▷ **Global Financial Services Industry Practice**
Serving the financial services industry globally

2003 Global Security Survey

Deloitte Touche Tohmatsu

2003 Global Security Survey

Table of Contents

Foreword

The degree to which commerce can be undertaken and value exchanged in a trusted environment has been, over centuries, one of the standards by which a nation's wealth and stature are measured.

Throughout history, it has fallen to financial institutions to not only design and deliver solutions to meet the financial needs of individuals but to also ensure that these products are delivered, and can be utilized, in a safe environment. This responsibility becomes more daunting in the information and web technology arena, which has fundamentally changed the way financial institutions conduct business as well as the behavior and expectations of consumers. In a global and networked economy, with all of the associated regulation, the challenges for financial institutions are numerous.

The globalization of business, the proliferation of, and dependency on, technology, and the preservation of a trusted and secure environment to facilitate financial institutions, all require financial services organizations to have in place the mechanisms to ensure sound and reliable security and privacy. Without these mechanisms, financial institutions cannot offer the trusted environment that is so crucial to their success.

There seems to be little insightful data on the state of either IT security or privacy in financial institutions — or any other sector for that matter — and there is almost no data that delivers a world-wide perspective. We have, therefore, undertaken this Global Security Survey to present a global view of how leading financial institutions approach the critical areas of security and privacy and to acknowledge the importance of this information to the financial services industry.

Our intention is to replicate this survey, not only with the financial services industry but across other industry sectors as well, and to deliver it annually.

We hope you find this report insightful.

Adel Melek, Global Leader
Information Security & Privacy Services

Objective of the Survey

The purpose of the Global Security Survey is to enable you to assess the state of information security within your organization relative to other comparable financial institutions. Overall, the survey attempts to answer the question: *How does the information security of my organization compare to that of my competitors?*

As an executive of a major financial institution, you are probably facing a myriad of questions when it comes to information security, questions like:

- *Should my organization establish the position of Chief Security Officer (CSO) or Chief Information Security Officer (CISO)? If so, what areas of responsibility fall under its authority?*
- *What level of staffing should be dedicated to information security?*
- *Are other organizations going ahead with budget increases for information security or are they cutting back?*
- *Should all applications within my organization have an identified owner?*
- *What are the elements of a formal information security strategy?*
- *Should compliance to my company's information security policy be mandatory or a directive?*
- *What is my organization's risk tolerance versus that of my competitors?*
- *How does general management view IT security spending — as a necessary cost of doing business or as an investment in enabling infrastructure?*

How We Designed, Implemented and Evaluated the Survey

Deloitte Touche Tohmatsu's Global Security Survey for financial institutions provides insights into these and other vital questions — and the answers come from the world's leading financial institutions. Understanding the strengths and weaknesses of your organization relative to those of your competitors helps your executive group make key strategic decisions and position your company appropriately.

This Global Security Survey reports on the outcome of focused discussions between Deloitte Touche Tohmatsu's Information Security & Privacy Services professionals and Information Technology (IT) executives of top global financial institutions.

Discussions with representatives of these institutions 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 levels of perceived risks, the types of risks with which financial institutions are concerned and the resources being used to mitigate these risks. The survey also identifies what technologies are being implemented to improve security and the value financial institutions are gaining from their security investments.

To fulfill this objective, senior members of Deloitte Touche Tohmatsu's Information Security & Privacy Services professionals,

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*.

Anonymous 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 one of the following geographic regions: Europe, Middle East, Africa (EMEA); Asia Pacific (APAC); Latin America and the Caribbean (LACRO); and North America. Respondents fell into three primary industry sectors. While industry sector focus was not deemed a crucial criterion in the participant selection process, 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 may not be representative of each identified geographic region.

Drafting of the Questionnaire

The questionnaire was comprised of questions composed by a team made up of senior professionals from Deloitte Touche Tohmatsu's Information Security & Privacy Services. The questionnaire went through five iterations where each question was tested against global suitability, timeliness, and degree of value. The purpose was to identify and record the state of information security and privacy in the financial services industry.

The Data Collection Process

Once the questionnaire was finalized and agreed upon by the survey team, the questionnaires were distributed electronically to the participating regions. Each 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.

Results Analysis and Validation

The DeloitteDEX team was 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. Clients' performance can be measured versus 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.

The DeloitteDEX team arranged the data by geographic origin of respondents. As the respondents numbered less than 100, it was not necessary to reduce the list by counting how many times particular answers to specific questions occurred in order to build frequency distributions. 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 straightforward.

Benchmarking

This survey is intended to enable benchmarking against comparable organizations. Benchmarking studies provide a quality and, often, quantifiable health check by comparing performance metrics to peer group organizations and best practice firms. Benchmarking can often facilitate in recommendations for performance improvements.

Areas Covered by the Survey

It is possible that your company may excel in some areas related to information security, e.g., investment and responsiveness, and yet fall short in other areas such as 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 aspects of a typical financial services organization's operations and culture:

Governance
- 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

Quality of operations
- Benchmarking
- Administration
- Detection
- Response
- Privileged users
- Authentication
- Controls

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

Who Responded

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 by not identifying their organizations. However, we can state that overall, the participants represent **35%** of the top 500 global financial services organizations.

