Deloitte.

Global Financial Services Industry

2007 Global Security Survey

The shifting security paradigm

Audit. Tax. Consulting. Financial Advisory.

Contents

Foreword

We've reached a milestone! For the past five years, Deloitte Touche Tohmatsu's (DTT's) Global Financial Security Industry (GFSI) Group —a group made up of Deloitte member firm Financial Services Industry practices—has conducted its annual Security Survey. If one believes the oft-repeated tenet that a year in technology is like ten in any other industry, then we've been chronicling the equivalent of fifty years of challenge, change and progress of security and privacy in financial institutions.

How much some things change. In the 2003 security survey, the DTT GFSI Group wrote, "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." It is an indication of the truly high visibility that security and privacy has attained that this statement is no longer the case.

How much some things stay the same. One of the survey respondents to the 2003 security survey offered this statement, "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." This statement is as true today as it was back then. The ever-increasing sophistication of security breaches seems to know no bounds. The industry has produced some great minds—which have been used for us as well as against us.

It has often been said that, over the course of a lifetime, children are the source of one's greatest joy and one's greatest concern. In a similar vein, this year's respondents might say the same of their people (employees, customers, third parties and business partners) —they are an organization's greatest asset yet its greatest worry. The most frequent breaches organizations experienced were those perpetrated by crooks against the customer. In addition, a large number of organizations anticipate breaches due to employees, both intentional action (misconduct) and unintentional action (errors and omissions). Even though the majority of breaches are due to mistakes and not malicious intent, they have no less impact.

But mistakes are not without their usefulness. Sam Levenson, the American humourist, once said, "You must learn from the mistakes of others. You can't possibly live long enough to make them all yourself." * Humour aside, from a security and privacy perspective, the message is clear: often times, it takes misfortune happening to others for us to learn what to do to protect ourselves. You can be sure that every time there is a major security disaster reported in the press, many other organizations scramble to ensure that their systems are not vulnerable in the same way.

Every year, this survey demonstrates the progress in security that has been made over the course of a year: the incidents of viruses/worms, insider fraud, and the leakage of customer data have all fallen. We know this doesn't mean that the criminals are going away—they're just thinking up something new—but the statistic represents major progress nonetheless. And much of the progress has been as the result of proactive—rather than reactive—measures.

Again, as in previous years, my sincere thanks to the Chief Information Security Officers, their designates, and the security management teams from financial services institutions around the world. I hope you will find that the calibre of this document more than justifies the time and effort you spent assisting us and I hope that readers of this survey will be enlightened by its insights.

Those of us in the security and privacy arena know that the answer to the question, "Are we there yet?" is that we may never be there—but we continue to work towards making sure that the journey is as safe and secure as possible.

Adel Melek, DTT, Global Leader
IT Risk Management and Security Services
Global Financial Services Industry (GFSI) Group

Objective of the survey

The goal of the 2007 Global Security Survey for financial institutions is to help respondents assess the state of information security within their organization relative to comparable financial institutions around the world. Overall, the survey attempts to answer the question: **How does the information security of my organization compare to that of my counterparts?** By comparing the 2007 data with that collected from the previous year's surveys, Deloitte member firms' FSI practices can determine differences and similarities, identify trends and ponder in-depth questions, such as: **How is the state of information security changing within my organization?** and **Are these changes aligned with those of the rest of the industry?**

Where possible, questions that were asked as part of the 2004, 2005 and 2006 Global Security Surveys have remained constant, thereby allowing for the collection and analysis of trend data. In order that questions remain relevant and timely with regard to environmental conditions, certain areas were re-examined and expanded to incorporate the "hot" issues being addressed by financial institutions at a global level. Deloitte member firm subject matter specialists were enlisted and their knowledge leveraged to identify questions with the most impact.

The value of benchmarking

Financial Services Institutions (FSIs), now more than ever, recognize the importance of performance measurements and benchmarks in helping them manage complex systems and processes. The Global Security Survey for financial institutions is intended to enable benchmarking against comparable organizations. Benchmarking with a peer group can assist organizations in identifying those practices that, when adapted and implemented, have the potential to produce superior performance or to result in recommendations for performance improvements.

Areas covered by the Survey

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

- **Governance**
  Compliance, Policy, Accountability, Management Support, Measurement.
- **Investment**
  Budgeting, Staffing, Management.
- **Risk**
  Industry Averages, Spending, Intentions, Competition, Public Networks, Controls.
- **Use of security technologies**
  Technology, Encryption, Knowledge Base, Trends.
- **Quality of operations**
  Business Continuity Management, Benchmarking, Administration, Prevention, Detection, Response, Privileged Users, Authentication, Controls.
- **Privacy**
  Compliance, Ethics, Data Collection Policies, Communication Techniques, Safeguards, Personal Information Protection.

Survey scope

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

"The strategic focus of financial institutions spanned a variety of sectors, including Banking, Securities, Insurance and Asset Management. While industry focus was not deemed a crucial criterion in the participant selection process, attributes such as size, global presence, and market share were taken into consideration."

Who responded

The 2007 Global Security Survey respondent data reflects current trends in security and privacy from 169 major global financial institutions. DTT's GFSI Group agreed to preserve the anonymity of the participants by not identifying their organizations. However, DTT's GFSI Group can state that, overall, the participants represent:

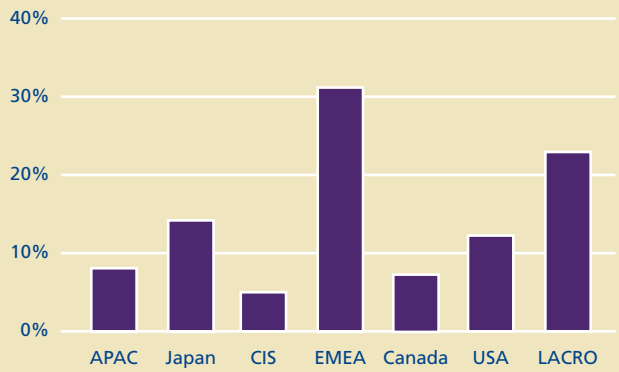
- Top 100 global financial institutions – 29%.
- Top 100 global banks – 26%.
- Top 50 global insurance companies – 14%.
- Top payments and processors – 40%.
- Number of distinct countries represented – 32.

Geographic region

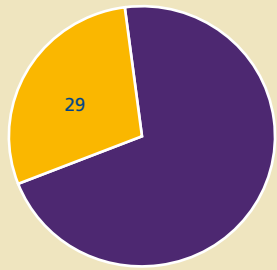
The pool of respondents provides an excellent cross-section from around the world, with a breakdown as follows:

- Asia Pacific (APAC) (excluding Japan) – 8%.
- Japan – 14%.
- Former Soviet Republics – Commonwealth of Independent States – (CIS) – 5%.
- Europe, the Middle East and Africa (EMEA) – 31%.
- Canada – 7%.
- USA – 12%.
- Latin America and the Caribbean (LACRO) – 23%.

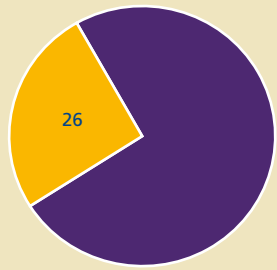
Geographic region



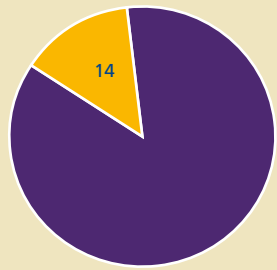
Top 100 global financial institutions (market value)



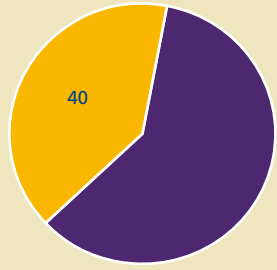
Top 100 global banks



Top 50 global insurance companies (market value)



Top payments and processors



*Results may not total 100% as DTTís GFSI Group is reporting selected information only.

Industry breakdown

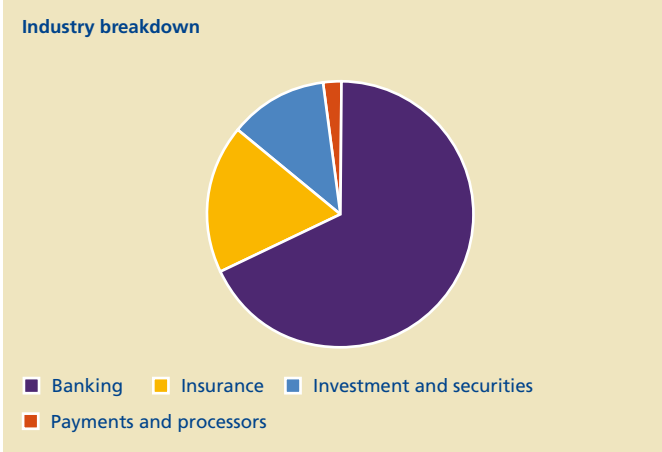
The final survey sample reflects all major financial sectors.

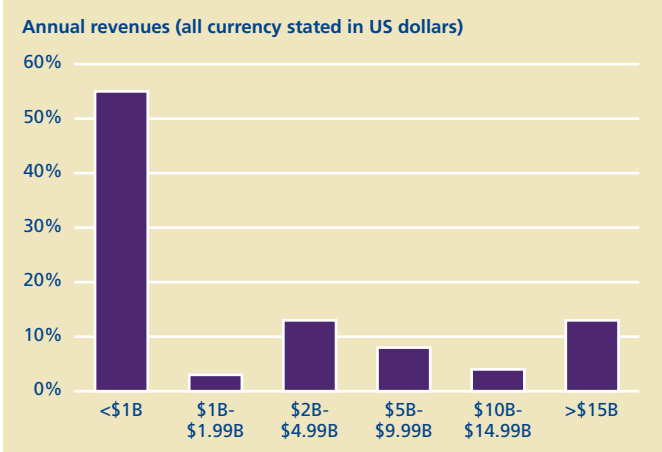
- Banking – 68%.
- Insurance – 18%.
- Investment and securities – 12%.
- Payments and processors – 2%.

Annual revenue

The respondent companies represent a broad spectrum based on annual revenues.

- Less than $1B in annual revenue – 55%.
- $1B-$1.99B in annual revenue – 3%.
- $2B-$4.99B in annual revenue – 13%.
- $5B-$9.9B in annual revenue – 8%.
- $10B-$14.99B in annual revenue – 4%.
- Greater than $15B in annual revenue – 13%.





Geographic segmentation observations

Regional highlight	APAC (Excluding Japan)	Japan	CIS	EMEA	Canada	USA	LACRO	Global
FSIs who feel that security has risen to the C suite or board as a critical area of business	78%	71%	83%	82%	78%	89%	88%	81%
FSIs possessing a security strategy	62%	75%	75%	61%	27%	68%	68%	63%
FSIs whose information security strategy is led and embraced by line and functional business leaders	0%	6%	14%	10%	0%	18%	14%	10%
FSIs who have incorporated application security and privacy as part of their software development lifecycle	30%	22%	0%	33%	18%	36%	46%	32%
FSIs who feel they have both commitment and funding to address regulatory requirements	77%	79%	67%	77%	50%	80%	64%	73%
FSIs who feel that government driven security regulations are effective in improving security posture in their industry	93%	89%	100%	82%	82%	90%	89%	86%
FSIs who have security linked to their IT security employee's appraisals	43%	40%	50%	44%	45%	70%	57%	50%
FSIs who feel they presently have both the required skills and competencies to respond effectively and efficiently to foreseeable security requirements	7%	31%	25%	39%	27%	20%	35%	30%
FSIs whose employees have received at least one training and awareness session on security and privacy in the last 12 months	69%	91%	75%	84%	82%	95%	61%	78%
FSIs who have an executive responsible for privacy	85%	100%	57%	60%	91%	84%	30%	66%
FSIs who have a program for managing privacy compliance	100%	95%	67%	78%	80%	89%	31%	70%
FSIs who have experienced repeated internal breaches over the last 12 months	36%	13%	38%	31%	55%	35%	26%	30%
FSIs who have experienced repeated external breaches in the last 12 months	79%	35%	63%	71%	91%	70%	63%	65%

■ Best in class ■ Worst in class

Asia Pacific (APAC) excluding Japan

In previous surveys, Japan has led the APAC countries on the majority of security and privacy fronts. A majority of APAC respondents (93%) agree that government-driven security regulations are effective in improving security in their industry, second only to the Former Soviet Republics – Commonwealth of Independent States – (CIS): which had 100% agreement.

