initiatives.

**6** Creating a competitive advantage out of rapid change and environmental turbulence requires financial institutions to maintain strategic flexibility.

September 11, 2001 was the ultimate test of the business continuity management programs of scores of companies. Almost two years later, on August 14, 2003 business continuity management plans were tested again with the US/Canada northeast power system outage. The final report issued in April 2004 by the US/Canada Power System Outage Task Force puts the losses in the neighbourhood of \$8-12B. As the number of unanticipated external disruptions continues, and

financial institutions continue to be highly interdependent, focus on building more resilient businesses and operating models to minimize the impact of unforeseen events will become mandatory. For financial institutions to effectively build resiliency strategies, they need to not only attempt to identify the risks they face and install the appropriate mitigating technologies, but also to act swiftly to integrate all areas of security affecting their organization with their corporate strategies. It has become clear that financial institutions will need to create competitive advantage out of their ability to respond to rapid change and environmental turbulence. Only then will they be in a position to move from simple recovery to experiencing the benefits associated with the continuation of business operations that are in line with the corporate strategy of facilitating growth and profitability.

Only a very small percentage of respondents felt that their strategic and security technology initiatives were well aligned. The survey showed small steps forward as financial institutions slowly begin to focus on optimizing the availability of all mission critical assets: people, data, technology, facilities and core business. This progression was reflected in the types of security measures respondents implemented or maintained over the last 12 months. As the perception of security continually evolves from that of a strictly IT issue, resiliency strategies will take into account multiple variables, like a severe loss of personnel or cyber terrorism. The survey identified that only about half of the respondents take personnel into account within their business continuity plans. With the lack of a holistic approach, financial institutions will find it difficult to adequately redistribute their executive management and critical personnel across geographies and offices in the event of an incident causing massive people loss.

**7** While the privacy policies of many FSIs are still driven by regulatory measures in the countries where they operate, a well-devised privacy strategy can be a major asset in attempts to stay ahead. The responses that showed the most improvement over last year was in the area of privacy. We attribute this to the increasing focus on privacy-related concerns, through legislation, industry self-regulation, and customer expectations. The survey identified that neither organizational size nor geographical region had a large impact on the fact that most respondents identified security and privacy as a risk management exercise required to protect brands, and prevent legal mishap. However, as the world becomes more digitally dependent and open, the security/privacy paradox becomes a major concern. The survey demonstrated that some FSIs treat privacy and security as one and the same. In some financial institutions, the security and privacy function share the same policies, processes, security privacy programs and even the same executive in charge. The difficulty with this approach is that security and privacy have their own objectives, their own goals, and their own requirements – differences that dictate the need for the two areas to be examined separately. A good example of one area infringing on another is when rigorous security processes actually contribute to a misguided privacy policy that makes it impossible for customers to have access to sensitive information which they are entitled to under various privacy regulations. The survey identified that although the fear of customer data being inappropriately accessed was the number one concern of the privacy function, less than half the respondents had the protection of customer data under the control of the Chief Privacy Officer. To avoid falling into this or a similar trap, innovative FSIs are creating separate structures, and soliciting feedback from all functions involved in the creation, exchange, and storage of information. FSIs that act first to link privacy and security to consumer trust and loyalty will achieve competitive advantage – even if the methods by which they achieve that objective need to adapt in the future to reflect a changing technological, regulatory and competitive landscape.

**8** The concepts of identity management and vulnerability management process are starting to get some real traction. In a recent survey of 175 Fortune 1000 companies, technologies were ranked according to their immediacy of planned implementation and level of security spending. Identity and vulnerability management were classified in the top quartile of a field of 15 technologies.

Many FSIs have long recognized the necessity for strong identity management for specific business applications and transactions. However, with the increase in identity theft and the level of sophistication of threats and fraudulent activities, many FSIs feel compelled to adopt solutions that are for wider use.

In January 2004, the US Federal Trade Commission reported that it received over half a million complaints in fiscal 2003 that represented in excess of \$4M in losses.

When we asked how many companies had experienced security breaches of some kind last year, approximately 39% of companies responded that they had. This year to that same question, 83% of companies responded in the affirmative. The greatest increase in security breaches has been in the area of worms and viruses, many of which have emerged in the last quarter of 2003 and first quarter of 2004. They have had a significant impact on organizations around the globe. The recent Sasser worm (May, 2004) was so fast moving that many organizations were not equipped to cope with the pace and, as of this writing, many companies are still dealing with its ramifications.

Many FSIs are realizing that a vulnerability management solution is required to properly manage the associated risks. The process would include:

- A schedule for automated vulnerability scans
- A way of detecting rogue devices on the network

- A way to track and manage repairs to the vulnerabilities identified and a method for establishing accountability for repairs
- A way to correlate vulnerability data with attack activity
- The ability to generate reports that detail vulnerability for compliance and auditing activities.

In an article by Gartner Consulting entitled *Top 2004 Predictions for IT Security Directors*, one of the key predictions was that enterprises that implement a vulnerability management process will experience 90 percent fewer successful attacks than those that make an equal investment in intrusion detection systems only.

**9** Financial services consolidation is a way of life but security remains an afterthought. A number of high profile mergers and acquisitions have taken place in the financial services industry across all sub-sectors, geographies and sizes. This wave was best seen when we attempted to re-approach last years' respondents with the opportunity to participate in the 2004 Security Survey and some organizations who responded separately last year were now one large organization. This wave is expected to continue. Information security and privacy, along with IT-related controls are not at the forefront of activities and considerations, leading to some gaps and threats. Across the industry, there are no consistent and proven industry best practices on this topic, leading to a longer timeline in achieving the intended level of security and IT controls and, in many instances, to the adoption of tactical solutions.

**10** Security is moving from the war room to the board room. As is often the case in responding to times of crisis, the regulatory and industry response to 9/11 and to corporate failures has been inconsistent. This inconsistency will result in future incompatibilities among nations, industries and organizations. As the economy adjusts, friction caused by the increased controls and incompatibilities will redefine trade patterns and relationships.

A survey of attendees at this year's World Economic Forum (WEF) Annual Meeting found, by a ratio of more than two to one, that members believe the next generation is likely to live in a more prosperous world (59%) but not a safer world (27%). They also believe that the outlook for their personal security is better now (65%) than it will be in ten years' time (41%).

The majority of the WEF members believe that 40% or more of their company's market capitalization is represented by brand and reputation. The conclusion from this is that perception and the resulting risk to shareholder value are actually a greater threat than the loss of specific assets. When people refer to the dynamics of trust and its place in today's business model, it is undoubtedly the concept of brand image to which they are referring but it has no concrete value assigned to it. Trust is subjective and can be severely damaged if there is the slightest belief that it can be undermined.