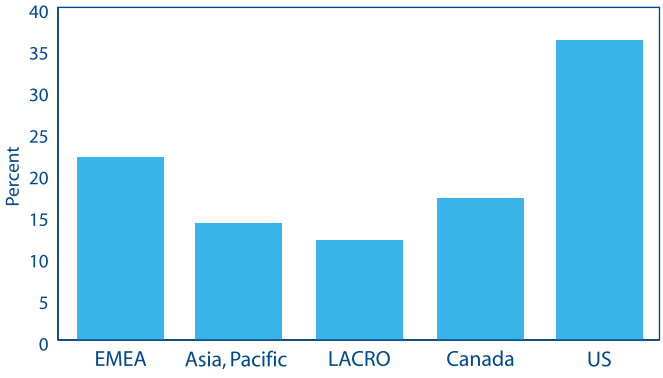
We are able to provide the following specifics about our respondents:

Geographic region

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

- EMEA - 22%
- APAC - 14%
- LACRO - 12%
- Canada - 16%
- United States - 36%

Figure 1 – Geographic Distribution of Respondents



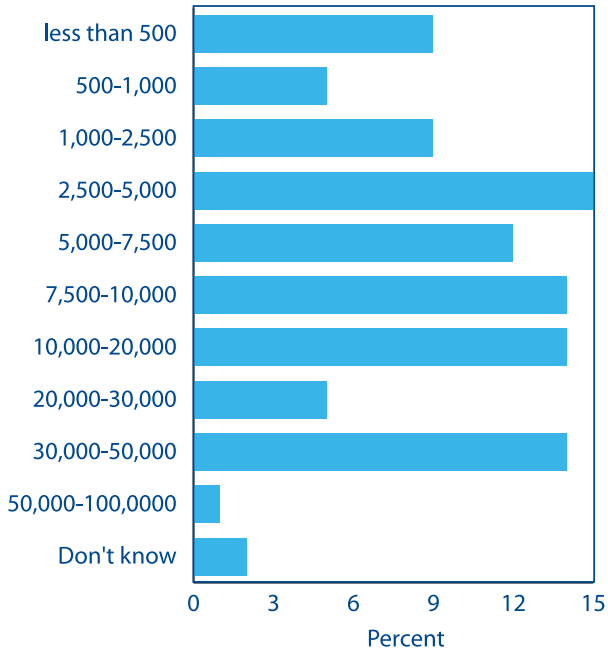
Ownership and size

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, **60%** were public, **27%** were private and the other **13%** were comprised of not-for profit, public sector or private subsidiaries of publicly held organizations.

By number of employees*, the participating financial institutions present a broad spectrum:

- 2.5K to 5K employees - 15%
- 10K to 20K employees - 14%
- 20K to 30K employees - 5%
- 30K to 50K employees - 14%
- 50K to 100K employees - 1%

Figure 2 – Number of Employees

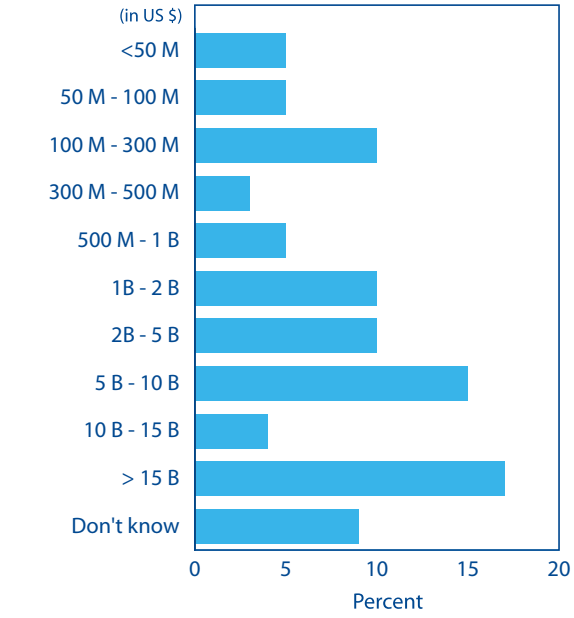


*Results may not total 100% as we are reporting selected information only.

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

- Up to US $1B in annual revenue - 28%
- US $1B - US $5B in annual revenue - 20%
- US $5B - US $10B in annual revenue - 15%
- US $10B - US $15B in annual revenue - 4%
- US $15B + in annual revenue - 4%

Figure 3 – Annual Revenues



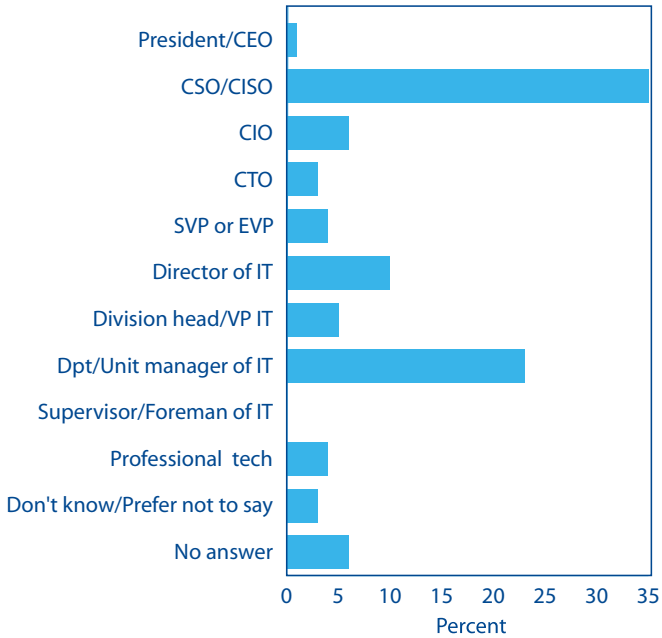
*Results may not total 100% as we are reporting selected information only.

Levels of respondents

The individuals who responded on behalf of participating financial institutions are in positions to provide accurate and authoritative answers*. They include:

- Chief Security Officer (CSO) or Chief Information Security Officer (CISO) - 35%
- Unit Managers within IT - 23%
- Chief Information Officers (CIO), Chief Technology Officers (CTO) or Chief Executive Officers (CEO) - 10%
- IT Directors - 10%

Figure 4 – Levels of Respondents



*Results may not total 100% as we are reporting selected information only.

Regional Observations

Overall, we have observed that there are more similarities than disparities among the responses across geographic regions. To some degree, this is due to the fact that many of the organizations that responded to the survey are global organizations. In addition, the information security community is well connected via common professional associations, industry forums and common threats to which they are all exposed.