Seventy-eight percent of respondents indicate that security has risen to the C-suite or board level as a critical area of business and 62% indicate having a security strategy. When it comes to security model structure, 57% of respondents have a centralized model while 29%, a decentralized model. The remaining 14% use a federated model. A majority of respondents (77%) indicate having both the commitment and funding to address regulatory requirements.

But respondents from this region fall far below other regions when it comes to having the required skills and competencies to effectively handle existing and foreseeable security requirements (7%). Along with Canada, none of the APAC respondents feel that their security strategy is led and embraced by line and functional business leaders. When it comes to breaches, 36% of APAC respondents experienced repeated internal breaches and 79% experienced repeated external breaches over the past 12 months. But APAC's commitment to privacy is not lacking: 85% have an executive responsible for privacy and 100% have a program for managing privacy compliance.

Organizations in the APAC region are only just beginning to move beyond their heavy reliance on network firewalls, intrusion detection systems (IDS), and patch management systems. It is likely that the high percentage of external incidents reflected in this year's survey results will decrease once APAC organizations adopt more proactive technologies. These include anti-phishing technologies, application firewalls, intrusion prevention systems (IPS), which protect against vulnerabilities before system/application patches and antivirus signatures are available, coupled with non technological controls such as awareness and training.

Japan

This year, Japan relinquishes its leadership on a number of security and privacy issues to the USA. In the 2006 survey, Japan led the world in eight areas—in 2007 that number has slipped to four. But Japan clearly outstrips every region when it comes to having an executive responsible for privacy: 100% compared with 66% globally. The region also has a strong program for privacy compliance (95%). Japan had the lowest incidents of repeated breaches in security of all regions over the past 12 months (internal incidents: 13%; external incidents: 35%). Japan has the third lowest number of respondents (6%) whose organizations' security strategy is led by the line and functional business leaders. Of respondents who feel that government-driven security regulations are effective, Japan is only slightly higher (89%) than the global average (86%). A full 91% of respondents report that employees have received at least one training and awareness session on security and privacy in the last 12 months.

Of respondents who feel that they had both the commitment and funding to address regulatory requirements, Japan is slightly higher (79%) compared to the rest of APAC (77%) and the global average of (73%). As to whether organizations feel that they have the required skills and competencies to respond to security requirements, Japan is well above (31%) the rest of APAC (7%), and slightly above the global level of 30%. Japan is clearly doing a lot right: its increasing awareness of security issues, the level of caution it has adopted and its insistence on such a high priority for privacy issues have apparently made Japan's organizations the most effective at avoiding security breaches. It may be tempting to link Japan's low incidence of security breaches to their strong focus on privacy issues. However, the reason may well be cultural rather than technological—crime is low in Japan, where stealing is thought to be dishonourable. Stories abound of items left in public places remaining undisturbed until the owner returns to retrieve them.

Former Soviet Republics – Commonwealth of Independent States – (CIS)

The CIS region is new to the 2007 GFSI security and privacy study. Responses come from a number of countries, including Russia, Ukraine and Kazakhstan. CIS respondents lead all regions globally (100%) when it comes to believing that government-driven security regulations are effective in improving security posture in their industry. The strong government influence is likely a factor in this finding. Interestingly, CIS leads all regions (in a tie with Japan) when it comes to possessing a security strategy (75%), but, at 67%, is slightly below the global average (73%) when it comes to having both the commitment and funding to address security regulations. This region has a way to go before it is able to effectively respond to regulation.

Eighty-three percent of organizations in this region feel that security has risen to the C-suite or board level as a critical area of business. When it comes to an information security strategy being led and embraced by the line and functional business leaders, this region, at 14%, is tied with LACRO and is second to the USA (18%). A quarter of CIS respondents indicate that they presently have both the skills and competencies to respond to existing and foreseeable security requirements. Sixty-three percent say that they have a federated security model while the remaining 37% have a centralized security model. Fifty-seven percent of respondents indicate having an executive responsible for privacy and 67% have a program for managing privacy compliance. When it comes to experiencing repeated breaches in security over the past 12 months, 38% have had repeated internal breaches and 63% of CIS respondents reported repeated external breaches.

Surprisingly, CIS leads all regions in two areas: FSIs possessing a security strategy at 75% (a tie with Japan); and FSIs who feel that government driven security regulations are effective in improving security posture in their industry at 100%. However, it is too soon to tell whether these practices and controls are in a mature and effective state.

Europe, the Middle East and Africa (EMEA)

As in previous years, the majority of EMEA respondents (82%) feel that security has risen to the C-suite or board as a critical area of business. The majority (82%) also feel that government-driven security regulations are effective in improving the security posture in their industry. Seventy-seven percent say they have both the commitment and funding to meet the government-driven regulations. A large proportion of respondents (61%) have a security strategy. When asked about their organization's security model structure, 73% have a centralized model while far fewer—10% and 12%—have decentralized and federated models, respectively. The data clearly shows support for a company-wide effort regarding security measures. EMEA has the highest percentage (39%) across all geographic regions when it comes to the required skills and competencies to handle existing and foreseeable security requirements. Eighty-four percent of respondents from EMEA maintain that employees have received at least one training and awareness session on security and privacy in the last 12 months. EMEA respondents also report having repeated security breaches in the last 12 months (repeated internal breaches: 31%; repeated external breaches: 71%).

The region is above the global average for security breaches, a continuing problem for EMEA. In 2012, the eyes of the world will be on the UK when it hosts the Olympic and Paralympic games. The games will generate jobs and revenue but, by far, the biggest component will be information. Protecting the infrastructure of the games will require physical and information security on an unprecedented scale. The Information Security Europe exhibition in London in March, the largest of its kind anywhere, featured an event that went right to the source of the problem. A panel on the final day of the event, called "Security by Obscurity" featured hackers talking about their practices and answering questions from the audience. The panel was introduced with the statement, "For legal reasons, the identity of the panelists will not be revealed."

Canada

A majority of respondents (82%) feel that government-driven security regulations are effective in improving security posture in their industry. Nevertheless, only 50% feel they have both the commitment and funding to address the regulatory requirements. Clearly influenced largely by legal and regulatory requirements, a large majority (91%) of respondents indicate the existence of an executive responsible for privacy and 80% indicate having a program to manage privacy compliance. Nevertheless, only 27% feel that they have the required skills and competencies to respond effectively to existing and foreseeable security requirements. Nearly half the respondents in Canada (45%) have security linked to their IT security employees' appraisals.

As to whether they had experienced any breach in security over the past 12 months, 55% indicate repeated internal breaches and 91%, repeated external breaches. Compared to other regions, these percentages are above the global average. What is interesting, and seemingly a bit at odds with the findings regarding breaches, is that Canada leads all regions by a large margin (81% versus the global average of 73%) in terms of evaluating the security posture of third-party vendors.

The high percentage of repeated external breaches, perpetrated primarily on customers, is likely due to the high concentration of large Canadian financial institutions and to the fact that most Canadian retail customers have more than one bank account.

There appears to be a large discrepancy between the respondents who said they possessed a security strategy in the 2006 survey (70%) and those who say they possess a security strategy in this year's survey (27%). In addition, none (0%) of the Canadian respondents agreed to the statement that the security strategy was fully led and embraced by line and functional business leaders, compared to 75% who felt that way last year. However, it is likely that these findings do not indicate the negative trend that they appear to. What respondents may have called a security strategy in previous years (e.g. policies, standards, guidelines, etc.) they have come to understand is not a security strategy at all. Therefore, this year's response may actually indicate an increasingly sophisticated, informed approach when it comes to evaluating security. In addition, there may be grey areas, as in the case of strategies that have been started and not completed, in which case, the answer to the posed question would still have to be in the negative. It is also highly likely that the comparison with other regions on this question is not an "apples to apples" comparison, since many of those respondents might not fully understand what constitutes a security strategy in the strictest sense.

The sophistication of the Canadian financial services industry and the understanding of the importance of aligning IT and business strategies is reflected in the answer to the question, "To what extent are business and IT security initiatives aligned with each other". Canada, at 45%, is second only to EMEA (46%) in responding to this issue. With increasing regulation and the ever-growing focus on enterprise risk management, alignment of strategies is clearly an area where a great deal of effort will be focused in the future.

Due to the concentration of financial institutions operating within Canada, there is a positive degree of collaboration among them, with a great deal of knowledge transfer and common definitions, such as a security strategy, informally established. Canadian respondents' candid responses to the questions of having a security

strategy and having it embraced by senior management, show that they are "telling it like it is"—which is, after all, what this survey depends upon in order to present objective findings.

United States of America (USA)

The USA leads all regions in the majority of areas. A leading 89% of respondents indicate that security has risen to the C-suite or board level as a critical issue. This region has the highest number of respondents (18%) who indicate that their security strategy is led and embraced by line and functional business leaders though the overall percentage is quite low.

According to this year's survey results, 45% of USA respondent organizations use a centralized security model; 35%, a decentralized model; and 5% each, a federated or other model. A low proportion of USA respondents (20%) feel that they have the required skills and competencies to deal with existing and foreseeable security requirements. As to whether they had experienced any breach in security during the past 12 months, US respondents reported 35% and 70% repeated internal and external breaches respectively.

USA respondent financial institutions have the highest proportion of employees (95%) who have received at least one training and awareness session on security and privacy over the last 12 months. When it comes to having an executive responsible for privacy as well as a program for managing privacy compliance, USA respondents indicate 84% and 89%, respectively. The USA also has the highest percentage of respondents (70%) that have security linked to their IT security employees' appraisals.

The USA leads all regions (80%) who have both the commitment and funding to address regulatory requirements. That commitment appears to extend to federal government efforts as well. In August last summer, the US Senate ratified a long-neglected cybercrime treaty that supporters say will allow greater international cooperation in cybercrime investigations. The treaty calls for signatory nations to cooperate on cybercrime investigations and to pass cybercrime laws that address issues such as computer intrusion, computer-facilitated fraud, child pornography, and copyright infringement. The agreement is expected to help USA agencies in their international efforts by minimizing obstacles to international cooperation that currently impede USA investigations and prosecutions of computer-related crimes.

Latin America and the Caribbean Region (LACRO)

LACRO respondents tie with APAC, and lag behind all other regions, in three categories. In LACRO, the fewest organizations (30%) have an executive responsible for privacy and the fewest (31%) have a program for managing privacy compliance. Respondents indicate the least number of organizations (61%) where employees have received at least one training and awareness session on security and privacy in the last 12 months. Surprisingly, LACRO reported security breaches in the last 12 months just below the global average (26% and 63% reported repeated internal and external breaches respectively). LACRO respondents feel that security has risen to the C-suite or board level as a critical area of business (88%), and that they presently have both the required skills and competencies to respond to security requirements—at 35%, they are the second highest of all regions.

A majority (89%) feel that government-driven security regulations are effective in improving security posture in their industry and 64% indicate having both the commitment and funding to address the regulatory requirements. The LACRO region is second (57%) only to the USA (70%) in having security linked to their IT security employees' appraisals. In this aspect, both regions exceed the global average of 50%.

While LACRO may lag behind other regions in some key areas, the potential of LACRO has been recognized by the major players in the industry. In May, at the third annual Latin American Summit in Chile, Microsoft's Chief Research and Strategy Officer announced the formation of a collaboration between Latin American and Caribbean universities. The Latin American Collaborative Research Federation, as it is called, will work with Microsoft Research to explore emerging information and communication technologies (ICTs) and their applications across the region. The purpose of the research will be toward solving important social and economic issues and developing Latin America's burgeoning knowledge economy.