The results of the WEF survey and our own global security survey highlight the following findings:

- executives rank security as a high priority and security initiatives are seen as a good investment
- security is a business issue driven by shareholder value, customers' perception, brand and reputation protection, legal and regulatory compliance, vulnerability and sustainability
- executives are beginning to understand the importance of an overall capability to prevent, prepare and respond in an uncertain environment

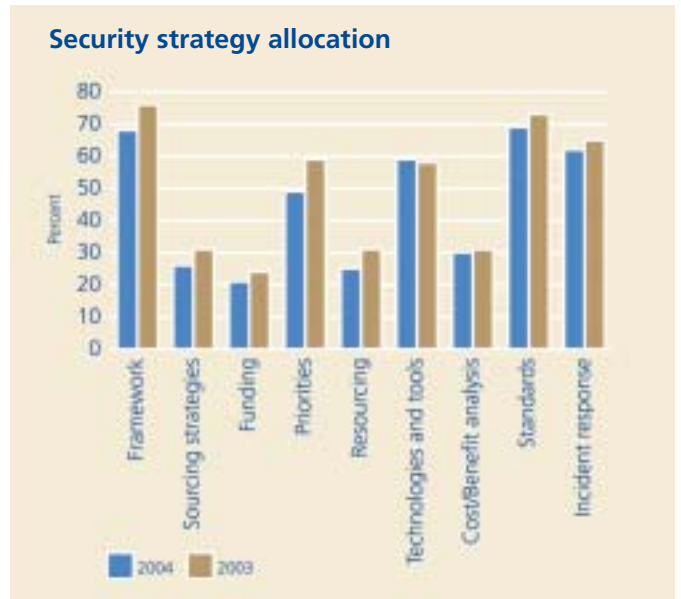
Private industry owns approximately 85% of the critical infrastructure in the United States and 80% globally. The vulnerability of these assets increases with the volume, speed and efficiency of commerce and it is up to the private sector to protect these assets. The challenge lies in applying continuous, integrated risk management to business decisions and daily operations.

# Governance

Over the last year, we encountered an interesting phenomenon: the total number of respondents that have a formal information security strategy actually decreased from 80% to 75%. North American & EMEA respondents were the only regions to have a security strategy (over 80%). However, improvements were evident; whereas last year only 47% of the respondents felt that the strategy was led and embraced by its functional and line managers, this year the number has grown to 54%.

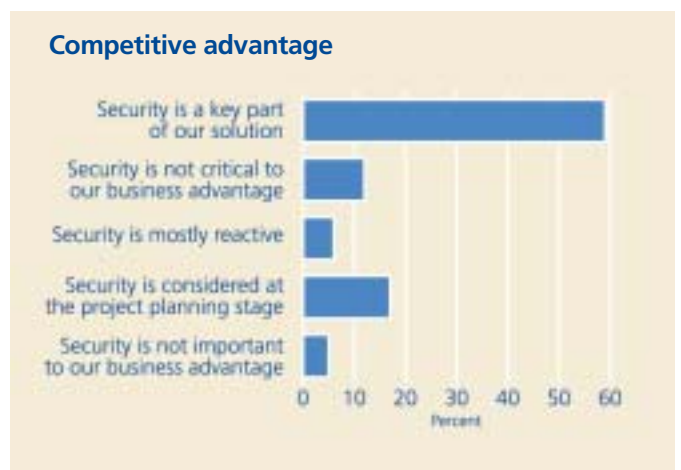


The attributes of the respondents' formal information security strategies are relatively consistent with those of last year's respondents. The use of the security strategy in helping identify priorities was lower than that of last year, which may help to explain why the majority of respondents felt that their security priorities were misaligned with those of the business.



Although the majority of respondents identified security as key to creating a competitive advantage in the marketplace, 40% of FSIs still do not think it is significant:

- Security is a key part of the solution: 59%
- Security is not critical to our business advantage: 12%
- Security is mostly reactive: 6%
- Security is considered at the project planning stage: 17%
- Security is not important to our business advantage: 5%



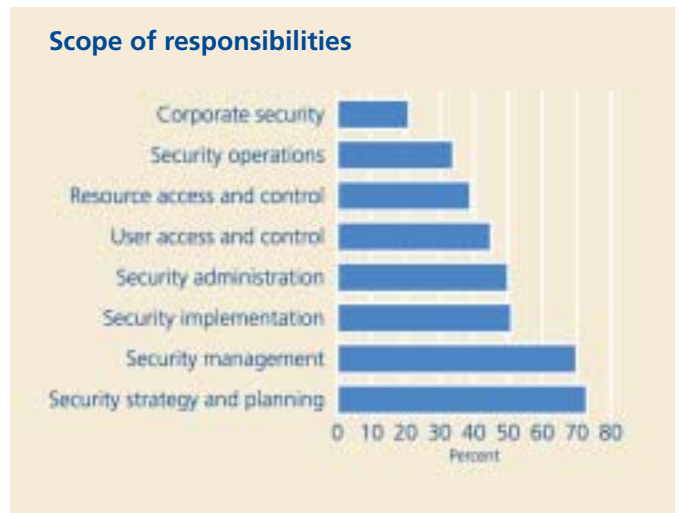
“Lack of internal security awareness is still one of our biggest threats.  
Technology can reduce risks to a point but it is people who are the weakest link.”

Global Security Survey Respondent

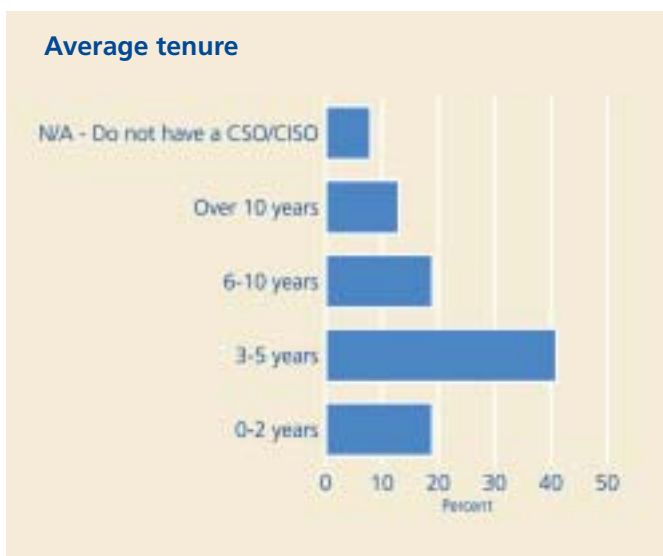
Chief Information Officers were identified as the most common position to which Chief Information Security/Chief Security Officer report:



Within the scope of responsibilities for the CSO/ CISO, security strategy and planning, and security management were the most prevalent with 73% and 70% respectively. Interestingly, the number drops dramatically to 51% when it comes to implementing and administering security.