EMEA

EMEA respondents appear to be the most motivated by fear of exposure and compliance to rules and laws among the other regions. They classify themselves as "effective users of demonstrated technologies". They are ahead of the pack when it comes to policy setting, security standards (e.g. BS7799), privacy, utilization of public key infrastructure (PKI), biometrics, and expenditure in security. Of all respondents, they had the greatest concerns regarding differing laws and regulations, not surprising given the diversity of languages and number of countries in the region. They also had the highest ranking among respondents in terms of lack of qualified security resources. The security function in EMEA takes the highest responsibility of compliance among all respondents, while reporting the least level of activities among respondents regarding ethical hacking and network penetration testing techniques, business continuity planning and disaster recovery planning and testing (BCP/DRP).

APAC

Asian respondents demonstrated conservatism and conformity. They are not risk takers, relatively late adopters of security technologies (with the exception of wireless and smart cards), characterized the level of risks that their organizations strive for as "effective and efficient" and report the highest concern about the increased sophistication of threats. They are also the most concerned about security budgets.

Respondents from Asia Pacific report that they are almost exclusively driven by laws and regulations related to privacy compliance. They have the lowest level of concern regarding interoperability of different products, and reported the least interest in "single sign on" and provisioning solutions, though they had the highest response in terms of implementing directory services technologies.

LACRO

LACRO respondents demonstrated a sober representation of the state of information security in most of the developing countries. They characterized themselves as fast followers. They had the highest response in terms of lack of a CISO/CSO within the organization, demonstrating that this region is still relatively less advanced in terms of information security. They recognize a lack of awareness and recognition as the biggest challenge they face followed by the increased sophistication of threats. Along with respondents from EMEA, they had the least deployment of ethical hacking and testing techniques, incident response, and security of third-party access. Surprisingly, they had the highest rating in terms of use of biometrics and adoption of security standards frameworks (e.g., BS7799). However, they had the least level of interest among all regions in wireless security, "single sign on," access management and provisioning technologies.

North America

Canada

Canadian respondents were the most likely of all respondents to be driven by competitors' activities. They characterized the level of risk that their organizations strive for as "effective and efficient." They also describe themselves as effective users of demonstrated technologies, yet they reported the lowest rate of security standards adoption among other regions. The Canadian respondents reported as high as the United States in terms of use of tools, adoption of new technologies, performance of ethical hacking and penetration testing, though they had the least utilization of Threat Risk Analysis measures. Canadian respondents reported the highest connectivity among financial institutions, predominantly due to Interac. Interac is a Canadian organization controlled by the five largest banks, the Confédération des caisses populaires et d'économie, and the Credit Union Central of Canada, through which its members access the shared ABM and EFTPOS networks.

Surprisingly, Canadian respondents represent the only region with materially less than 100% deployment of anti-virus tools. In addition, they had the least deployment of biometrics and the highest rating for concerns over the fragmentation of security products. Canadian respondents reported the least concerns about availability of qualified security resources, budgets and increased sophistication of threats. Along with those from the LACRO region, Canadian organizations expressed no concerns over differing international laws and regulations.

United States

Not surprisingly, US respondents' answers demonstrated the highest level of maturity in almost all categories, with a few exceptions, such as adoption of security standards, privacy and the utilization of certain technologies. CISO/CSOs in the US have the broadest security scope of coverage, with the exception of the compliance function, for which EMEA reported the highest coverage. They are early adopters of technology, and characterize the level of risk that their organizations strive to achieve as "effective and efficient." Respondents from the United States show the highest level of BCP/DRP development, maintenance and testing over the past 12 months, which comes as no surprise given the events of September 11, 2001. Surprisingly, the United States reported the least deployment of physical security tools, and PKI/biometrics.

"New technologies and new business models are causing us to blindly run full speed toward the unknown. And the hot breath of threats and risk is on our necks at all times. We are constantly under siege."

Global Security Survey Respondent

Key Findings of the Survey

The following points summarize the highlights of our research:

1. **Respondents are worried about the increased sophistication of threats against their computer systems.** The subject of cyber attacks has traditionally been rife with myths, such as, attacks are an uncommon and infrequent occurrence, they are almost exclusively the work of juvenile hackers, and they are perpetrated predominantly by insiders rather than by people from outside the company. While these myths may have been true in a less sophisticated world of computer technology, they are no longer true today. Respondents are increasingly worried about the sophistication of the attacks — and their fears are valid. Even relatively low-grade threats (e.g., viruses and worms) can result in significant financial losses. The evolution of viruses and worms continues unabated. In May, 2000, the "Love Letter" virus did an estimated $2.6 billion in damages. High-grade threats such as theft of proprietary information and financial fraud can have a staggering impact on a targeted organization. A CSI/FBI Computer Crime and Security Survey conducted annually for eight years shows the increasing frequency of attacks from the Internet and the decreasing frequency of attacks on internal systems. In addition, attacks are increasingly aimed at either financial institutions or financial information stored in less secure third-party sites. A significant **39%** of respondents to this Global Security Survey acknowledged that their systems had been compromised in some way within the last year.

2. **Respondents are recognizing the need for employee awareness and education.** Awareness and education programs which address Internet and e-mail usage can go a long way to mitigating the impact of some of the problems related to corporate governance. Safeguarding information assets is now a vital part of corporate governance. A powerful and effective awareness and education program that guides boardroom and workforce activities is seen as positively contributing to problem mitigation, problems such as the release or misuse of personal information or the compromise of confidential documents.