Key findings of the survey

1. Changing priorities: the need to keep pace with the threat landscape

Conducting the security survey on an annual basis provides us the opportunity to observe developing trends as well as the change in priorities from year to year. In 2007, respondents listed their top five initiatives as:

- Access and identity management – 50%.
- Security regulatory compliance – 49%.
- Security training and awareness – 48%.
- Governance for security – 37%.
- Disaster recovery and business continuity – 37%.

Over the five years of conducting the survey, we have observed that some initiatives remain steadfast, while others are ousted to make room for those that better respond to the changing landscape.

For obvious reasons, security regulatory compliance is the sole initiative that has remained within the top five since the survey's inception. Data protection has been the subject of intense media attention over the last 18 months, due to an alarming number of high-profile losses or theft of customer identities. With the majority of respondents experiencing internal audit findings related to access control, it is not surprising to find that identity and access management has moved from number five in 2006 to number one in 2007.

As respondents realign their initiatives to remain ahead of the threats, they are clearly moving away from a sole focus on shoring up the infrastructure and perimeter against external breaches (improvements to infrastructure did not even make the top initiatives list this year). Instead, organizations are recognizing the need for "defense in depth" through a layered approach of preventative, detective and corrective controls that include technological and non-technological safeguards.

Amid the seemingly never-ending news stories about data loss, leakage of customer information and other disasters, even the best-run organizations are realizing that they are probably not fully prepared for a major disaster or business interruption. In 2006, disaster recovery and business continuity made its way onto the top five initiatives list—and it's back again in 2007. As organizations become more globally interdependent and more reliant on factors outside their direct control (thus exposing themselves to greater and unforeseen risks) they are beginning to plan for what was once envisioned as unimaginable.

2. Identity and access management: the top operational initiative

Respondents of this year's survey identified access and identity management (50%) as their top operational initiative. This is understandable when you consider that three out of the five top internal audit findings are related to identity and access management: excess access rights (45%); lack of audit trails/logging (30%); and access control compliance with procedures (29%).

A major challenge for any large financial institution is ensuring that the privileges for trusted employees are in keeping with the requirements of their position. As an example, in the physical world, no matter how exemplary the track record and work ethic of an individual on the trading desk, that person will never require access to the executive level suites or to the records contained there. Yet sometimes, in the digital world, such access is inadvertently allowed, even though the person's position would never warrant it. It is also common for digital identities to continue to exist well beyond the time the individual has left the organization, or changed their position within the same organization. Studies have shown that, on average, 17 accounts are created for an individual during their tenure with an organization but, on average, only 10 are removed when that person leaves.

There is also the issue of a wide range of users on the organization's network, including employees, vendors, contractors and partners, who may all need access to network resources and applications, from basic Internet access to access to sensitive internal data. As access grows, so does risk. The number of people who need access and applications (that, in turn, have to be developed ad maintained) continues to increase. As organizations race to meet the demand, it is crucial that the corresponding information security controls keep pace – since the survival of a financial institution depends upon the trust it inspires in its users. Tools such as web access management (WAM) offer identity and access management for web facing applications. Though they may be used initially for managing external user access, there is also a growing use of company portals and online databases for employee access.

Another issue around access management is that individuals in positions far down the organization chart from the C-suite could actually be in a greater position to influence shareholder value than the C-suite itself. This is because certain positions, system administrators, for example, are granted privileged access because of their positions. They are, therefore, in a position of high trust. And high trust brings with it the potential for high impact.

This situation is never wholly unavoidable but one of the keys is that background checks and hiring standards must reflect the impact that the individual could have if that person decided to abuse their privilege. Often, simple criminal background checks are not enough, e.g. a conviction for fraud in one province or state may not show up in a simple criminal background check undertaken in another province or state, let alone in another country.

From a business perspective, many organizations are considering implementing access and identity management solutions for benefits beyond those of risk mitigation, security and control. For the CFO, cost reduction can be quickly realized through automated provisioning, deprovisioning and self service password and account reset. With help desk calls ranging between an industry estimate of $10 to $20 per call, these solutions can result in a significant reduction in help desk calls and quickly pay for themselves.

Business owners generally agree that access and identify management solutions invariably improve their business performance because the automated, speedier delivery of these services directly impact interaction, with various constituencies such as a broker, a customer or an employee. With simplified sign-on or synchronized passwords and immediate access to accounts and resources, performance improves and focus can be placed on personalizing the experience by delivering more tailored content.

What is promising about the findings on this topic is that organizations have recognized identity and access management as a critical issue and are proactive in taking steps to address it. A full third of respondents (33%) have deployed web access management systems with many more either piloting presently or piloting in the next 12 months.

Table 1 – Technology and stages of deployment

Technology	Fully Deployed	Currently Piloting	Planning pilot in next 12 months
WAM	33%	6%	9%
User Provisioning	28%	28%	17%
Directories	60%	9%	6%
Smart cards	20%	23%	14%
Biometrics	10%	16%	10%
Tokens	44%	20%	12%
Public Key Infrastructure	28%	11%	11%

3. Application security: generic countermeasures are no longer adequate

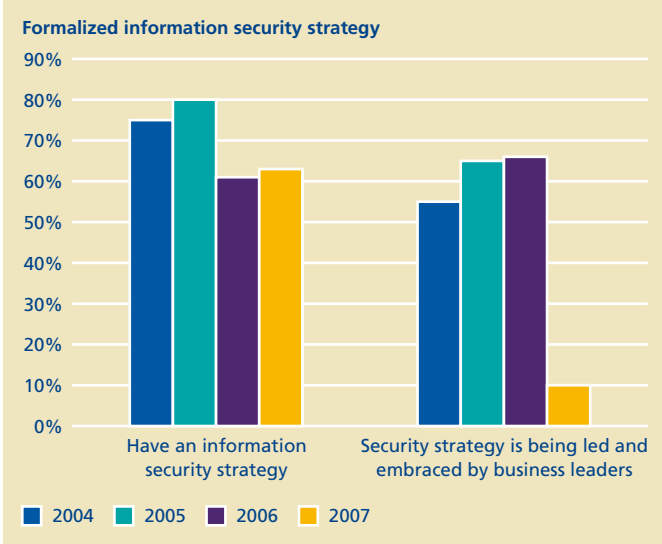
There are those who maintain that the two greatest contributors to communication in the modern age are the printing press and the Internet. For financial institutions in particular, the Internet is pivotal —for some, it is a sole point of contact. As a result, financial institutions continue to invest in on-line applications with the goal of providing secure, borderless, convenient and personalized services to their customers and employees.

But cyber attack risk and threat are ever-present. When they are successful, the result is often financial and reputation damage that impacts customer trust. Organizations have traditionally used general protection measures such as encryption, access control, and network security. But these generic countermeasures are proving inadequate at protecting on-line applications.

It is becoming very clear that decisions made during the software development lifecycle—from user interface design to facilities for patch management—can significantly impact the likelihood of security incidents and the success of a response to them. This is a critical area of concern; in fact, a recent Gartner summit revealed that application security is the number one issue for CIOs. Yet when asked whether their organizations have incorporated application security and privacy as part of their software development lifecycle, the responses were extremely low across the board.

This is one of the greatest pressures faced by financial organizations today, one that is driven by stringent security and privacy regulation as well as the expectation of trust on the part of the customer, the business partner, and the employee. To remain competitive, organizations must mitigate software security risks when they acquire, outsource, implement or host software applications.

The Information Security and Privacy team must continually raise the bar for secure software development by 1) examining software developed internally; 2) demanding trustworthy software from vendors and business partners and 3) ensuring that applications have the adequate controls for audit trails. There must be no ambiguity around the premise that applications are the primary gateway to sensitive data and must be secured from the ground up.



4. The information security paradox: The problems behind the headlines get executive's attention but not their ownership

The casual observer would think, given the nature of the business of financial institutions, that a security strategy would be very much the norm. Our survey supported this assumption—according to respondents, security is a key imperative at more senior levels (board level: 57%; executive management level: 66%).

But, alas, only 63% of respondents have an information security strategy. Others have one in draft form or intend to have one in the next 12 months. Further, only 10% of this year's respondents indicate that their information security strategy is led and embraced by line and functional business leaders. Herein lies the paradox: **even though information security incidents are grabbing the attention of business executives and boards, these individuals do not yet feel that they "own" the problem; in their estimation, the execution of solutions are the mandate of IT.**

Progress is on the horizon, however; 26% of respondents have recognized the need for a security strategy as an initiative for 2007. When asked for the major reasons why information security projects fail to deliver on their promises, nearly half the respondents (48%) indicate shifting priorities (lack of a security strategy to guide an approach). This would indicate that respondents may be starting to understand the need for a strategy and to realize that the absence of a roadmap is detrimental, particularly for financial institutions, in both the short and long terms.

When organizations do not measure return on information security investments, there are difficulties in tracking, budgeting, and planning for the future. This results in the lack of a sustainable and meaningful commitment from the business and functional executives. The survey reveals that a mere 12% of respondents have established formal metrics and another 34% are working on establishing them. But most alarming is the finding that 54% of respondents either have little, if any, way to measure return on security investment or do not attempt to measure it at all.

ROI numbers are the language that executives speak; without them, the security function continues to be seen simply as part of IT and it will not gain the stature that is necessary to promote it as an enabler and a competitive advantage.

5. Data Protection: the layered approach is still the most effective

The traditional approach to information security—concentrating primarily on infrastructure and perimeter strengthening against external breaches—becomes less effective as the threat landscape changes. As information security continues to evolve, so too do business systems; they are now becoming data centric rather than system or transaction centric.

Spending on security technologies is being driven by several concerns. As exposed by many of this year's news headlines and recurring internal audit findings, the majority of financial institutions have long-term problems in the way they have been managing their sensitive and customer data.

Breaches resulting from lax data protection measures can have a significant impact on the brand and reputation of a financial institution and the resulting effect on shareholder value is actually a greater threat than the loss of specific assets.

Many organizations have, and will continue to experience, issues with how they collect, store, manage, archive, use and destruct sensitive data if they do not invest in a coordinated, strategic information security program that addresses all forms of information across the enterprise.

Last year's survey espoused the common sense of the layered approach to help mitigate risk—and that has not changed this year. A layered approach to security, one that combines governance, strong perimeter protection with other forms of access control, logging and monitoring, and data protection techniques, is the right prescription for any organization.

Layering is growing in popularity, as evidenced by the evolution and emergence of a number of technologies, particularly in the applications security, access and identity management and data protection spaces. This trend demonstrates the continuous evolution of information security as respondents begin the transition from infrastructure protection to information protection. In the end, organizations that do not ensure the appropriate implementation of controls to address the range of threats and risks, both internally and externally, face uncertainty, increased cost and turmoil.

Although no organization is immune from risk, its response to risk can either paralyze a potentially successful growth strategy or help to sustain profitable growth. Organizations need to find the appropriate balance between protecting themselves against the risks inherent in information systems and recognizing the benefits of maintaining secure information systems.

6. Security breaches: people remain the weakest link

From an organization's perspective, people include employees, customers, third parties and business partners. All of these people are vital to the organization's survival and are privy to the organization's information in varying degrees and through different means. As a result, all of these people represent risk. Well aware that infrastructures and perimeters have been fortified, today's sophisticated crooks no longer batter the fortress directly—they take a subtler approach through its people.

This year, 65% of survey respondents reported repeated external breaches. When considering each breach, it is useful to look at 1) the group of people it was perpetrated against, (e.g. employees, customers, third parties or business partners); 2) the type of breach the organization suffered and 3) the number of repeated occurrences of that breach (revealing how successful the organization is at combating it).

The top three breaches (those that were repeated the greatest number of times) were viruses and worms; e-mail attacks, e.g. spam; and phishing/pharming. All of these breaches are perpetrated via the customer. For example, a customer receives an electronic, official-looking request on what appears to be their bank's letterhead, requesting sensitive information (e.g. account information, passwords, etc.). By e-mailing back that information, the customer has effectively granted the crook access to their personal financial data and to the financial institution.