Of CSO/CISOs, 40% have had a tenure between 3-5 years:

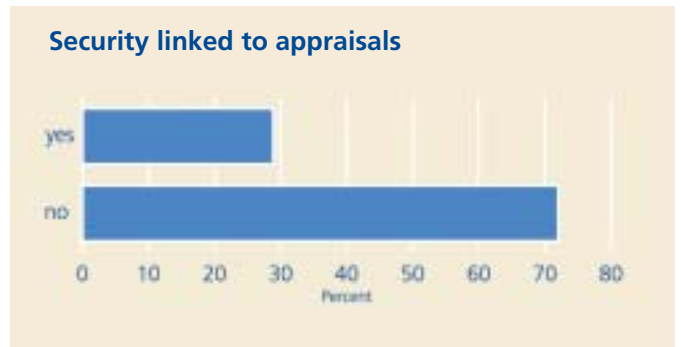


Knowledge of security risk resides mainly within the senior to middle management ranks of the respondents' organizational structures. Clearly, the executive team cannot wait passively for evidence that security is insufficient, and they need to be involved in the process of risk identification while receiving continuous feedback on the effectiveness of security program performance. If these control mechanisms are in place, and executive management have defined clearly stated management objectives, then having the majority of knowledge residing within the middle ranks will work. It will then be middle management's role to identify the ongoing performance measures to form an important feedback mechanism for executives to assist in making decisions about IT investments, human resource allocation and security strategy.



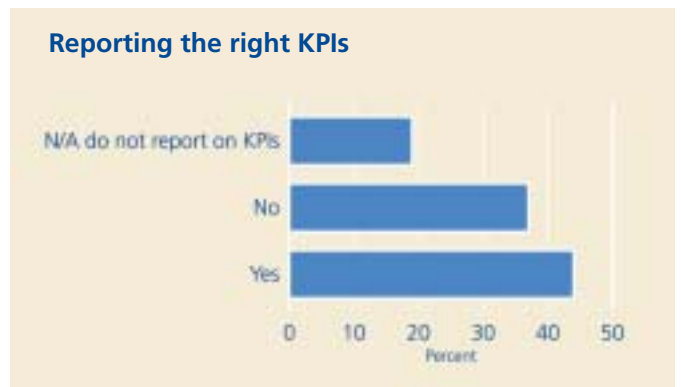
Improved security practices are slowly being implemented, as the structure and programs of financial institutions mature over time and through experience. One practice that has not seen a lot of growth is holding the IT and security personnel accountable for their performance in relation to security. Only 54% of respondents indicated that their security strategies were embraced by line and

functional business leaders, which may help to explain why 72% admitted that security was not linked to the performance of their IT and security staff.



- Security is linked to your IT/Security staff: 28%
- Security is not linked to your IT/Security staff: 72%

Scorecards, KPIs and security dashboards are the hot tools in the security community. KPIs allow FSIs to measure a particular organizational performance activity, or act as an important indicator of the precise health condition of the FSI. The difficulty in the use of KPIs lies with their identification and definition. In order to be effective, KPIs need to be defined as succinctly as possible and the information needs to be consistent. These difficulties are reflected in the survey answers; the majority of respondents indicated that the security function is not using the KPIs that executives require to improve their security programs.



As the financial services industry environment continues to change, FSIs must continually prepare themselves to respond to a variety of security scenarios. The survey revealed that just over half of respondents feel that they currently have the skills and competencies necessary to handle existing security requirements and those that do not, are adequately closing the gap. This feeling is consistent with their levels of confidence as it relates to protecting themselves from internal and external attacks.



Across the globe, there is a movement toward improved corporate governance as FSIs focus on meeting emerging regulatory requirements. As FSIs better understand the cost of losing consumer trust due to negligence and corporate scandals, corporate governance standards remain a critical issue for the financial industry. This attitude helps explain why 69% of the respondents feel that they have both the senior management commitment and the proper funding for security projects needed to address regulatory or legal requirements.



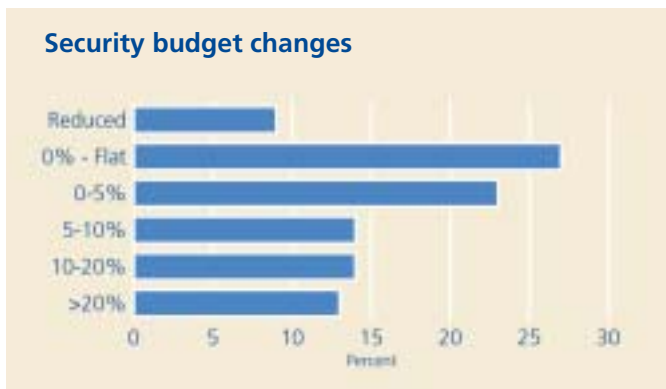
It was interesting to note that although 79% of the respondents indicated that their CSO/ CISOs played an active role in the financial institution’s efforts to become compliant with regulations, only 36% of respondents indicated that there were senior management objectives in place. Despite this, 69% of respondents still feel they have responded well to compliance requirements and 74% feel that they have the adequate commitment and funding from executive management.

The majority of respondents indicated that the security function responded well to regulatory compliance and transparency requirements mandated by regulations:

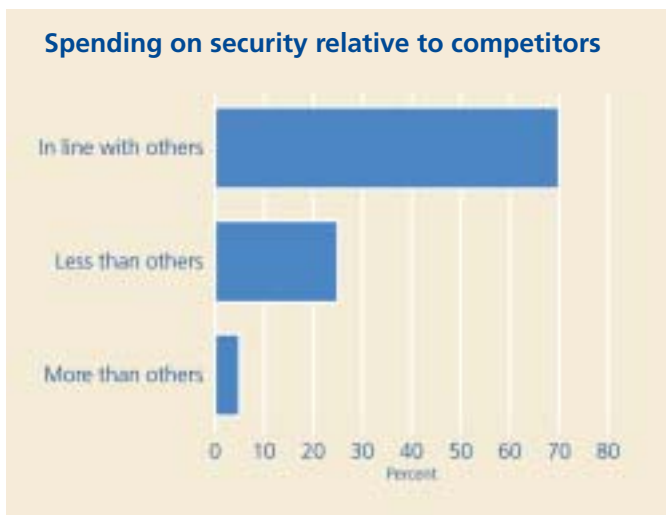
- Yes: 69%
- Partially: 21%
- No: 5%

# Investment in security

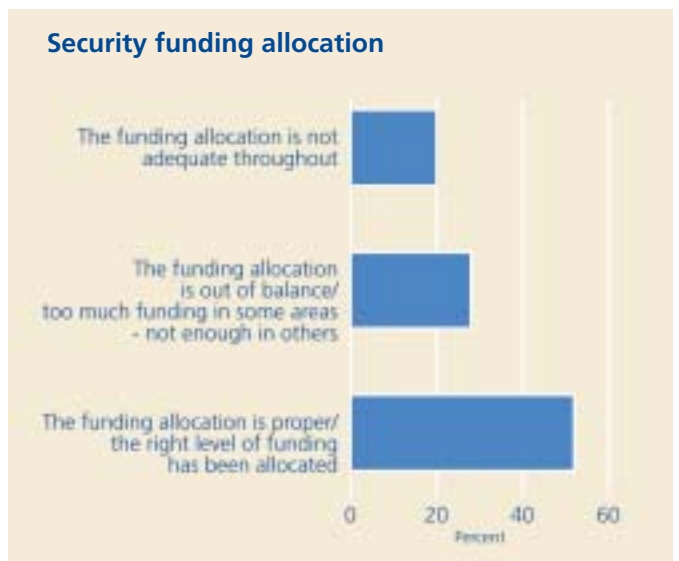
The financial services industry has exhibited substantial volatility when it comes to security spending. As FSIs respond to the unprecedented events of the last few years – the bursting technology bubble, the collapse of corporations due to improper financial reporting, war and terrorism, and increasing regulatory pressures-FSIs are attempting to win back the confidence of their customers through increased spending on privacy and security. Across the globe, 25% of financial institutions witnessed a zero percent growth rate in budget. The US was the region which experienced the greatest budget growth while financial institutions operating within LACRO witnessed the greatest reduction.



The majority of respondents indicated that they would characterize their spending on security as in line with other comparable organizations and, for the most part, in line with their own security plans.



In terms of funding allocation, the majority of respondents felt that money was either appropriately allocated to the right areas, or that some areas were misaligned. The areas that saw the most growth internally were People and Payroll, at more than 13% with Hardware and Security Tools close behind.



Echoing the differences of IT budgets allocated across the globe, the percentage dedicated to security varied from region to region. On average, the percentage of spending on security compared to IT budgets, remained relatively constant from last year at about 6-7%. However, this year, we have had a number of respondents who have not been able to respond with an exact figure, or elected not to provide figures.

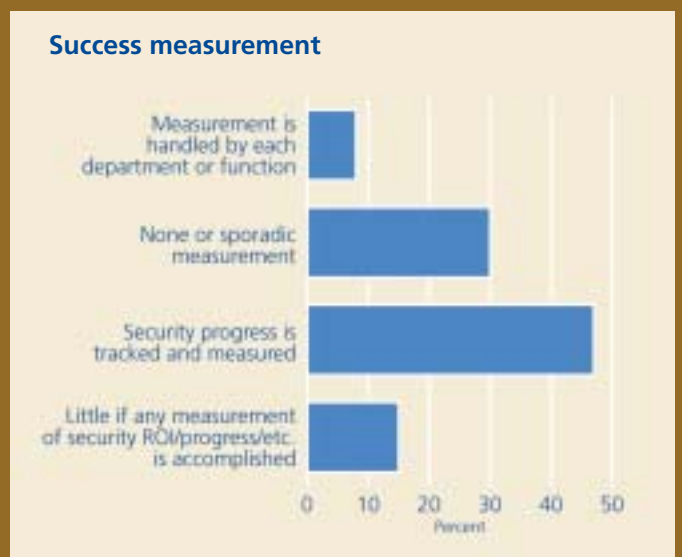
We have observed that this year, in Africa and APAC there was a surge in comparison to last year, while in North American and EU countries, the percentage of spending remained relatively constant. In the industrialized world, few countries, including Australia, Canada, Japan, New Zealand and Spain seemed to be doing more with less, with an average security budget of 1-3% of the overall IT budget. The US remained almost unchanged from last year at a 6-7%.

*IT management processes are fundamental to the organization's controls. IT needs to be at the table, working concurrently with the lines of business and finance groups.*

# Value

Consistent with the finding of last year, management still perceives spending on IT security as a risk management exercise. Due to the influx of newspaper articles outlining security breaches, increased regulation and corporate governance pressures, more money and attention is being spent on attempts to win back consumer trust, building loyalty and being the sole provider of customers' needs. When it came to measuring the success of security

investments, respondents indicated that the majority of organizations are attempting to conduct some form of measurement. This result is in line with the results around the increased use of performance measurements but also demonstrates that the practice is still in its infancy, as the right metrics for measurement may not be fully understood and/or correctly identified.

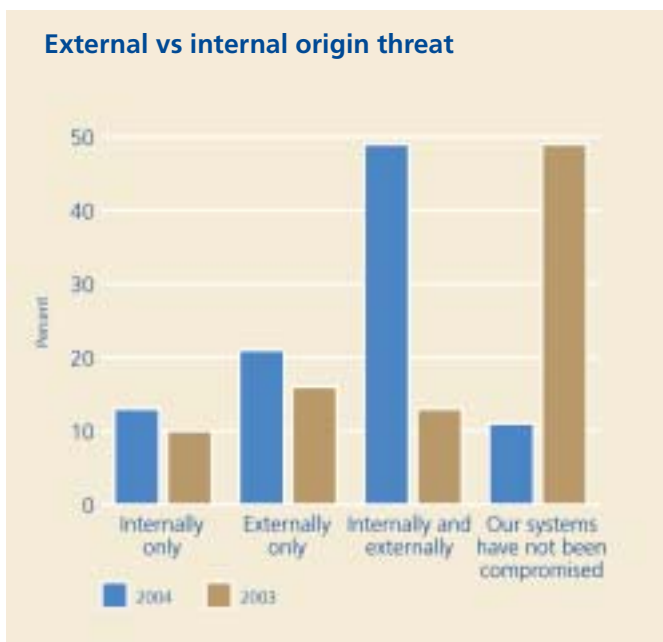


# Risk

The convenience of being able to pay one's bills online, use web services and submit electronic claims is offered to us through emerging technologies and innovative solutions. However, with this convenience comes the inevitable increase of online card fraud, identity theft, phishing and viruses, among many other threats. Like never before, this technologically advanced era highlights the fine line between openness and exposure. This balancing act leads financial institutions to ask, How well prepared are we, and Do we understand the risks that confront us?