3. **Reporting relationships play a key role in the perception of the importance of the information security function.** Where the information security function reports within an organization is a matter of great importance. Until recently, the information security function typically reported within the IT department to someone relatively low in the chain of command. In the mid-nineties, forward-thinking organizations began establishing information security units that were independent of IT and reported at the same level directly to the CIO. As the nature of cyber risks evolved in scope, complexity and intensity, it became clear that having Information Security report directly to the CIO did not go far enough. Information Security needed more authority, respect and access. The notion of establishing a Chief Security Officer or Chief Information Security Officer emerged and gathered momentum. With a CSO, it was argued, the different dimensions of security could be brought into alignment and work together to strengthen the security posture of the organization. Furthermore, the CSO would have a seat at the table with the CIO, the COO, the CFO, and Information Security would be perceived as a risk management expenditure rather than an obscure line item in the IT budget. Over **61%** of the financial institutions that participated in our survey have a CSO or CISO, and another **14%** of respondents report having more than one.

4. **IT security budgets appear to be a single digit percentage of the overall IT budget.** Overall security budgets are increasing, as outlined in an earlier observation. We observed that there are some disparities among the respondents in terms of how much of the overall IT budget the security budget represents. However, the figure appears to be mostly in the upper single digit percentage. In developed countries, that percentage appears to be around **6-8%**, while in other regions it is lower.

5. **There is an absence of Key Performance Indicators (KPI) for Information Security functions.** By and large, the absence of KPIs became clear for most respondents across all regions. While the CISO/CSOs had their own notions of KPIs, they all agreed that business management did not have clear expectations. CISO/CSOs also explained that their first priority has been alleviating the security exposures that their respective organizations have experienced. They believe that much needed KPIs will emerge as the maturity and scale of their security functions goes to the next level.

6. **Conventional wisdom for staffing is obsolete and a new model needs to take its place.** Information security staffing is another issue that affects the perception of the importance a company places on information security. The rule of thumb has been one information security professional for every 1,000 users. But this out-dated wisdom is left over from the mainframe environment. Today, most financial institutions are engaged in e-commerce with customers, suppliers and partners. Most have far flung offices and most have workforces that interact over the Internet. The information assets of these institutions are high-value items (e.g., research and development, financial transactions, etc.). And yet, despite this, in many instances and in all industry sectors, IT security staff has suffered cuts due to the severe economic downturn.

7. **Fragmented security products contribute to the lack of unified security programs.** The disparate levels of product maturity offered by the current security vendors have been observed by all respondents. Continuous mergers, acquisitions and the disappearance of product vendors have left a bad impression with many security executives who made decisions to acquire a particular vendor's solutions. In addition, information security professionals acknowledge that there are many new solutions for the varied security problems that face organizations. Most, however, are solutions that do not integrate well to form a robust solution set. Finally, many of the security products lack the inherent scalability, reliability and audit-trail that are expected of such products.

8. **There is a lack of clarity on the impact of multiple governance initiatives on information security.** A number of new governance initiatives are emerging worldwide, including Sarbanes-Oxley, EU Directive, Basel Accord, USA PATRIOT Act, and The Personal Information Protection and Electronic Documents Act (PIPEDA). While many of these governance initiatives are placing more emphasis on introducing new controls and holding management accountable for asserting the integrity and representation of their financial information, it is unclear what role will be expected of the information security function in assisting management to provide such assertions.

Governance

As far as a formal information security strategy, 80% of respondents have one.

However, when asked if line and functional leaders led and embraced that strategy, **only 47% answered "yes."**

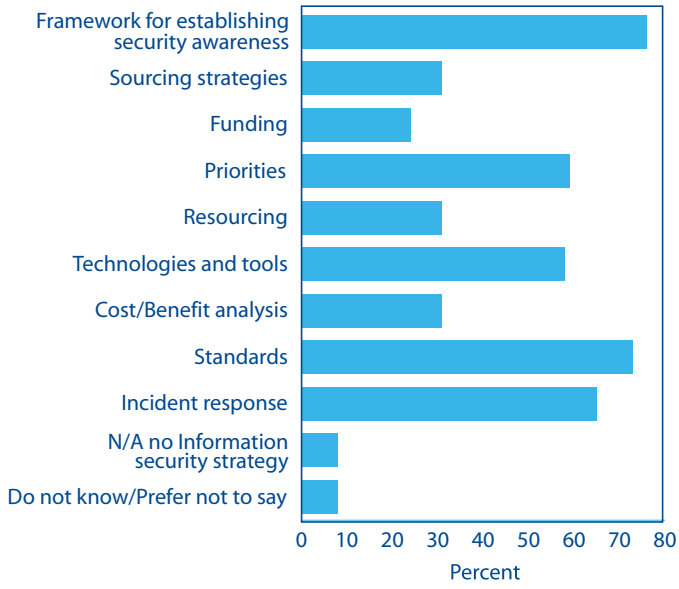
"We feel that the biggest threat to us is security awareness, or lack of it. One person who opens a virus-laden attachment can cause a lot of damage. People are the weakest link. Technology can only help reduce risks to a point."

Global Security Survey Respondent

Formal information security strategies, according to respondents, encompass numerous aspects of information security, including:

- Framework for establishing security awareness - 76%
- Standards - 73%
- Incident response - 65%
- Priorities - 59%
- Technologies and tools - 58%

Figure 5 – Formal Information Security Strategies



Respondents also outlined the scope of the information security function itself:

- Policy setting - 97%
- IT security - 94%
- Infrastructure security - 87%
- Security assessment/reviews - 85%
- Security administration - 81%
- Security operations - 79%
- Physical security/corporate security - 36%

Respondents acknowledged the following aspects of clear accountability:

- All applications have an identified owner - 73%
- Obtain feedback on information security program - 54%
- Performance goals and metrics to measure program - 45%
- Clearly defined and measurable senior management objectives - 46%