The high number of respondents who had repeated occurrences of the top three external breaches reveals that these breaches continue to be successful. When asked whether they should be held accountable for protecting the computers of their customers who do online business with them, 66% of respondents replied in the negative. This finding does not necessarily imply that organizations are unconcerned about their customers' computer security; it is more likely a reflection of the enormity of tackling such a difficult issue. Further, when asked if their organizations had moved beyond password authentication for end user internet transactions, only a little more than half (51%) answered in the affirmative, while 14% and 7% intend to do so in the next 12 and 24 months, respectively.

In addition to breaches perpetrated through the customer, a high number of repeated occurrences of breaches can be attributed to employees, both intentional action (misconduct) and unintentional action (errors and omissions).

Given this situation, it is easy to understand why security training and awareness—always a top concern for executives—joined the ranks of the top five priorities this year. However, although this strategy is good, the execution is typically flawed: first of all, most training and awareness programs are directed towards internal users only (which means that the customer risk category—the source of the greatest breaches—is virtually ignored). Second of all, the training tends to be too high-level and generic to have the desired impact. Organizations that are in the process of developing training and awareness programs need to take into account the audience. They need to provide case studies that the audience can relate to, not a "one size fits all" training program. And results need to be measured—not just by throughput and output but by consequences. In other words, at assessment time—or even more frequently—the question needs to be asked: did the person conduct themselves in a manner that upheld the security requirements of the organization? Truly effective security awareness is achieved through an ongoing process of learning that is meaningful, contextualized and personalized to an individual in their particular role.

Until there is a concerted effort to provide tailored security knowledge and awareness programs to all of the people who comprise an organization's risk categories, organizations will continue to be at the mercy of the growing threat profile.

7. The information security leader: the evolution continues

The role of the CISO continues to gain visibility. The number of organizations with a CISO increased this year to 84% (from 75% last year) and of those, 81% report to the C-suite. Most important is the trend that shows the CISO moving towards strategic activities (94%) and away from typical operations (62%).

In the early days, IT security originated out of IT and had a primary focus on solving IT security issues (e.g. infrastructure, access controls, firewalls, IDS, etc.). As this year's survey indicates, the mandate of the information security function has been redefined. There is now a greater focus on strategic activities (97%: security and planning) while the basic functions of implementation and integration are maintained (76%) and less focus on traditional operations (53%: security operations).

The information security function is often called upon to oversee or collaboratively manage activities outside its traditional, highly technical purview. As a result, many technically focused information security functions now need to look to solving broader business challenges. However, this higher business level is a scary new world for many IT-focused security leaders and their functions, exposing gaps that new responsibilities, organizational structures and leadership require. This phenomenon has caused organizations to re-examine the effectiveness of, and in some cases transform, their existing organizational structures and reporting lines. Many are being forced to re-architect the competencies required of their respective information security functions.

Traditionally, the information security leader has been a technology steward whose role and mandate focused on infrastructure and perimeter protection. Today, as DTT's GFSI Group's survey reveals, the role of the information security leader is rising through the ranks to the upper levels of the organization. This is a trend that will continue, in response to the changing nature of threats and growing customer and employee demands.

8. Third-party relationships: a competitive necessity but a whole new area of risk

The recent headlines have been sensational: computer tapes containing pensioners' and customers' data are discovered missing while being transported by a third-party vendor. In another incident, information is stolen for almost 48 million credit and debit cards during a computer breach at a well known discount retailer.

In the first case, the data (originating from a technology and outsourcing giant) was not encrypted. While this causes immediate security and privacy issues, as well as cost and reputation impact, it also causes public relations issues, with existing customers questioning the competence of the organization to offer encryption products and security outsourcing services. In the second case, groups representing 300 banks file a class action law suit over the breach, called "the largest ever" by the news media.

These incidents—and there are many more examples—highlight the risks inherent in third-party and business partner relationships. In the eyes of the media and the public, the organization that owns the data is always at fault—even if the problem originated with a service provider or a business partner. This is typically due—although not always—to the originating organization's size, stature, name recognition and the amount of data such an organization possesses. Financial institutions rarely, if ever, escape media and regulatory scrutiny when such incidents occur.

There are a number of nascent initiatives to formalize and institutionalize regular security audits on third-party service providers. BITS, an organization in the US, seeks to strengthen the security and resilience of financial services through a variety of measures designed to maintain public and private sector confidence. Similarly, progressive organizations such as VISA and other major payment card industry players are uniting behind data security standards, with the expectation that their merchants will demonstrate compliance. This is likely to become the norm in coming years, particularly as governing bodies and interest groups continue to raise the bar around information security best practices, breach notification, disclosure, individuals' protection and financial retribution.

Regardless of these measures, it is the responsibility of the financial institution to manage its third-party relationships, including those with business partners and vendors. The onus is on these organizations who value their brands to protect their data in an end-to-end manner, in all formats and in all media, whether that data is within the organization's premises or within the premises of a business partner or service provider.

Governance

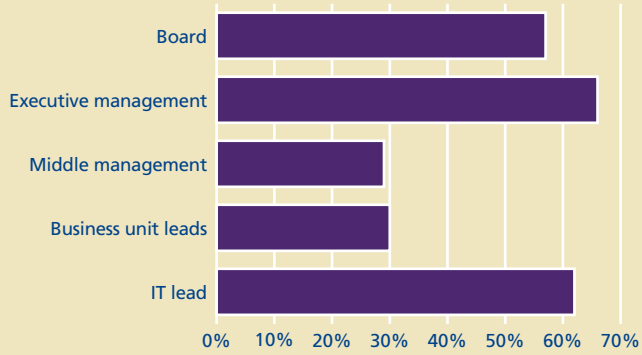
Information security continues to attract the attention of upper management of financial institutions—and for obvious reasons. Identity theft, data leakage, account fraud, phishing, and a slew of other internal and external breaches, in addition to criminal activity, are all making news these days, forcing financial institutions to give these issues their undivided attention.

Information security is no longer a technology-focused problem. It has become the basis for business survival as much as any other issue. Now the public is becoming involved—crimes like identity theft are becoming more prevalent to the general society. The same financial environment that encourages and rewards businesses who provide access to plentiful information turns on them quickly when safeguards are not sufficiently evident. Financial institutions are particularly vulnerable given the nature of the information they hold.

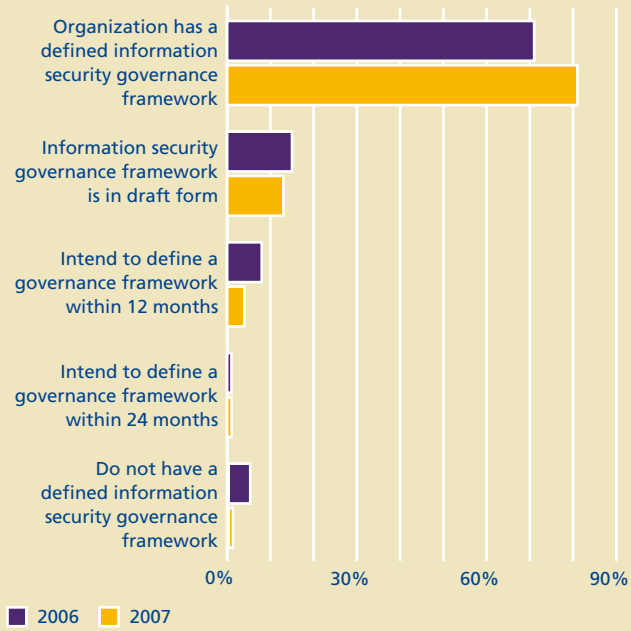
The findings of the 2007 global security survey support this sensitivity. A key finding shows that 81% of respondents, many more than in studies of previous years, feel that the issue of security has risen to the level of the C-suite or board as an issue of critical concern.

A major challenge for financial institutions continues to be the management of information security risks. The challenge is compounded by the need to reassure stakeholders that risks are being managed at acceptable levels but, at the same time, risk is being taken—based on informed decisions—in order to grow the business. Given this tall order, nothing less than top-down, information security risk management will meet the challenge.

Levels at which information security is considered a key imperative in the organization



Presence of a defined information governance framework

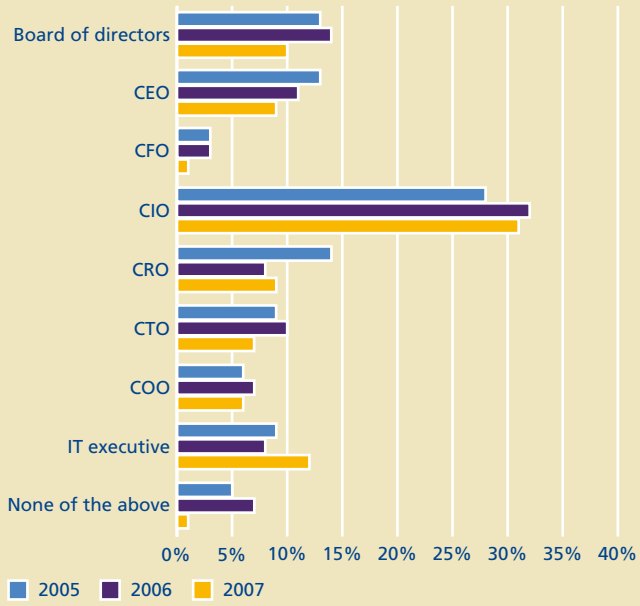


Information Security Governance is a framework predicated on principles and accountability requirements that encourage desirable behaviour in the application and use of technology. Results from the present study indicate 81% of respondents (an increase from the previous year) have a defined information security governance structure (e.g. defined responsibilities, policies and procedures) while another 18% are in the process of establishing one. The 1% of respondents (a significant decrease from previous years) who lack a defined governance framework, feel that their security initiatives are not aligned with the needs of the business.

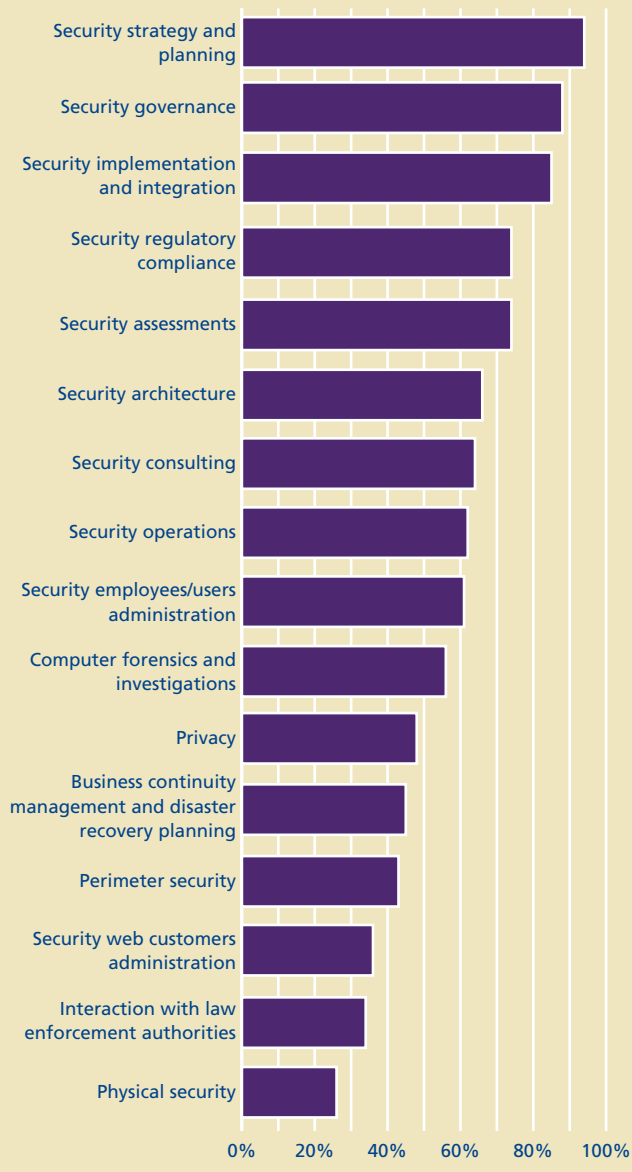
Further breakdown shows:

- 13% of respondents have an information security governance framework in draft form.
- 5% of respondents intend to have an information security governance framework within the next two years.
- 1% of respondents do not have, nor intend to have, an information security governance framework.