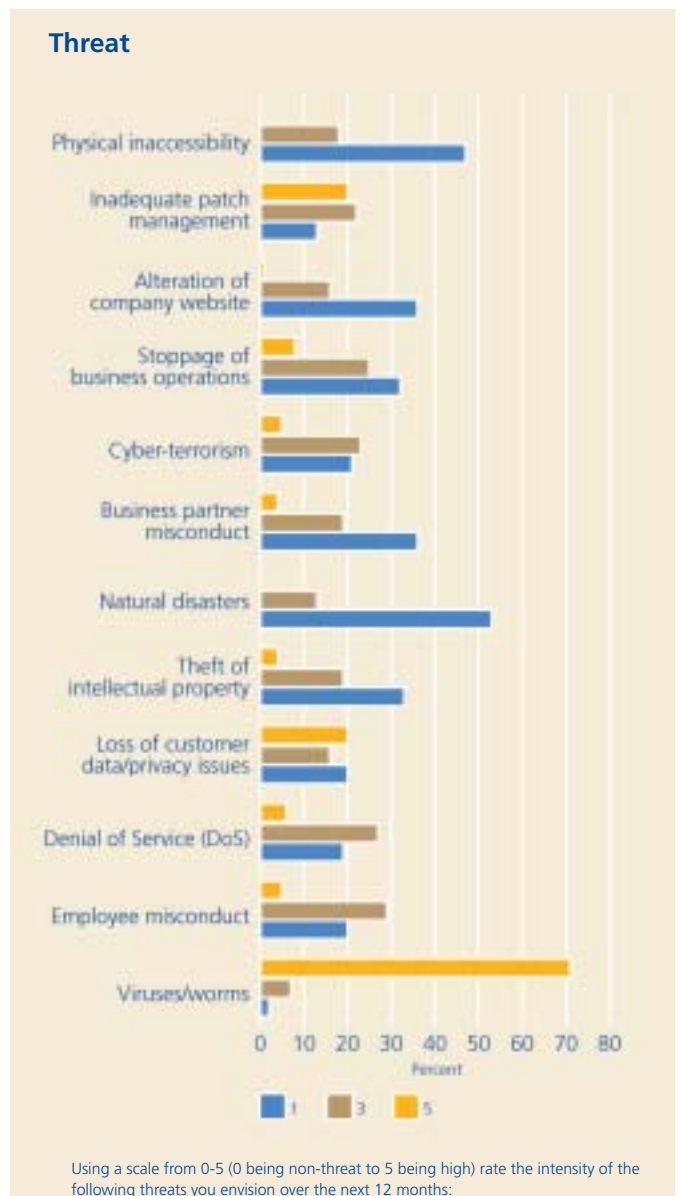
In total, 83% of respondents acknowledged that their systems had been compromised in some way within the last year. Similar to last year, outside intrusions were more common than those from the inside; the majority of respondents have experienced both:

- 21% report attacks from an external source, compared to 16% last year
- 13% report attacks from an internal source, compared to 10% last year
- 49% report attacks from both sources compared to 13% last year



When asked to rate the intensity of various threats over the next 12 months, respondents were most worried about viruses and worms, loss of customer data and being inundated with patches. Employee misconduct was rated high but not severe, a reflection of improved internal security measures and an increase in employee training and awareness.

Eighty-nine percent of the respondents felt that having a risk management process within their organization was either very or extremely important, and 81% identified risk management as part of their strategic planning exercise:



- 81% report that risk management is part of strategic planning
- 16% report that risk management is informally considered
- 3% report that they have no strategy in place around risk
- 0% report that risk is not even considered

Similar to last year, the majority of respondents are confident that their networks are protected from cyber attacks (e.g. DOS attack, malicious code, sabotage etc.) but the number who feel extremely confident has decreased both internally and externally.

For the second year, respondents are still comfortable relying on the risk tolerance levels of their competitors:

- Less risk than the industry as a whole, even at a higher cost – 29%, compared to last year's 27%
- More risk and a lower cost than the industry – 10%, compared to last year's 15%
- Same risk as the rest of the industry – 45%, compared to last year's 35%
- Ignore our competition – 10%, compared to last year's 8%

In contrast to last year, when the majority of respondents strived for a risk level that was "effective and efficient", this year, respondents were split between being efficient and taking only the level of risk necessary:

- 30% of the respondents strive to take only the risks necessary, compared to last year's 19%
- 44% of the respondents strive to be effective and efficient, compared to last year's 62%
- 13% of the respondents indicated that they still wanted to be "world class and bullet proof", compared to last year's 6%



In contrast to last year, when the majority of respondents had a difficult time answering questions around their intangible assets such as software and software licenses, this year's respondents were able to answer and felt confident that they were compliant.

# Use of security technologies

Consistent with last year's responses and in line with the cautious attitude exhibited around risk, respondents identify themselves as "effective users of demonstrated technology". Only 9% of the respondents were willing to take the risk associated with being an early adopter, which may also help explain the high confidence respondents have in relation to preventing attacks.

Although financial institutions are increasing their wireless offerings around the world aimed at reducing customer dependence on branches and call centers, little is being done to proactively protect themselves from internal wireless communication exposures:

- 45% have scanned the network to identify rogue wireless networks, compared to last year's 41%
- 33% have issued employee guidelines for the safer use of Wireless Fidelity(WiFi), compared to last year's 29%
- 59% have instituted security policies related to organizational wireless usage and acceptance, compared to last year's 49%

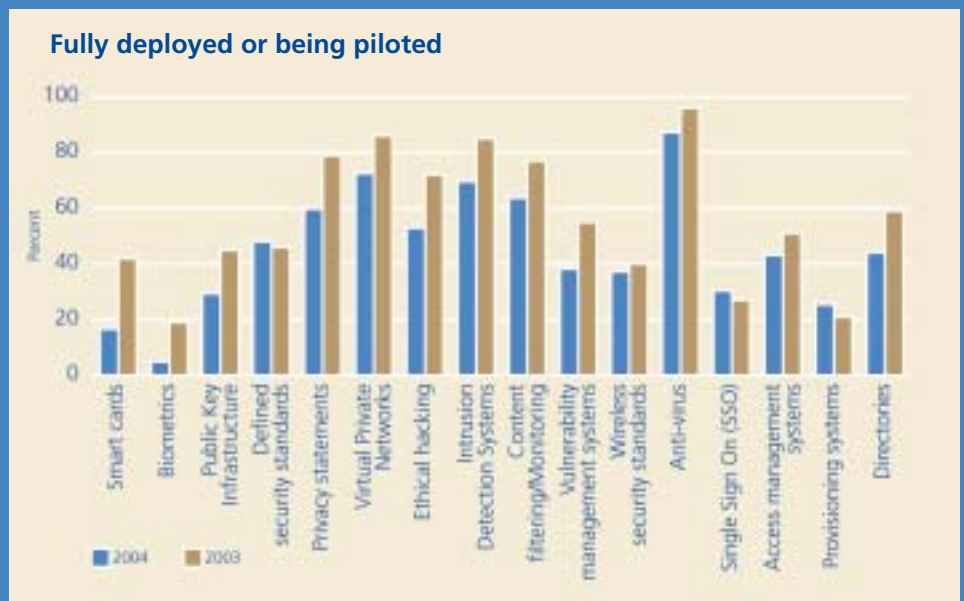
It came as no surprise, the high rate of adoption of certain technologies such as anti-virus, VPNs, intrusion detection systems and privacy statements.