Figure 6 – Security Function

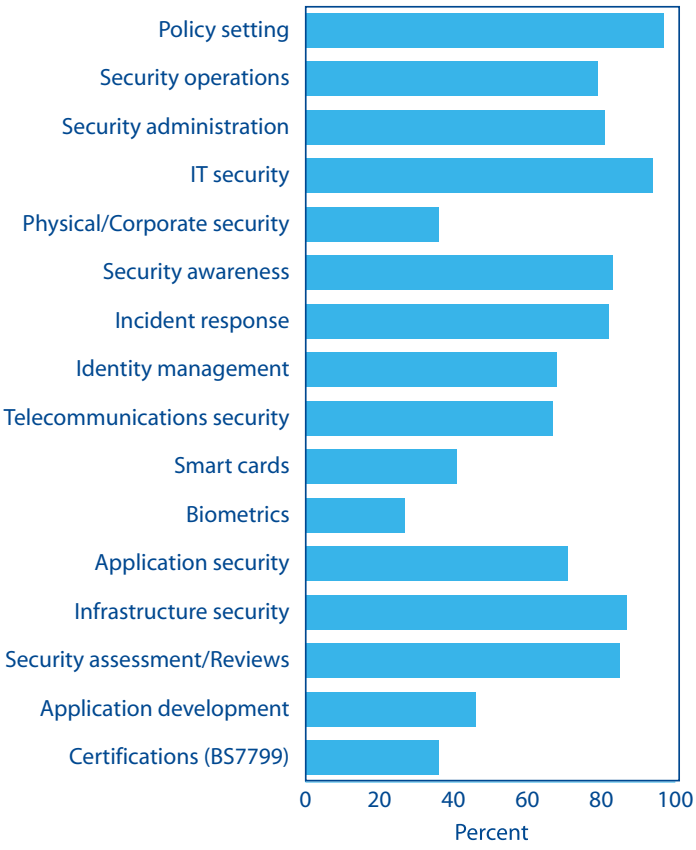
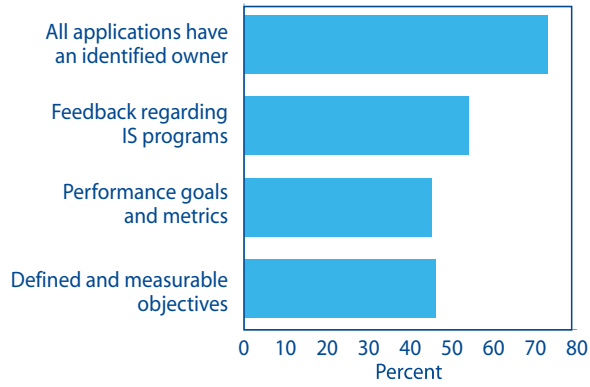


Figure 7 – Clear Accountability



Investment in Security

Respondents, on average, **cited the figure of 6% of the total IT budget** as being designated for information security.

Despite the severe economic downturn experienced in the last two years, **most respondents have increased their budgets, or at least held the line:**

- 47% of respondents report that their IT security staffing levels have increased within the last year
- 29% of respondents reported that staffing levels remained unchanged
- 19% of respondents reported decreases in staffing levels

"Security is not a technical or a project issue. It is more and more an enabler for business opportunities. Information represents the main assets of a company. To protect it in a more and more open network represents a day-to-day challenge."

Global Security Survey Respondent

Respondents indicated that **they have come to grips with some of the organizational issues involved in information security:**

- 63% currently have or plan to establish CSO or CISO positions in the next two years
- 53% of respondents stated that their CSO/CIO have an average tenure of up to ten years.

To whom does the CSO report?

- 32% report to the CIO
- 9% of them report directly to the board of directors
- others report across a range of corporate officers — 6% to the CTO, 6% to the CRO, 5% to the COO and 4% to the CEO

Asked to characterize **information security spending relative to their perception of how other organizations spend on security**, respondents answered:

- Moderate - 44%
- Conservative - 24%
- Aggressive - 12%
- Inadequate - 10%

They characterize the **organization's investment in security** as:

- Ahead - 4%
- On plan - 47%
- Catching up - 37%
- Falling behind - 8%

Most respondents report that **general management perceives spending on IT security in realistic terms:**

- Necessary cost of doing business - 63%
- Discretionary expense - 22%
- Investment in enabling infrastructure - 13%
- Would be cut in hard times - 1%

Most respondents report that **general management appreciates the "value" of IT security,** one way or another:

- Risk Management - 49%
- Business Enabler - 33%
- Essential to Business Strategy - 28%
- Necessary Evil - 24%
- Not visible - 12%

Figure 8 – Perception of IT Security Spending

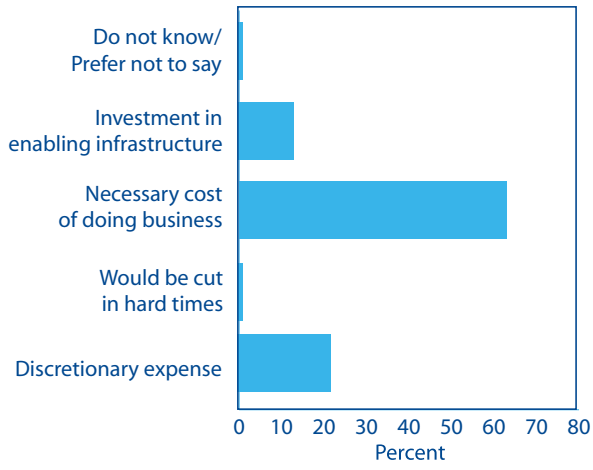


Figure 9 – "Value" of IT Security

Value

Although *Value* was listed as a separate category in our survey, we have included the results in this section on Investment in Security. We feel that the perceived value of IT security is directly related to the investment in security that a company is willing to make.

Risk

How well prepared are the respondents? How well do they feel their organizations understand the risks that confront them?