Levels of reporting – who the CISO is reporting to



Functions of CISO – what the CISO is responsible for



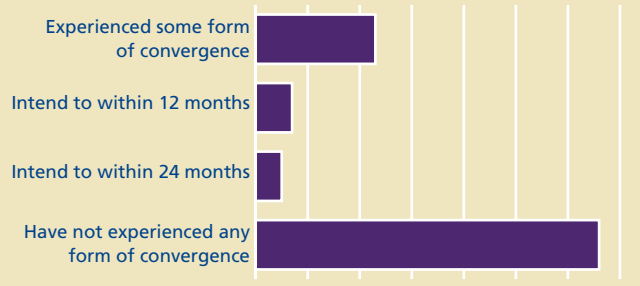
The number of organizations with a Chief Information Security Officer (CISO) has remained consistent with 2006 at 84%. The summary of CISO's tenure below shows that some organizations are continuing to add this position or are grooming the new generation for the position while others continue to retain the existing CISO for longer periods.

Summary of CISOs tenure:

- Tenure of up to two years: 30%.
- Tenure of from three to five years: 31%.
- Tenure of from six to ten years: 22%.
- Tenure of over 11 years: 17%.

An organization's governance structure can be described based on who is involved in governance activities, who has the authority to execute the process and who is ultimately responsible for the area.

Convergence between IT and physical security

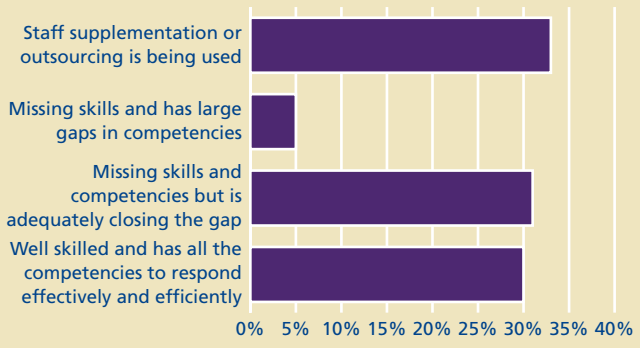


This year, 81% of the CISOs indicate that they report either to the C-suite level (e.g., CIO, CFO, CRO, and CEO) or to the Board of Directors, with the majority (31%) reporting to the Chief Information Officer (CIO). It is interesting to note that of the organizations who believe that security has risen to the C-suite, 69% have their CISO reporting to the C-suite.

As the security industry matures, the mandate of the information security function is being redefined, with a greater focus on strategic activities (94% on security strategy and planning) while maintaining the basic function of implementation and integration (85%) and less of a focus on operations (62%). With global regulation being a significant driver for information security programs, a greater number of information security leaders are undertaking compliance responsibilities (74%).

In regards to which security model organzations have established, 71% responded to having a centralized security model, while 13% each have a federated and decentralized model.

Capability of security professionals



As financial institutions continue to focus on compliance, interdependencies between business functions and optimizing security investments, there is talk in the marketplace about the convergence of physical and logical security.

This can take a number of forms: structurally, where the two groups are combined/aligned or technologically, where technologies are integrated to serve the needs for the organization. Despite the talk, only 23% (a slight rise from 21% from last year) of respondents have considered some form of convergence, while another 12% (a major rise from 4% from last year) are planning to look into it within the next 24 months. When it comes to reporting structures, 55% of respondents have a Chief Security Officer (CSO) and another 16% report that the CISO is also functioning as a CSO.

An information security strategy should provide a solid base for ongoing operations as well as for the enhancement of an overall security program, which is another reason why strategic activities (security strategy and planning) was the number one function (94%) that the CISO is responsible for.

On the subject of change to the numbers of security professionals over the last 12 months, 45% report adding professionals, 47% report neither adding nor reducing head count and 8% report reducing the number of professionals. These numbers indicate a positive trend towards maintaining and enhancing the overall security program. Of course, increasing the number of security professionals does not mean a better security program—capability to handle existing and foreseeable security requirements determines the effectiveness of any program. Thirty percent of respondents report having well skilled staff with all the competencies to respond effectively and efficiently, 31% report not having the skills and competencies but feel they are adequately closing the gap, and 33% report using staff supplementation or outsourcing. There is no better evidence of serious attention to information security than an increasing headcount and a continuing focus on the necessary skills and competencies.

The information security strategy should be aligned with corporate initiatives and maintain a close link between the requirements of the business, the drivers that generate the requirements and the defined strategy.

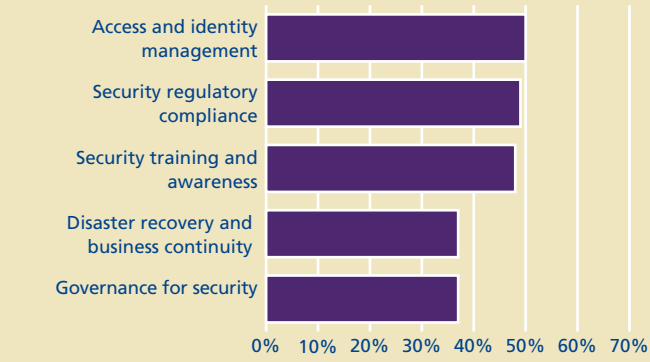
This year, the top five initiatives for information security have evolved to include areas that affect and challenge financial institutions around the globe.

Organizations indicate their top five security initiatives for 2007 as:

- Access and identity management – 50%.

- Security regulatory compliance (including internal audit) – 49%.
- Security training and awareness – 48%.
- Governance for security – 37%.
- Disaster recovery and business continuity – 37%.

Top five security initiatives of 2007

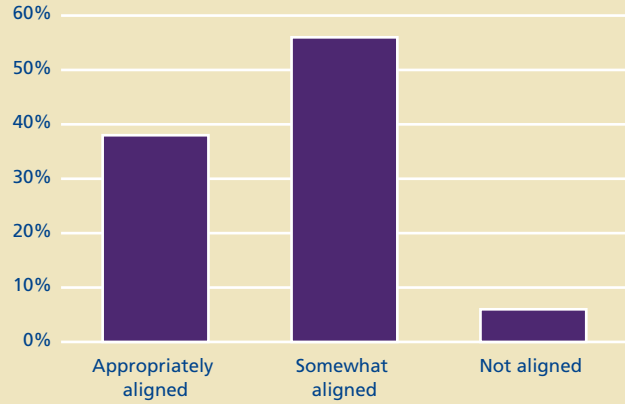


The top five security initiatives from last year's list that were not carried forward are identity theft and account fraud, as well as infrastructure improvement. They have been replaced with security training and awareness, and governance for security.

The fact that security training and awareness and governance for security are becoming critical initiatives for 2007 can be traced to several reasons. One, is that as breaches continue to happen, human error is recognized as one of the causes; another is that government is increasingly regulating the industry, requiring top-down governance, clearly a factor in security being elevated to the C-suite level. These initiatives will provide input and impetus to the information security strategy and the planning process, as well as help in identifying the specific elements that information security governance should address. The top priority areas for 2007 demonstrate a recognition on the part of respondents that the complexity and breadth of information security continue to evolve and the cost of an ineffective security program continues to escalate.

To be able to demonstrate effective information security governance, it is necessary to understand and define expected outcomes, performance targets, efficiency measures and related reporting requirements.

Alignment of business and IT security initiatives



A third of respondents (34%) consider reporting and measurement to be a top initiative for 2007. When asked how they measure return on information security program investments, respondents say:

- We have established formal metrics –12%.
- We are working on establishing formal metrics – 34%.
- Little, if any, measurement is made of security ROI – 19%.
- We do not measure – 35%.

These responses show that a solid percentage are serious enough to have formal metrics already established (12%) or to be in the process of establishing them (34%).

A critical role of the information security function is to act as a liaison between those who own the data and those who implement the controls. When asked about the nature of the alignment between business and security initiatives, respondents are divided as follows:

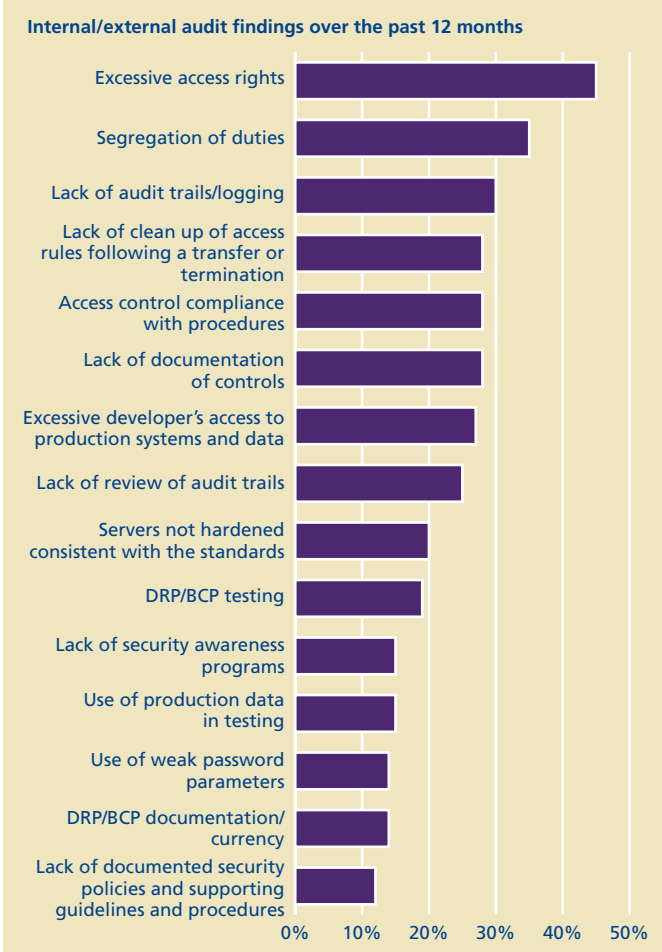
- Business and security initiatives are appropriately aligned – 38%.
- Business and security initiatives are somewhat aligned – 56%.
- Business and security initiatives are not at all aligned – 6%.

Financial institutions continue to operate in an environment of increasing regulation and government legislation that demands more resources for compliance. While an organization's security program will need to address these requirements in some form, risk management will remain a governance issue, requiring top management involvement.

This fact is demonstrated by a majority (73%) of respondents who indicate having both the necessary commitment and funding to address regulatory requirements. Regarding the adoption of international standards such as ISO 27001:2005, 26% are considering and plan to undergo certification within 12 months, while 38% are in the information gathering stage with intent to do so, and 9% have either achieved certification from BS7799-2:2002 or are in the process of transitioning to ISO 27001:2005.

When asked about the top five internal/external audit findings by their organization over the past 12 months, respondents indicate the following:

- Excessive access rights – 45%.
- Segregation of duties – 35%.
- Lack of audit trails/logging – 30%.
- Lack of documentation of controls – 28%.
- Access control compliance with procedures – 28%.
- Lack of clean up of access rules following a transfer or termination – 28%.
- Excessive developer's access to production systems and data – 27%.
- Lack of review of audit trails – 25%.
- Servers not hardened consistent with the standards – 20%.
- DRP/BCP testing – 19%.
- Use of production data in testing – 15%.
- Lack of security awareness programs – 15%.
- Use of weak password parameters – 14%.
- DRP/BCP documentation/currency – 14%.
- Lack of documented security policies and supporting guidelines and procedures – 12%.
- Lack of authorization of changes prior to implementation – 10%.
- Lack of separate testing environment – 9%.
- Existence of default passwords – 9%.
- Lack of server hardening standards – 8%.
- Lack of alignment with known standards (i.e. ISO, CobiT) – 7%.