The following technologies were either being deployed or piloted within organizations:

- Defined security standards – 52% deployed and 14% piloted
- Privacy statements – 68% deployed and 3% piloted
- Intrusion detection/prevention systems – 76% deployed and 9% piloted
- Access management – 54% deployed and 4% piloted
- Provisioning systems – 30% deployed and 13% piloted
- Directories – 56% deployed and 4% piloted

In an effort to understand how respondents felt the landscape would be changing, we asked what technologies they would be deploying over the next 18 months:

- Defined security standards: 19%
- Intrusion detection/prevention systems: 15%
- Access management: 14%
- Provisioning systems : 15%
- Directories : 22%



# Quality of operations

Technology and other project initiatives have grown faster than the ability of most financial institutions to manage them. Creating a competitive advantage out of environmental turbulence requires financial institutions to maintain strategic flexibility that enables them to better prepare for what they cannot predict.

As the number of unpredictable risks continues to climb, financial intuitions need to focus on building more resilient businesses and operating models to minimize the impact of unforeseen events.

For many of the respondents, building a resiliency strategy is not just about understanding the risks, options and economic trade-offs; it is about having an alignment of its people, processes, technology and functional strategies. It was interesting to note that only 26% of the respondents felt that their strategic and security technology initiatives were well aligned:

- 65% of the respondents felt that their strategic and security initiatives were somewhat aligned
- 9% of the respondents felt that their strategic and security initiatives were not appropriately aligned

With increasing scrutiny on security budgets, and the increasing number of organizations who are monitoring security performance, it was not a total surprise that 63% of organizations have deployed and are using customized security technologies. What is somewhat surprising is that 32% feel that they are not being utilized effectively.

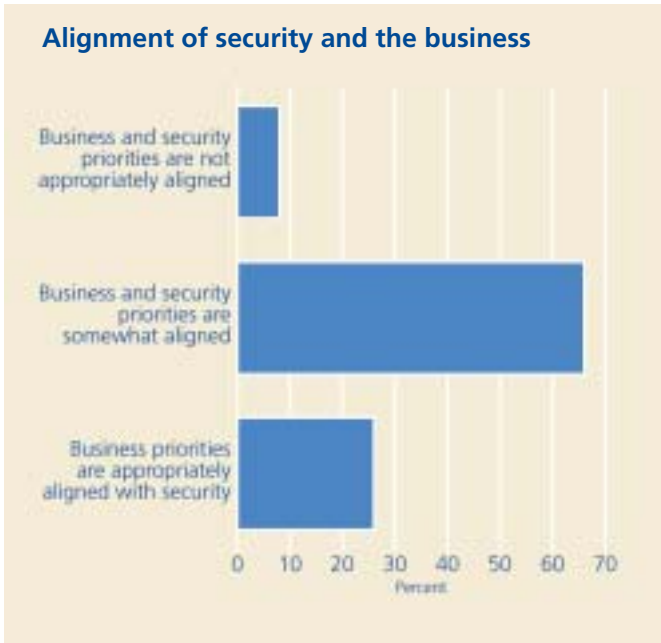
As respondents attempt to make their organizations more

resilient, they structure their human, physical and technical resources to be able to operate continuously when disaster strikes. This is reflected in the types of security measures respondents have implemented or maintained over the last 12 months:

- Security policy: 84%
- Business continuity planning: 75%
- Security training and awareness: 77%
- System security tools: 75%
- Business continuity plan testing: 70%

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

- 91% of the respondents say that their organizations have one, compared to last year's 88%
- 54% characterize themselves as "very confident" that their backups either work or are being stored off site in accordance with policy, compared to last year's 43%
- Testing was the most prevalent component within the respondents business continuity management programs at 71%



In line with respondents' belief that security is still mainly an IT issue, and that only 51% of the respondents take into account personnel within their business continuity plan, it is logical to assume that the majority of organizations have not adequately geographically redistributed their executive management and critical personnel in the case of an incident causing extreme loss

of personnel. A well-conceived deconcentration strategy goes beyond people, and extends to the structure of telecommunications, power and transportation grids. Telecommunications failure was identified as the second major cause of downtime within respondents' critical business systems.

As organizations attempt to achieve security in an open environment, an increasing number are choosing to focus on their core competencies and outsource those functions that are not considered central to their business. As a result, security functions (firewalls, IDS, VPNs, scanning, vulnerability assessment) within the IT infrastructure are experiencing the move from in-house control to outsourced management.

**“The Deloitte survey is a valuable tool that we can use to assess and benchmark our firm's information security against our counterparts in the financial services industry.”**

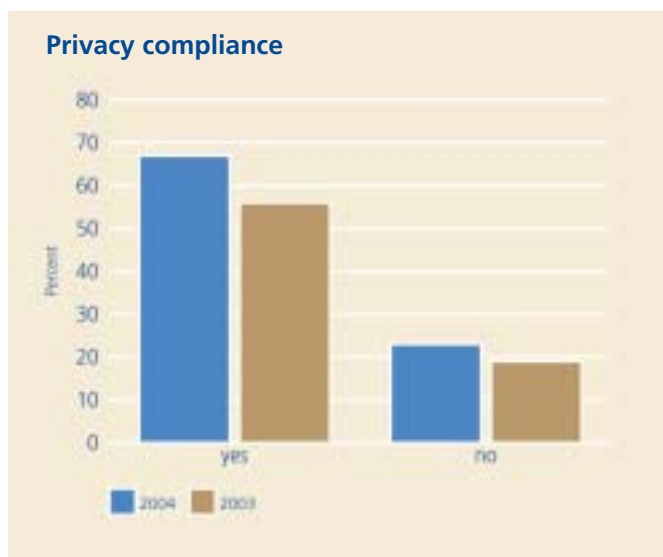
Global Security Survey Respondent

# Privacy

The concept of personal information privacy has been discussed by writers and philosophers for hundreds of years. Privacy for corporations has evolved into a well-defined methodology, documentation of information systems, data uses and requirements. As this survey has indicated, trust is a major concern for financial institutions. When privacy protection is properly executed, it is a key contributing factor in building and maintaining trusted relationships.