In total, 39% of respondents acknowledged that their systems had been compromised in some way within the last year. The responses contradict the outdated beliefs that 80% of the cyber crime problem is caused by insiders, while only 20% of the problem is committed by outsiders:

- 16% report attacks from an external source
- 10% report attacks from an internal source
- 13% report attacks from both sources

Respondents are "confident" but circumspect about how well their organization's networks are protected from cyber attacks (e.g., DOS attack, malicious code, sabotage, etc.) whether launched from inside or outside. Their feelings are summed up as follows:

- Not very confident - 18% (internal), 3% (external)
- Somewhat confident - 44% (internal), 35% (external)
- Very confident - 27% (internal), 40% (external)
- Extremely confident - 5% (internal), 13% (external)

In regard to how their organization's risk tolerance measures up versus that of their competitors, the respondents are a little more comfortable:

- Less risk than industry as a whole, even at higher cost - 27%
- More risk and have a lower cost than industry - 15%
- Same risk as the rest of industry - 35%
- Ignore our competition - 8%

When asked to characterize the level of risk that their organizations strive for, **62% of respondents depict their risk management approach as "efficient and effective" rather than "necessary risk only" (19%) or "world class and bullet proof" (6%).**

- 65% of respondents said their organizations had taken the important step of classifying critical business assets in terms of value and risk
- 51% said that these assets were being "appropriately protected"

Figure 10 – Organization's Protection from Cyber Attacks

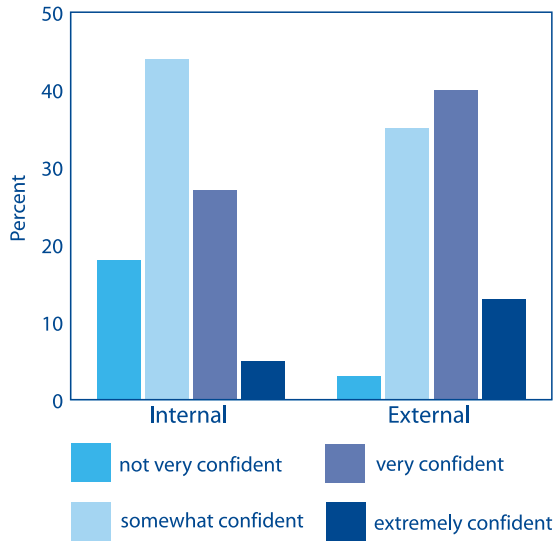


Figure 11 – Risk Tolerance Measures

Use of Security Technologies

In line with the cautious attitude exhibited in some of the risk-related questions, respondents characterize their organization as "effective users of demonstrated technology" rather than "early adopters" or even "fast followers."

With regard to **strong authentication for remote access:**

- 86% report using strong authentication
- 55% report using strong authentication for privileged users

Some respondents have even undertaken **proactive measures to help manage exposure to wireless communications (WiFi) risks:**

- 49% have instituted security policies related to organizational wireless usage and acceptance
- 41% have scanned the network to identify rogue wireless networks
- 29% have issued employees guidelines for the safer use of WiFi

Security technologies deployed is predictable but reassuring:

- Anti-virus - 96%
- Virtual private networks - 86%
- Intrusion detection systems - 85%
- Content filtering/monitoring - 77%
- Public key infrastructure - 45%
- Smart cards - 43%
- Biometrics - 19%

"There is no such thing as 100% security. Security is not only a technology issue but a management issue as well and it demands ongoing effort."

Global Security Survey Respondent

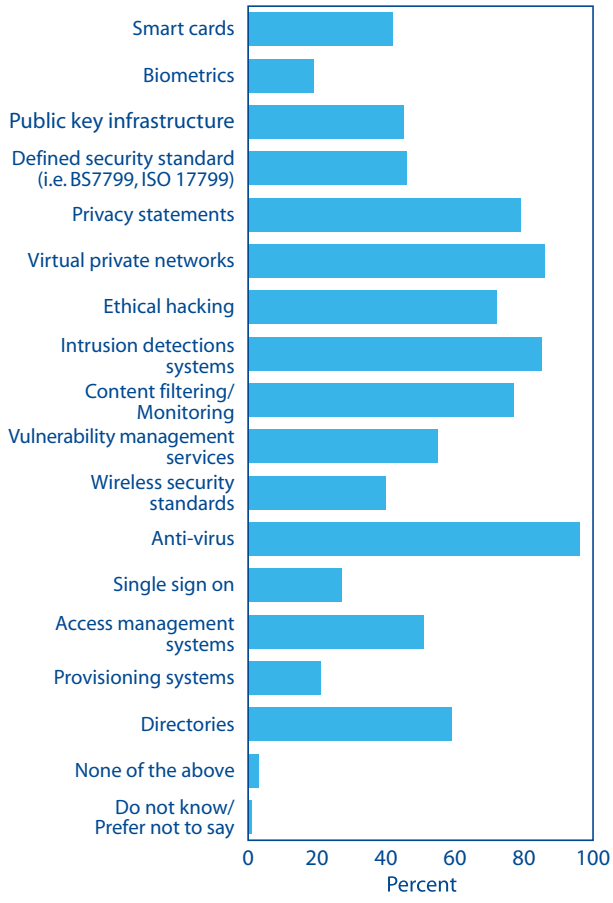
Even more reassuring is that **the list of technologies "to be deployed within the next 18 months," is topped by those that offer stronger authentication:**

- Public key infrastructure - 45%
- Smart cards - 42%
- Biometrics - 19%

Within 18 months:

- 78% of the financial institutions in this survey will have rolled out Public Key Infrastructure
- 70% will have incorporated smart cards
- 29% will have deployed biometrics in some form

Figure 12 – Use of Security



Quality of Operations

How have the respondents' IT security programs been working in the operational environment? What are they getting done? What kind of tangible impacts have these programs had?