- Sharing of user IDs with a commonly known password – 7%.
- Scope of coverage – 4%.
- Consistent design of and compliance with security policies across geographies and lines of business – 4%.
- Lack of virus scanning and/or process to keep it current – 4%.
- None of the above – 2%.

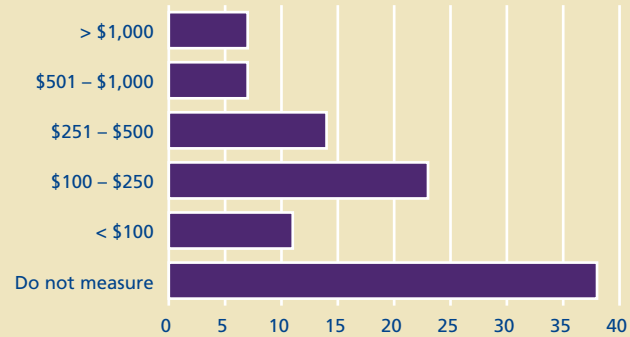
Three of the top five audit findings relate to access, a fact that supports access and identity management being identified as one of the top initiatives for 2007.

Investment in information security

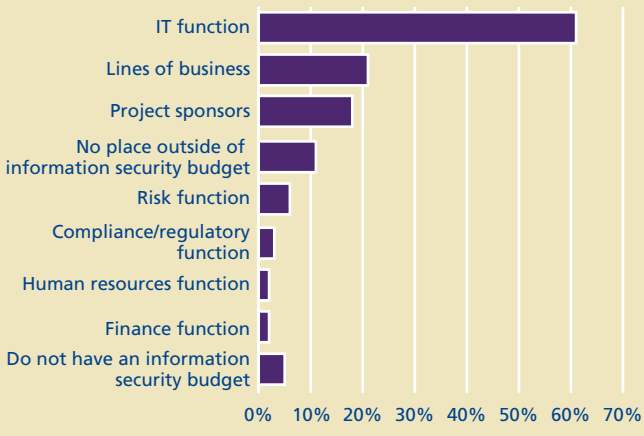
Information security spending by financial institutions continues to rise. Almost all survey respondents (98%) indicate increased security budgets, with 11% reporting an increase of over 15% over 2006. The number of respondents whose security budgets are 1 – 3% of their IT budget (44%) remains relatively unchanged from previous years. The number of respondents whose security budgets are 4 – 6% of their IT budgets increased from 14% in 2006 to 36% in 2007, while 19% indicate that their security budgets are over 7%.

In order to gain a more accurate and meaningful measure of information security spending, this year's study captured data on a per capita basis as well. A solid proportion of respondents (38%) do not measure per capita spending. Of those who indicated that their organization have their information security budget separate from their IT budget, 7% of those respondents spend more than $1000 per person, 7% spend between $501 and $1,000, 14% spend between $251 and $500, 23% spend between $100 and $250, and 11% spend under $100 per person. The DTT GFSI Group's findings demonstrate that information security is still perceived to be an IT issue—58% of respondents indicate that they still do not have an information security budget separate from their IT budget. Outside the IT function, which accounts for 61% of the overall supplemented funding for information security, the lines of business, at 21%, represent the largest area to receive supplemented funding for information security.

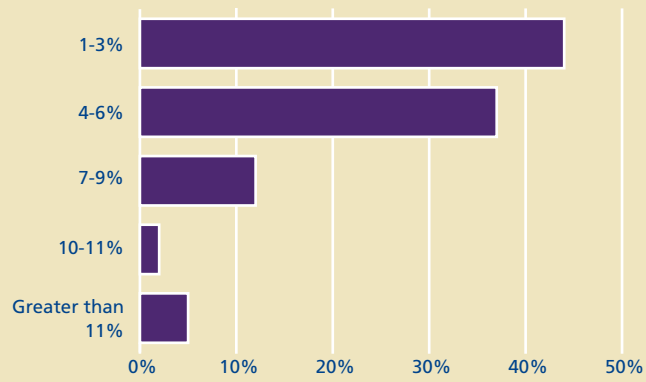
Annual security spending on a 'per employee' basis



Additional information security funding



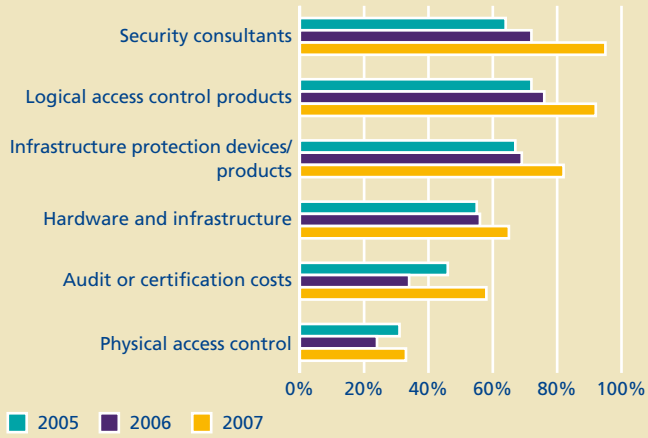
Information security budget (Percentage of IT budget)



Security spending continues to be fuelled by a variety of concerns. The following breakdown of spending within the information security budget in 2007 shows several new areas of spending:

- Security consultants: 95%, up from 72% in 2006.
- Logical access control products: 92%, up from 76% in 2006.
- Awareness /communication costs – 92%, up from 56% in 2006.
- Infrastructure protection devices/products: 82%, up from 69%. in 2006.
- Personnel and organizational costs – 76%, up from 57% in 2006.
- Hardware and infrastructure: 65%, up from 56% in 2006.
- Studies/research costs – 65%, up from 43% in 2006.
- Compliance and risk management – 62%, up from 26% in 2006.
- Audit or certification costs: 58%, up from 34% in 2006.

Information security budget segmentation



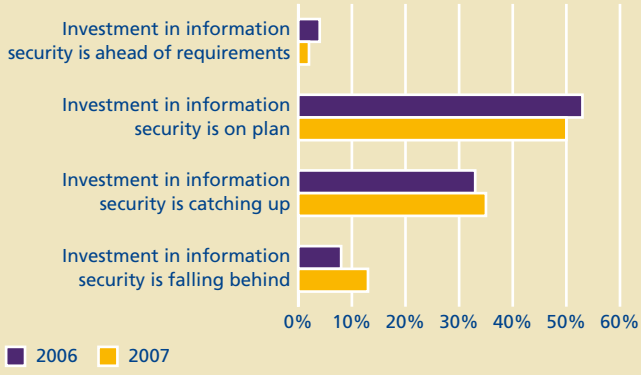
- Security R&D – 53%, up from 17% in 2006.
- Continuity of services (BCP, DRP) – 44%, up from 23% in 2006.
- Physical access control: 33%, up from 24% in 2006.
- Insurance costs – 9%, up from 2% in 2006.

This year's survey continues to support the notion that the human aspect of an information security program is critical to its overall success. While security technology deployment continues to receive the bulk of information security dollars, there is an increase in the number of respondents who now include security awareness and communication costs (employee security training and awareness) in their budgets. This finding is substantiated by the fact that 48% of respondents have identified security awareness and training as the third most important initiative for 2007.

Experience teaches us that effective security awareness is achieved through an ongoing process of learning that is meaningful, contextualized and personalized to an individual in their particular role. Training and awareness need to deliver measurable benefits to the organization through sustainable behavioural changes.

This year, 50% of respondents indicate that their investment in information security is in line with the needs of the business, while 35% feel that they are behind and need to catch up.

Investment in information security

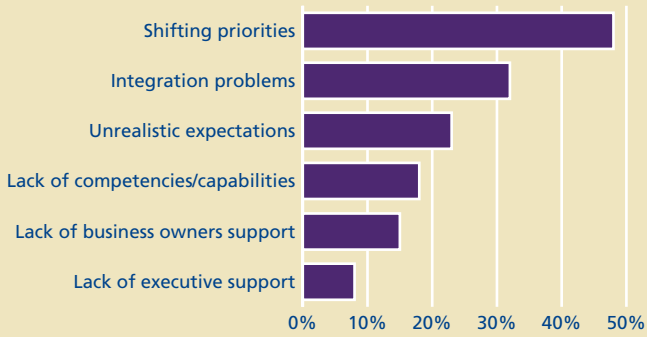


With greater scrutiny of security budgets and increasing attention to the areas of security and compliance, the number of respondents who feel that their projects often fail to deliver what they promise is as follows.

- 1% of all survey respondents stated that over 60% of their projects failed to deliver what they promised.
- 4% of all survey respondents stated that 46% to 60% of their projects failed to deliver what they promised.
- 4% of all survey respondents stated that 31% to 45% of their projects failed to deliver what they promised.
- 12% of respondents stated that 16% to 30% of their projects failed to deliver what they promised.
- 32% of respondents stated that 1% to 15% of their projects failed to deliver what they promised.
- 18% of respondents stated that none of their projects failed to deliver what they promised.
- 29% of respondents do not measure if their projects failed to deliver what they promised.

What factors are seen as the causes for the failures? Not surprisingly, respondents indicate shifting priorities (48%) as the top cause of failure followed by integration problems (32%). Failure is inevitable when priorities shift because the focus becomes so diluted that no goal is met satisfactorily. Another factor that contributes to failure of projects is lack of a documented security strategy (which 37% of respondents do not yet have). When asked how effective their information security function was with regard to meeting the needs of business, 96% of respondents (34%: very effective and 62%: somewhat effective) feel that the information security function is in the most part effective.

Major causes of failure for information security projects



Risk

IT and information security remain crucial considerations for financial institutions, which are held to the highest standards of trust and security. Financial institutions are expected to manage risk effectively, protecting themselves from security breaches from both internal and external sources. The information security strategy is guided by the information security vision which, in turn, is guided by the institution's approach to risk management. A firm's tolerance for risk (risk appetite) dictates its approach to managing risk. As one would expect, 26% of respondents characterized their organization's tolerance for risk to be low; and 66% indicate a moderate level of risk (necessary risk only). A low 8% indicate high risk tolerance on the part of their organization. For the fifth year in a row, respondents indicate that they rely on the risk appetite levels of their counterparts in the industry, with 41% of respondents indicating that they take on comparable levels of risk:

- Take lesser risk compared to the industry, even at a higher cost – 20%.
- Take more risk compared to the industry and at a lower cost – 6%.
- Take the same risk as the rest of our industry – 41%.
- Do not compare – 19%.
- No empirical data available – 14%.

In comparison to last year, 27% of respondents indicate an increase in security breaches in the countries where they have operations, 24% observed a decrease in security breaches but a majority (49%) indicate no dramatic change.

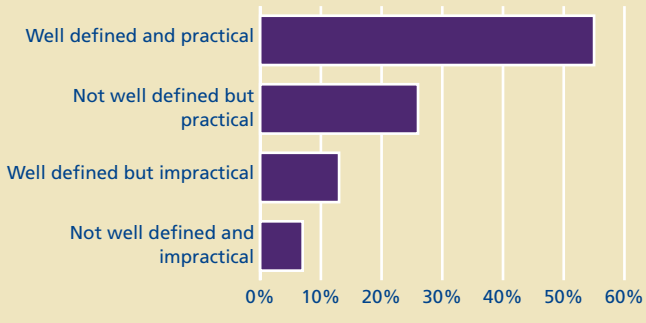
Financial institutions using a systematic approach to managing risk are more inclined to have an ongoing investment in information security and the right controls in place for the business. A risk management program will help in assessing the probability of internal, external, deliberate and accidental threats to information assets. A significant proportion of respondents (74%) have identified and classified their critical IT business assets in terms of different levels of risk. Furthermore, when asked if their organization identifies, quantifies, and prioritizes risk against criteria for risk acceptance and objectives relevant to the operations, 73% responded in the affirmative.

When asked if such risk assessment results have an impact on certain issues, respondents identified those issues as follows:

- Remediation – 76%.
- Regulatory compliance efforts – 68%.
- Training and awareness – 63%.
- Budget and resource allocation – 61%.
- Project portfolio – 42%.
- Physical security initiatives – 38%.
- Compensation and bonuses – 6%.