It is encouraging to note that the number of respondents who had programs in place to manage privacy compliance increased from last year:

- 67% of organizations have a program for managing privacy compliance, compared to 56% in 2003



Of the respondents who had a Chief Privacy Officer in place, 25% of them were the same individual as the CSO/CISO. This combining of roles is at the root of the security/privacy paradox, where the question of whether the roles are one and the same is open to debate. To hold the same person accountable for two roles assumes that person has the awareness of strategies, methodologies, programs and information requirements for two similar but different functions. As the survey points out, the areas of concern are different. For security, the focus is on viruses and worms. For privacy, the focus is on unauthorized access to personal information and managing third party information sharing.

Respondents acknowledged the following top three areas of concern for privacy compliance:

- Unauthorized access to personal information
- Managing third party information sharing
- Managing customer privacy preferences



When asked how organizations view privacy initiatives, 46% of respondents indicated that they were focusing on risk avoidance, 25% were focusing on brand and reputation and 29% on compliance and legal and personnel issues. This is aligned with respondents' feelings towards the most influential drivers in ensuring that their organization achieves privacy compliance:

- Legal and industry regulation: 93%
- Reputation and brand: 64%
- Fines, penalties and potential litigation: 21%

The use of an “opt in” versus an “opt out” policy is still under debate and evenly split, with 53% acknowledging an opt out policy and 47% with an opt in.

Other areas related to privacy remained relatively consistent:

- Written privacy, fair information practices or data collection policies in place – 91%, compared to 76% last year
- Formal processes in place to deal with complaints about its personal information management practices or policies – 85%, compared to 67% last year
- Identification of the types of personal information that is collected and classified according to sensitivity – 60%, which is the same percentage as last year's
- Formal policies in place with respect to the destruction of personal information – 73%, compared to 59% last year



# Summing up and challenges

Financial services institutions that have mature structures and progressive operations have a more pragmatic approach to information security. These organizations are combining proven and effective technologies with their security strategies. To help them continually adapt and meet ongoing changes, they are undertaking rigorous efforts to define appropriate KPIs and to structure accountability in a way that is reflected in each individual's performance appraisal. **These organizations have a good understanding of the fact that technology, when appropriately secured, can be a key business enabler.** They are also prepared to protect themselves from that same technology that enables breaches.

One of the challenges to organizations around protecting their information is the fine line they must tread between opening themselves up to customers and partners for revenue growth and balancing this requirement with the cost of security solutions to prevent attacks. These days, the "return on investment" of being a hacker is good; hacking tools are getting more automated and require less skill to use. Motivation is high because the information that a hacker targets increases in value as it becomes more complete.

The way in which financial institutions respond to external attacks has come a long way since the Morris worm back in the mid 1980s. As virus attacks continue to rise and become more targeted (like the Sobig virus which was aimed at the Internet addresses of financial institutions), organizations need to continue to improve their overall resilience and business processes.

Threats such as identity theft, international money laundering and theft of intellectual property are areas most feared by consumers, spurred by their need to feel reassured that their financial institutions are treating their

information and their money appropriately. Long before Carl Shapiro and Hal Varian's book, *Information Rules*, hit bookshelves across the globe, organizations knew the power and opportunity associated with sharing information. What the book pointed out was how easily this could be done on a global cross-industry basis with the use of emerging technologies. As the world becomes more digitally dependent and open, the security/privacy paradox becomes more of a concern. The survey shows that some organizations consider privacy and security one and the same function, with the same policies, processes, security privacy programs and even the same executive, in charge. **But security and privacy have their own unique objectives, goals and requirements. These differences require that the two areas be examined separately.** In some organizations, rigorous security processes actually contribute to a privacy policy that makes it impossible for customers to have the required access to information to which they are entitled under various privacy regulations. Innovative financial institutions are splitting the functions and creating separate structures, as well as inviting feedback from all functions involved in the creation, exchange, and storage of information.

The last few years have produced many different strategies to thwart the risks of attacks on information. One of the most innovative was from Microsoft. Reminiscent of the "wild west", when bounties were offered to aid in the capture and prosecution of villains, the company's response was to offer a reward of up to \$5M for information leading to the arrest and conviction of hackers who attacked their software. Opinions were mixed as to the effectiveness of this and similar methods but they, nonetheless, highlighted the need for responses beyond traditional security and privacy practices. Today, our "sheriffs" are organizations such as the FBI, NSA,

CIA, Interpol and Scotland Yard. In many instances, these organizations have attempted to identify and capture those responsible for security crimes but many of the wrongdoers are still at large. As a result, organizations recognize the need to take matters into their own hands, by paying closer attention to industry standards and better practices. The best solutions are when these practices and standards are infused in proficient business processes along with awareness, education, training, technology and strategy.

Financial institutions are under pressure to achieve security in an open environment while not interfering with the corporate strategy designed to facilitate growth and profitability. The security function faces internal and external pressure to implement security and privacy solutions that add value. More emphasis has been placed on defining performance metrics and attempting to calculate the return on security investments. Defining value in the context of security solutions is challenging as many organizations look for models that can help measure security efficiency and effectiveness. A security solution alone is not the answer – there must be a way of measuring the value it brings and the efficiency that is created. The efficiencies must result in direct benefit to the stakeholders through increased revenue or reduced costs.

With constant change on the global competitive landscape, the future of the financial services industry is unclear. The proliferation of networks coupled with emerging technologies has meant new customer needs, new partnerships and unique business transformation opportunities that consequently expose financial institutions to new risks. Pressure to raise standards to meet corporate governance requirements leads financial institutions to constantly review how they measure, monitor, and manage performance in their business.

## About Deloitte's Global IT Risk Management & Security Services

As one of the largest groups providing IT Risk Management and Security Services in the world, Deloitte is able to leverage the business, industry, and geographic expertise of over 140,000 business professionals across hundreds of offices worldwide. Deloitte Touche Tohmatsu member firms' IT Risk Management & Security Services practice is uniquely positioned to help clients with cost-effective security solutions that are delivered locally where they are needed. We understand how business and technology successfully function together.