In terms of a training or awareness session on security and privacy issues and statutory compliance in the last 12 months:

- 73% of respondents say that employees have accepted their responsibility in protecting corporate information, systems and facilities
- only 45% have taken part in at least one program

"The behavioral aspects are as worrying as the technical aspects. Everyone has to understand that it is their personal responsibility to manage risk and assets. We worry about the capability that has not been applied. Although we are doing our best, it is probably not enough."

Global Security
Survey Respondent

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

- 88% say that their organizations have one
- 73% have reviewed their DR/BC plans after the terrorist attacks of September 11, 2001
- Only 43% characterize themselves as "very confident" that their backups either work or are being stored off-site in accordance with policy

Organizations are increasingly relying on third-party providers, outsourcers, etc. to perform important functions (and even, in some cases, security functions). But the question remains as to how much due diligence has gone into assessing whether these third-party providers are secure.

- Only 44% of respondents say they receive information on a regular basis that allows them to assess the effectiveness of third-party providers
- Only 38% have conducted their own rigorous assessment of the third-party's skills, capabilities, culture, etc.

It is a positive sign that 24% of respondents have cyber risk insurance, and that another 5% intend to acquire such coverage.

Responsiveness

Although *Responsiveness* was listed as a separate category in our survey, we have included it in this section because we feel that the responsiveness of the IT security function is directly relevant to the quality of the company's operations.

Privacy

What drives organizations to address privacy issues? We would like to say it is a concern for the privacy of customers. But, according to respondents, self-interest is the primary motivation:

- Legal and industry regulation - 90%
- Fear and exposure to business risk (e.g., legal/financial penalties, damaged reputation) - 54%
- Customer demand or expectations - 47%

When asked how their organizations view privacy initiatives, 50% of the respondents indicated the same self-interest was at work and that their efforts focused almost exclusively on risk avoidance. **31%** said that issue was something the lawyers and specialists dealt with.

Only **13%** (less than the number that answered "do not know") see privacy initiatives as a **"strategic platform for value creation and competitive positioning."**

Only **40%** of respondents have a **Chief Privacy Officer (CPO)**, and only **6%** intend to appoint one within the next two years. There has been far more hype about CPOs than CSOs.

Nevertheless, despite this weak expression of enthusiasm for privacy among financial institutions, **some effort is apparent:**

- Written privacy, fair information practices or data collection policies in place - 76%
- Always gain consent from individuals to the collection of their personal data - 68%
- Formal process in place to deal with complaints about its personal information management practices or policies - 67%
- Identification of the types of personal information that is collected and classified according to their sensitivity - 60%
- Formal policies in place in respect to the destruction of personal information - 59%
- Strategy for managing privacy compliance - 56%

Figure 13 – What Drives Privacy Initiatives

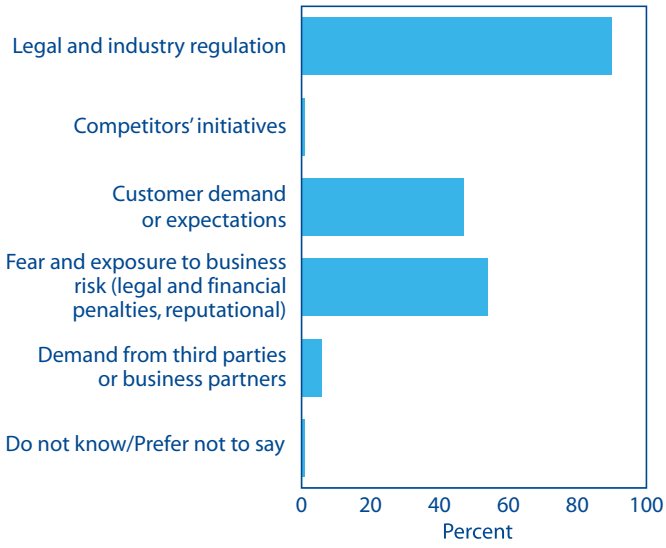


Figure 14 – Privacy Initiatives in Place

Summing Up and Challenges

Financial institutions face unprecedented threats in the current global environment. Numerous factors, including weak economic conditions, lack of stakeholder confidence in corporate governance, increased regulatory oversight, heightened danger of terrorist attacks and conflict contribute to the hostile landscape.

The threats faced by financial institutions stem from a variety of factors:

- Their increasing use of electronic commerce means that financial institutions face more threats of financial fraud and theft of customer information both from inside and outside their organizations, much of it perpetrated by organized criminal enterprises.
- Participation in an increasingly global economy means that financial institutions face a growing danger of theft of proprietary information on behalf of unscrupulous competitors.
- Recognized as a critical infrastructure, the financial services industry faces a heightened risk of being targeted for cyber terror attacks.
- The increasing interconnectivity of their networks means that financial institutions are vulnerable to swarms of costly new viruses and worms.

Are financial institutions ready to meet the challenges of these unprecedented threats? Do financial institutions understand the increasingly hostile dimensions of cyberspace?

As this survey of some of the world's leading financial institutions reveals, the answers are not simple.

More work to be done

- Although the financial sector has been designated as a "critical infrastructure," only 46% of respondents had altered their security programs accordingly, evidence that financial institutions are not taking the threat of cyber war seriously enough.
- There is discouraging evidence of ill preparedness; only 43% characterize themselves as "very confident" that their backups either work or are being stored off-site in accordance with policy.
- The global economic slowdown means that organizations are not hiring and IT security staff are not switching jobs. Yet the situation dictates that information security staffing levels should be increased to reflect the widening variety and increasing sophistication of the threats against financial institutions.
- Tightened spending means that potential IT security projects are scrutinized more carefully and, in some cases, passed over in favor of spending on other IT projects. As information security and related functions mature and scale to the new environment, key performance indicators must be developed to help business management grasp what budget dollars dedicated to information security really buy.
- The effort that most respondents make in the area of privacy is in the interests of protecting themselves. They do not view it as a marketing advantage and they do not accord it much importance in terms of appointing an executive who is responsible for it.
- The role of information security relative to the new controls and management accountability, dictated by Sarbanes-Oxley, the EU Directive, Basel Accord, USA PATRIOT Act, The Personal Information Protection

and Electronic Documents Act (PIPEDA) and other legislation in the United States and Europe, has yet to be understood and articulated.