Asked whether they perceive their company directives to be complete and practical for secure application development, over half of respondents (55%) feel that directives are well defined and practical. With regard to application security, when asked how well their application security and privacy is implemented (as part of the software development lifecycle), 49% indicate it varies from project to project, 37% indicate that it is incorporated in the software development lifecycle, and 14% indicate that, in most cases, it is an afterthought. By and large, the financial services industry considers application security to be a serious matter.

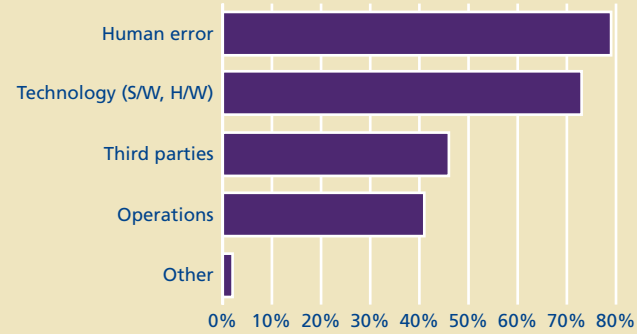
Completeness and practicality of directives for security application development



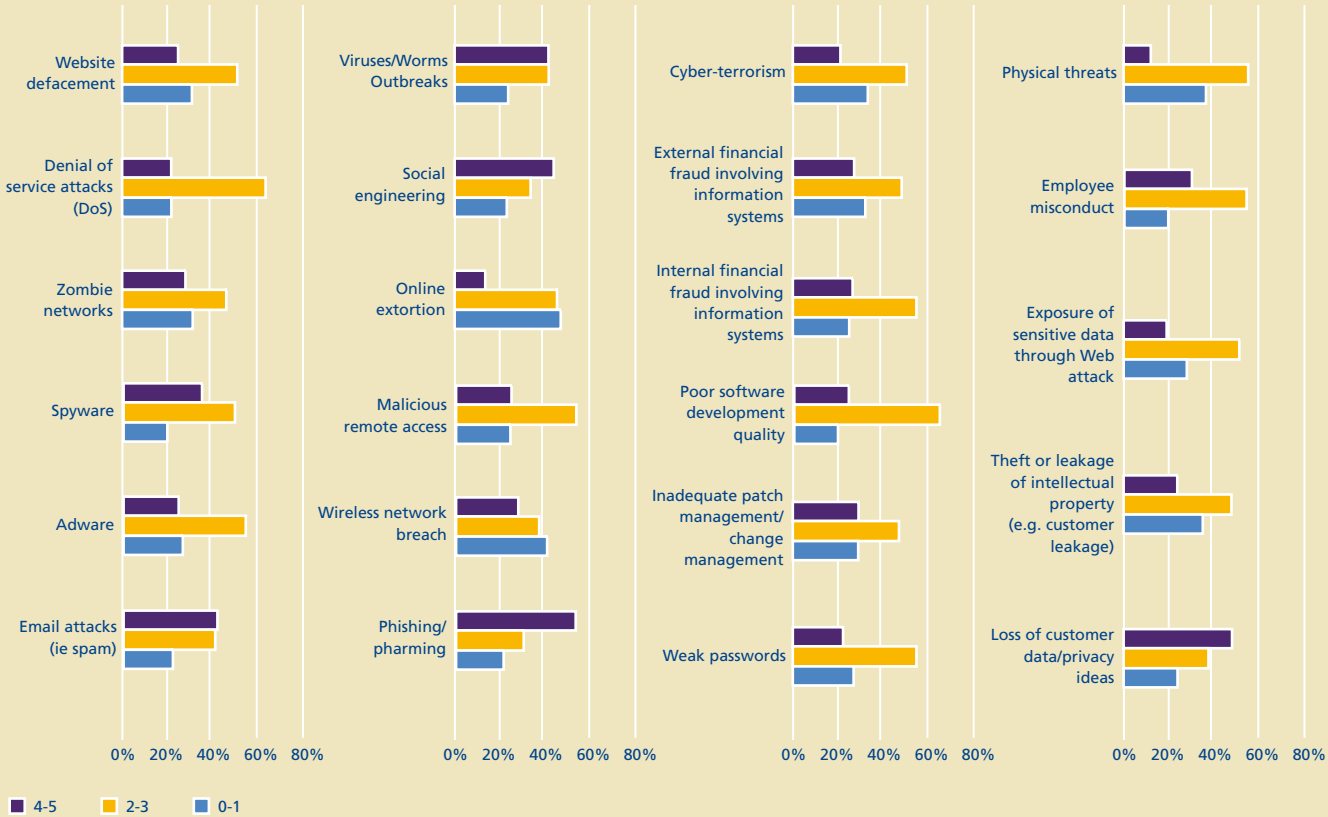
The survey provided a list of threats and asked respondents to rate them (on a scale from 0: non threat to 5: very high threat) over the next 12 months. The threats comprised two categories: malicious external threats and operational threats.

Operational threats overall were considered more critical by respondents, evidenced by the fact that they picked access and identity management as the top initiative for 2007. When asked about their perceptions regarding the root causes of failures of information systems in their organization, respondents chose human error (79%), technology (73%), third-parties (46%), and operations (41%), respectively. With human error topping the list of causes of failures, it is no wonder that security training and awareness are a top initiative for 2007.

Perception of the root causes of failures



Threats envisioned over the next 12 months



Using a scale from 0-5 (0 being a non threat to 5 being a major threat) respondents rated the intensity of the following threats they envision over the next 12 months

The increasing demand for mobility, agility and interoperability from the IT and security functions has led to exponential growth in a variety of communication mediums, all of which open the door to new types of risk. Considering both internal and external attacks, 77% of respondents indicate that they have experienced some form of repeated security breach—a drop from the 82% reported in the previous year. One-time breaches are bad enough but when they occur repeatedly, they indicate a major risk to the organization. However, simply because a breach is frequent does not make it serious in terms of impact—a breach from viruses is typically more frequent than one from employees (intentional or unintentional) yet the latter poses a higher threat by far to the organization. The organization's attention to breaches—and efforts to alleviate them—should be in proportion to the potential impact of the breach.

On the subject of external breaches, the survey question regarding breaches asked respondents to qualify either one occurrence or repeated occurrences of a particular breach. The following findings apply to repeated occurrences. It is interesting to note that, this year, e-mail attacks (spyware) take the number one spot on the list with 52% of respondents reporting them.

Breaches due to employee misconduct (intentional) action also make the list at 31%. On a positive note, breaches reported due to viruses/worms, phishing/pharming, spyware/malware, have fallen from previous year levels of 63%, 51%, and 48%, respectively. This year finds a relatively small decrease in the incidents of denial of service, zombie networks, and website defacement, down from last year's levels of 10%, 9%, and 4%, respectively.

External breach experience

	One occurrence (%)	Repeated occurrences (%)
Viruses/Worms outbreaks	11	40
Email attacks (i.e. spam)	5	52
Spyware	6	26
Zombie networks	2	6
Denial of Service	7	8
Website defacement	2	2
Malicious remote access	4	4
Online extortion	1	1
Wireless network breach	1	1
Phishing/Pharming	5	35
Social engineering	5	17
Employee misconduct	8	31
Theft or leakage of intellectual property	5	8
External financial fraud involving information systems	5	13
Exposure of sensitive data through Web attacks	1	1
Physical threats	8	10
Accidental instances	4	14
Other form of external breach	3	2
Do not know	3	4

Emphasizing the positive news about internal breaches, incidence of viruses/worms, internal financial fraud, and leakage of customer data have all fallen from the previous year levels of 31%, 28% and 18%, respectively. However, breaches due to accidental instances (13%) and loss of customer data/privacy issues (8%) are reported this year for the first time.

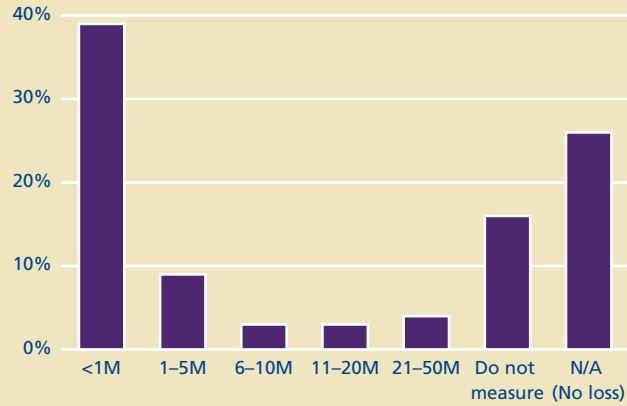
Internal breach experience

	One occurrence (%)	Repeated occurrences (%)
Viruses/Worms outbreaks	8	13
Wireless network breach	1	0
Loss of customer data/privacy issues	4	8
Internal financial fraud involving information systems	7	11
Theft or leakage of intellectual property (e.g. customer leakage)	3	7
Accidental instances	5	13
Other form of internal breach	2	10
Do not know	3	2

The damage from breaches includes mostly direct financial costs (58%) with some exposure to internal costs (30%) and "reputational" costs (12%) as well. This year's damages are as follows:

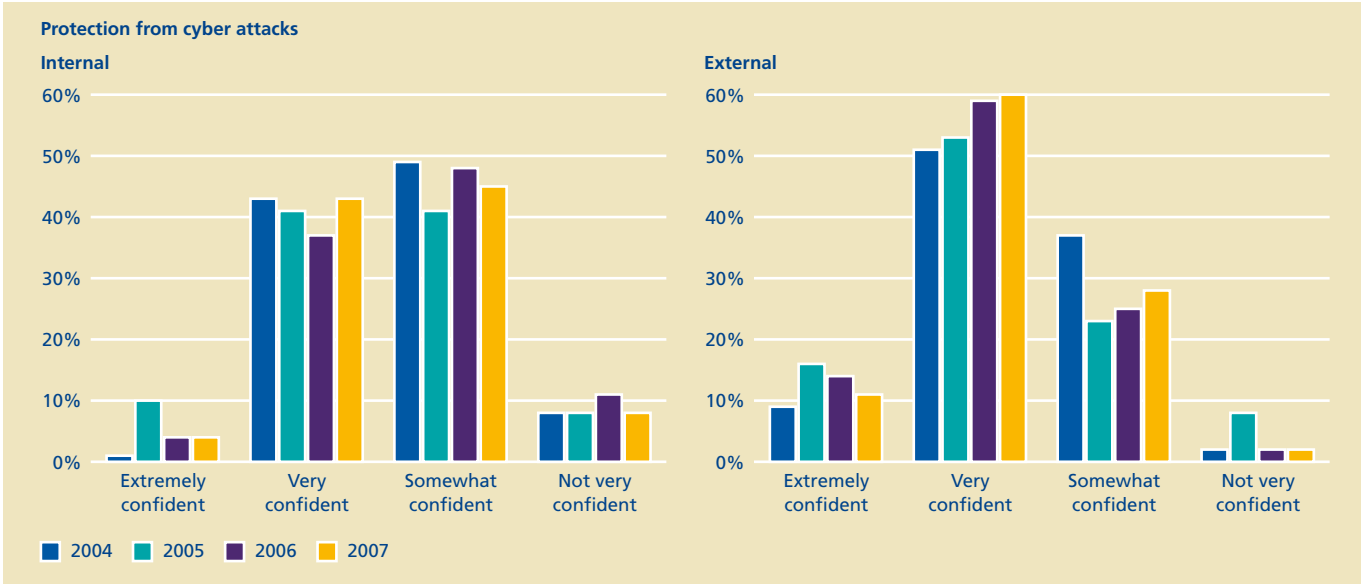
- Less than 1M – 39%.
- 1 to 5M – 9%.
- 6 to 10M – 3%.
- 11 to 20M – 3%.
- 21 to 49M – 4%.
- Do not measure – 16%.
- N/A have not experienced a financial loss – 26%.