Deloitte boasts over 2500 IT Risk Management & Security Services professionals, with over 400 Certified Information Systems Security Professionals (CISSP) and 770 Certified Information Systems Auditors (CISA). We offer a robust, holistic approach to IT Risk Management and Security with our BSI Management System trained consultants and Lead System Auditors we help align your organization's key controls for ISO 17799 certification, and achieve certification to the BS 7799-2. In our experience, information security can be most effectively addressed through the following services:

- Threat and vulnerability assessments
- Application & business process control reviews
- Application security & control design
- Enterprise security architecture
- Privacy
- IT risk management strategy
- IT security Strategy
- Governance & implementation
- ISO 17799 / BS 7799
- Identity management solutions
- Infrastructure security solutions
- Vulnerability management solutions

- Enterprise security management
- Systems project assurance
- Data quality & integrity
- Third party reporting (SAS70, SysTrust, WebTrust)
- IT controls and security audit
- IT internal audit
- IT controls for Sarbanes Oxley
- Disaster recovery planning
- Business continuity planning
- IT risk management benchmarking

For more information about Deloitte's IT Risk Management & Security Services practice, please visit our website at [www.deloitte.com/gfsi/itsecurityservices](http://www.deloitte.com/gfsi/itsecurityservices)

### About Deloitte's Global Financial Services Industry Practice

Deloitte Touche Tohmatsu member firms serve financial services institutions globally through our Global Financial Services Industry (GFSI) practice. GFSI's industry specialists represent every major financial center in the world and bring decades of experience and leadership in banking, securities, insurance and investment management to each client assignment.

Deloitte's Global Financial Services Industry practice helps clients gain a competitive advantage in the marketplace by

- drawing from industry specialists in every major financial center in the world,
- tracking market and industry trends,
- conducting industry research, and
- providing oversight services to our clients

For more information about our practice, please visit our website at [www.deloitte.com/gfsi](http://www.deloitte.com/gfsi).

### Global Contacts

If you were not a respondent to this survey and you would like to have your organization evaluated in comparison to comparable organizations in your industry, we invite you to contact the IT Risk Management and Security Services professionals indicated below or in your country from the list on the following page.

### Global IT Risk Management & Security Services Regional Leaders

Adel Melek

Global Leader, Regional Leader, Canada

1 (416) 601 654

[amelek@deloitte.ca](mailto:amelek@deloitte.ca)

Mike White

Regional Leader, EMEA

27 (11) 806 58 99

[mikwhite@deloitte.co.za](mailto:mikwhite@deloitte.co.za)

Kevin Shaw

Regional Leader, Asia Pacific

61 (3) 9208 7637

[kevshaw@deloitte.com.au](mailto:kevshaw@deloitte.com.au)

Manuel Aceves

Regional Leader, LACRO

52 (55) 5279 7055

[maceves@dtmx.com](mailto:maceves@dtmx.com)

Ted DeZabala

Regional Leader, United States

1 (212) 436 2957

[tdezabala@deloitte.com](mailto:tdezabala@deloitte.com)

# Deloitte Contacts

Global IT Risk Management & Security Services

## Athens

Ioannis Tzanos  
30 (210) 678 1100  
itzanos@deloitte.gr

## Brussels

Chris Verdonck  
32 (2) 800 24 20  
cverdonck@deloitte.com

## Detroit

Mark Ford  
1 (313) 394 5313  
mford@deloitte.com

## Dublin

Gerry Fitzpatrick  
353 (1) 417 2645  
gerry.fitzpatrick@deloitte.ie

## Hamburg/Frankfurt

Stefan Weiss  
49 (0) 40 3 20 80 4674  
stefanweiss@deloitte.de

## Johannesburg

Mike White  
27 (11) 806 58 99  
mikwhite@deloitte.co.za

## London

Yag Kanani  
44 (20) 7303 8124  
ykanani@deloitte.co.uk

## London

Simon X.Owen  
44 (20) 7303 7219  
sxowen@deloitte.co.uk

## Madrid

Alfonso Mur  
34 (91) 514 51 03  
amur@deloitte.es

## Montréal

Marcel Labelle  
1 (514) 393 5472  
marlabelle@deloitte.ca

## Mumbai

Abhay Gupte  
91 (22) 282 4399  
agupte@deloitte.com

## Neuilly

Valerie Flament  
33 (1) 40 88 24 64  
vflament@deloitte.fr

## New York

Ted DeZabala  
1 (212) 436 2957  
tdezabala@deloitte.com

## New York

William Levant  
1 (212) 436 2172  
wlevant@deloitte.com

## Paris

Francois Renault  
33 (1) 55 61 61 22  
frenault@deloitte.fr

## San Francisco

Kenneth DeJarnette  
1 (415) 783 4316  
kdejarnette@deloitte.com

## São Paulo

Ricardo Mauricio Balkins  
55 (11) 3150 1916  
rbalkins@deloitte.com.br

## Sydney

Tommy F.Viljoen  
61 (2) 9322 7361  
tfviljoen@deloitte.com.au

## Tokyo

Keiichi Kubo  
81 (3) 6213 1112  
kkubo@deloitte.co.jp

## Toronto

Donald Mccoll  
1 (416) 601 6373  
dmccoll@deloitte.ca

## Toronto

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

## Wellington

David A. Old  
64 (4) 470 3614  
dold@deloitte.co.nz

## Zurich/Geneva

David Pike  
41 (1) 421 6401  
djpik@deloitte.com

# Acknowledgements

## Respondents to the Survey

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

### Author

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

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

### Methodology and Analysis

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

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

### Survey Development

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

Alex Chapman  
1 (416) 601 5750  
alchapman@deloitte.ca

### Editing

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

### Marketing Support

Alyssa Bourdeau  
1 (416) 601 5932  
abourdeau@deloitte.ca

## [www.deloitte.com](http://www.deloitte.com)

© 2004 Deloitte Touche Tohmatsu. All rights reserved.

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, financial advisory services, and consulting. Our member firms serve over one-half of the world's largest companies, as well as large national enterprises, public institutions, and successful, fast-growing global growth companies.

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 of the member firms 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. For regulatory and other reasons certain member firms do not provide services in all four professional areas listed above.

The scope of this survey was global, and, as such, encompassed financial institutions with worldwide presence and head office operations in one of the following geographic regions: Europe, Middle East, Africa; Asia Pacific; Latin America and the Caribbean; and North America. Attributes such as size, global presence, and market domination 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.

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 account for 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 undertake, and is not intended to constitute legal, accounting, tax, investment, consulting or other professional advice or services. 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 direct, indirect, incidental, consequential, punitive or other damages, whether in an action of contract, statute, tort (including, without limitation, negligence) or otherwise, relating to the use of these survey results or information contained herein. These survey results and 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 of the information. For more information on the Global Security Survey, please contact your local Deloitte Touche Tohmatsu professionals.