Encouraging signs

Even though there is much work to be done, there is every indication that things are moving in the right direction and that the tide of concern on the topic of information security will gain momentum.

- Survey responses regarding technology deployed, or to be deployed within the next 18 months, indicate that financial institutions have decided to get serious about authentication.
- The trend of establishing a Chief Security Office or Chief Information Security Officer is gaining momentum. With a CSO or CISO, it is argued, the different dimensions of security can be brought into alignment and work together to strengthen the security posture of the organization.
- In the United States, The President's Critical Infrastructure Protection Board's recent draft entitled *National Strategy to Secure Cyberspace*, means that security audits, training programs and the managing and monitoring of security are likely to receive increased attention by senior management and by boards of directors.
- There is an increasing awareness on the part of consumers, users, corporations and politicians that privacy and security are becoming increasingly important matters of discussion as part of the national dialogue.
- A solid strategy and effective implementation that addresses the broader issues and relationships will be required by any enterprise that wants to maximize its potential in the marketplace in the coming decade.

This Global Security Survey underscores the challenging nature of the current situation: financial institutions are feeling the downward pressure of market forces that inhibit the growth of IT security and the upward pressure to take action in the face of imminent danger from threats more diverse than they have ever faced in the past. The next few years will be challenging indeed.

"There is a complex relationship between Security and Privacy. Security is required to protect personal and sensitive information but is itself a threat in some respects to privacy. The more we employ security (tightly bound authentication, authorization, traffic analysis, data analysis and mining) the more potential threats exist to privacy information. It is this existence of the security/privacy paradox that makes the relationship so complex."

William Levant, Partner
Security & Privacy Practice
Deloitte & Touche

About Our Global Information Security & Privacy Services

As one of the largest independent groups providing security services in the world, we are able to leverage the business, industry, and geographic expertise of over 100,000 business professionals across hundreds of offices worldwide. This puts Deloitte Touche Tohmatsu's Information Security & Privacy Services in the unique position to help clients with cost-effective security solutions that are delivered locally-where they're needed. Our people have served in corporate and government security positions around the world, and can deliver solutions that appreciate client situations. In our experience, information security can be most effectively addressed through three core security solutions: Identity Management, Application Integrity, and Infrastructure Security.

About Our Global Financial Services Industry Practice

Deloitte Touche Tohmatsu member firms serve financial services firms globally through our global financial services industry 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. For more information about our practice visit our web site at 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 Information Security & Privacy Services professionals indicated below or in your country from the list on the following page.

Global Information Security & Privacy Services Regional Leaders

Adel Melek, Global Leader
Regional Leader, Canada
1 (416) 601-6524
amelek@deloitte.ca

Tom Patterson
Regional Leader, EMEA
49 (0) 69 75695-523
topatterson@deloitte.de

Kevin Shaw
Regional Leader, Asia Pacific
61 (3) 9208 7637
kevshaw@deloitte.com.au

Manuel Aceves
Regional Leader, LACRO
52 (55) 5279 7055
maceves@dttmx.com

Ted DeZabala
Regional Leader, United States
1 (212) 436 2957
tdezabala@deloitte.com

Global Information Security & Privacy Services Contacts

Amstelveen
Patrick van Gool
31 (20) 454 7000
pvangool@deloitte.com

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

Brussels
Erik Luysterborg
32 (2) 639 4832
eluysterborg@deloitte.be

Buenos Aires
Alan Kerwin
54 (11) 4320 2774
akerwin@deloitte.com.ar

Cayman Islands
Jeremy Smith
1 (345) 814 3315
jersmith@deloitte.com

Chicago
Tom Church
1 (312) 946 2390
tchurch@deloitte.com

Düsseldorf
Burkhard Petin
49 (211) 8772 711
bpetin@deloitte.de

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

Hong Kong
Peter Koo
86 (10) 6528 1599
petkoo@deloitte.com.hk

Johannesburg
Kobus Burger
27 (11) 806 5227
kburger@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

Los Angeles
Scott Kandel
1 (213) 688 4159
skandel@deloitte.com

Madrid
Juan Miguel Ramos
34 (91) 514 5000
juramos@deloitte.es

Manchester
David S. Hughes
44 (161) 455 8537
dshughes@deloitte.co.uk

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

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

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

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) 6400 5590
keiichi.kubo@tohmatsu.co.jp

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

Toronto
Yezdi Pavri
1 (416) 601 6191
ypavri@deloitte.ca

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

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 our firm 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
Richard Power
1 (415) 783 4745
rgpower@deloitte.com

Richard Power is an authority on the subjects of information security, computer crime, and industrial espionage. He has advised Fortune 1000 corporations and government agencies throughout the world. He is the author of the book, *Tangled Web: Tales of Digital Crime from the Shadows of Cyberspace* and the *CSI/FBI Computer Crime and Security Survey*. Richard is currently Global Manager of Security Intelligence for Deloitte Touche Tohmatsu's Global Information Security Organization (GISO).

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

Survey Development
Marc Mackinnon
1 (416) 601 6150
mmackinnon@deloitte.ca

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 damages 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.

www.deloitte.com/gfsi

Deloitte Touche Tohmatsu is one of the world's leading professional services organizations. The member firms of Deloitte Touche Tohmatsu deliver world-class assurance and advisory, tax, and consulting services. With more than 119,000 people in over 140 countries, the 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. Our internationally experienced professionals strive to deliver seamless, consistent services wherever our clients operate. Our mission is to help our clients and our people excel.

Deloitte Touche Tohmatsu is a Swiss Verein, and each of its national practices is a separate and independent legal entity.