Damage sustained due to attacks



When asked whether they should be held accountable for protecting the computers of their customers who do online business with them, 66% of respondents replied in the negative. This finding does not necessarily reflect lack of concern but more likely, a hesitancy to tackle such an enormous undertaking. Further, when asked if their organizations had moved beyond password authentication for end user internet transactions, a little more than half (51%) answered in the affirmative, while 14% and 7% intend to do so in the next 12 and 24 months, respectively. Clearly, financial institutions are doing their best to ensure that security is not diluted.

Respondents remain confident that their organization's networks are protected from attacks internally, with a majority indicating that they are very confident (43%) or extremely confident (4%). When it comes to external attacks, 71% indicate that they are either "very confident" or "extremely confident".



A respectable 74% of institutions have classified their information assets with respect to confidentiality and privacy while 63% provide users with instructions, reference material and the required training to classify their information assets.

A large majority of respondents report information security incidents to law enforcement with 8% reporting on all incidents but 77% only when relevant.

Use of security technology

In deciding whether to adopt a new technology, timing is critical. Those who invest too soon run the risk of entering into costly implementation fraught with integration difficulties. Those who wait too long run the risk of being left behind with old technologies. This dilemma helps to explain the consistently cautious attitudes related to risk from one year to the next. Some respondents in this year's survey (44%) classify themselves as the early majority or "effective users of demonstrated technologies" with only 16% willing to take the risk associated with being an early adopter. Nearly a third of respondents (30%) classify themselves as the late majority, implying they are willing to wait until the technologies become the norm or are less expensive.

Wireless technologies are more susceptible to breach than other technologies. Respondents were asked how their organizations handled the use of three types of wireless technologies: wireless LAN, infra red networking and mobile devices.

Organizations handling of wireless technology

	Prohibit use	Offer employee guidelines on secure use	Publish policies on acceptable business	Implement and encourage use of secured technologies
Wireless LAN capability (e.g. IEEE, 802.11a etc.)	45%	14%	16%	25%
Infra red networking	75%	9%	8%	8%
Mobile devices (i.e. PDAs, Blackberries)	13%	23%	27%	37%

Unauthorized disclosure of personal information leads to violation of regulatory compliance and has the potential to cause extensive damage to the financial institution's reputation, along with significant direct and indirect costs. As well as complying with global regulation to protect information, each institution must ensure that contractual obligations with outsourcers, partners and contractors, as well as privacy policies are implemented to help monitor risks. Content monitoring and filtering technologies can help detect the malicious and accidental misuse of private data and the intellectual capital of the organization. To this end, 31% of organizations indicate that they currently track and report publicly the loss of customer data; while 76% monitor employee use of the internet and information systems for unauthorized or inappropriate access/usage.

Fully deployed technologies have remained relatively consistent over the years, with promising technologies aligned with priorities. This is an area of identity management that has received a lot of attention over the last few years as financial institutions deal with the ongoing challenge of identifying, managing and controlling users and their access permissions. Some organizations are experiencing ongoing difficulties selling the business case for identity management while others are touting the benefits of complementary solutions to help get buy—in from various parts of the organization. One of these solutions is Enterprise Single Sign On (SSO) (which 33% of respondents indicate that they use). SSO allows users to use a single password to access various resources thereby saving costs in a number of areas, such as password resets.

When asked which of the following technologies they have deployed or are piloting, respondents indicate the following:

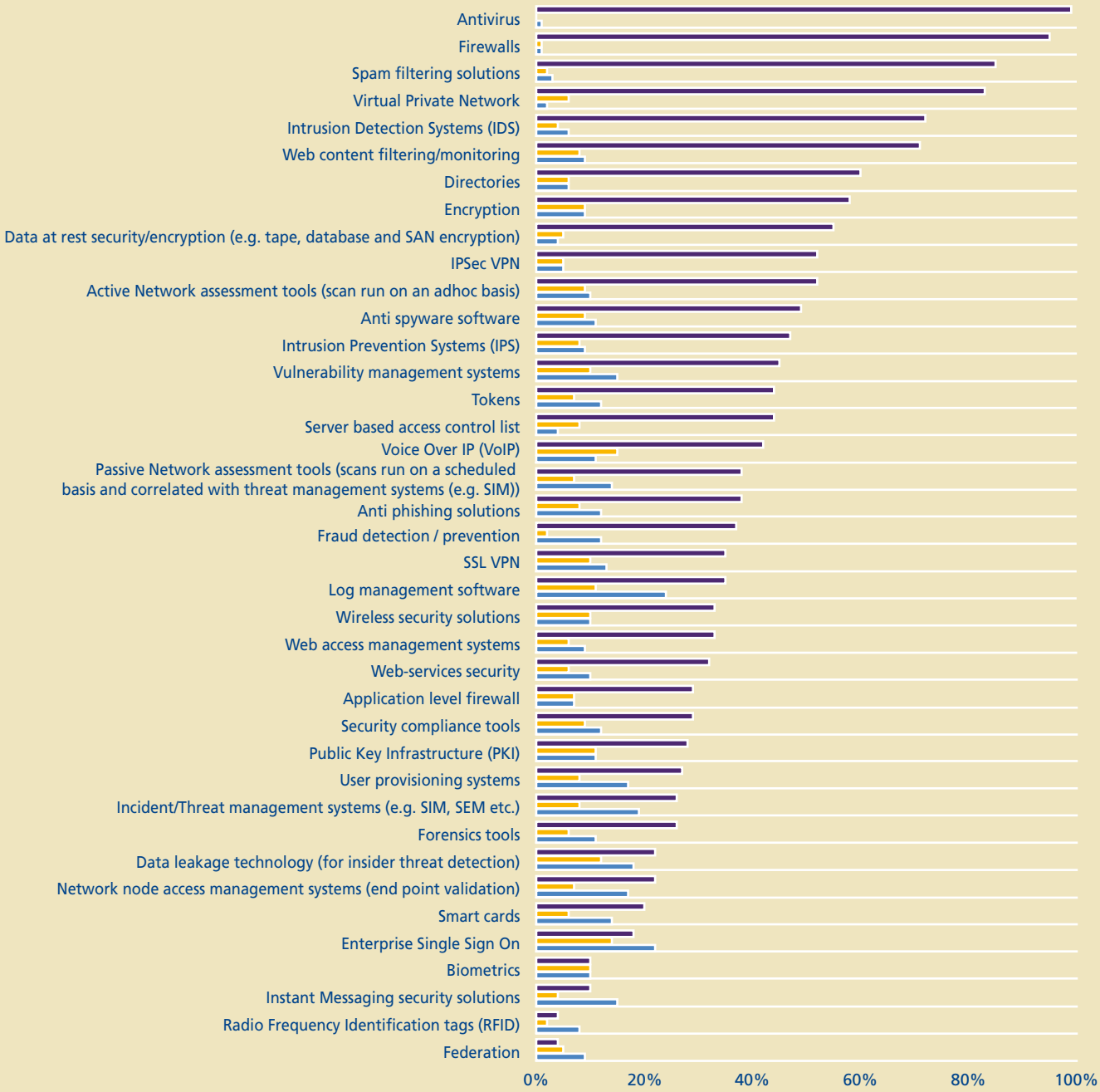
- Antivirus – 99%.
- Firewalls – 96%.
- Virtual Private Network (VPN) – 89%.
- Spam filtering solutions – 86%.
- Web content filtering/monitoring – 78%.
- Intrusion Detection Systems (IDS) – 76%.
- Directories – 66%.
- Encryption – 66%.
- Active Network assessment tools (scan run on an adhoc basis) – 61%.
- Data at rest security/encryption (e.g. tape, database and SAN encryption) – 60%.
- Anti spyware software – 58%.
- Voice Over IP (VoIP) – 57%.
- IPSec VPN – 57%.
- Intrusion Prevention Systems (IPS) – 55%.
- Vulnerability management systems – 55%.
- Server based access control list – 52%.
- Tokens – 51%.
- Anti-phishing solutions – 46%.

- Log management software – 46%.
- Passive Network assessment tools (scans run on a scheduled basis and correlated with threat management systems (e.g. SIM)) – 45%.
- SSL VPN – 45%.
- Wireless security solutions – 42%.
- Security compliance tools – 39%.
- Public Key Infrastructure (PKI) – 39%.
- Fraud detection/prevention – 39%.
- Web – services security – 38%.
- Web access management systems – 38%.
- Application level firewall – 36%.
- User provisioning systems – 35%.
- Incident/Threat Management systems (e.g. SIM, SEM etc.) – 34%.
- Data leakage technology (for insider threat detection) – 34%.
- Enterprise Single Sign On – 33%.
- Forensics tools – 32%.
- Network node access management systems (end point validation) – 29%.
- Smart cards – 26%.
- Biometrics – 20%.
- Instant Messaging (IM) security solutions – 14%.
- Federation – 9%.
- Radio Frequency Identification tags (RFID) – 6%.

In an effort to understand how respondents feel about the changing landscape, this year's survey asked which technologies they would be piloting or deploying over the next 12 months. The technologies with corresponding percentage responses are following:

- Log management software – 24%.
- Enterprise Single Sign On – 22%.
- Incident/Threat Management systems (e.g. SIM, SEM etc.) – 19%.
- Data leakage technology (for insider threat detection) – 18%.
- User provisioning systems – 17%.
- Network node access management systems (end point validation) – 17%.
- Vulnerability management systems – 15%.
- Instant Messaging (IM) security solutions – 15%.
- Smart cards – 14%.
- Passive Network assessment tools (scans run on a scheduled basis and correlated with threat management systems (e.g. SIM)) – 14%.
- SSL VPN – 13%.
- Tokens – 12%.
- Security compliance tools – 12%.
- Fraud detection/prevention – 12%.
- Anti phishing solutions – 12%.
- Voice Over IP (VoIP) – 11%.
- Public Key Infrastructure (PKI) – 11%.
- Forensics tools – 11%.
- Anti spyware software – 11%.
- Wireless security solutions – 10%.
- Web – services security – 10%.
- Biometrics – 10%.
- Active Network assessment tools (scan run on an adhoc basis) – 10%.
- Web content filtering/monitoring – 9%.
- Web access management systems – 9%.
- Intrusion Prevention Systems (IPS) – 9%.
- Federation – 9%.
- Encryption – 9%.
- Radio Frequency Identification tags (RFID) – 8%.
- Application level firewall – 7%.
- Intrusion Detection Systems (IDS) – 6%.
- Directories – 6%.

Security technologies deployed, piloted and planned



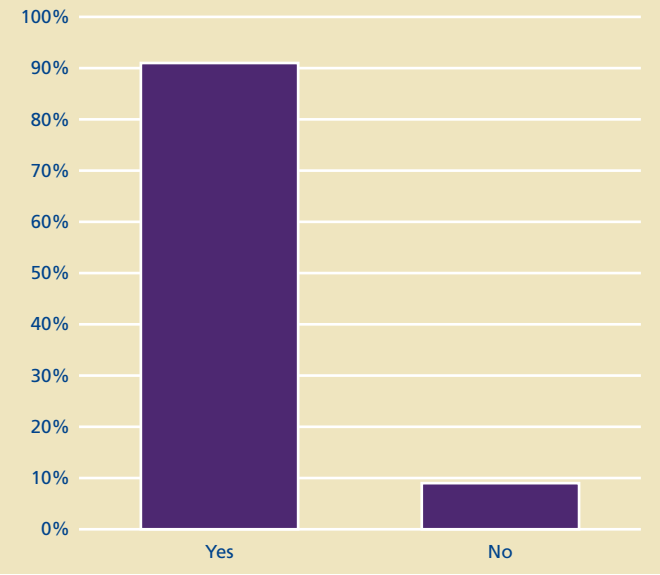
Quality of operations

Financial institutions fully realize that they must proactively work toward protecting customer data and thwarting emerging threats. Security efforts are clearly evident in many organizations through an increasing focus on areas such as training and awareness, improved processes, and complementary technologies, as well as the ongoing dissemination and sharing of good practice within the industry. As they focus more on these areas, financial institutions are finding themselves with a stronger line of defense in the evolving security landscape.

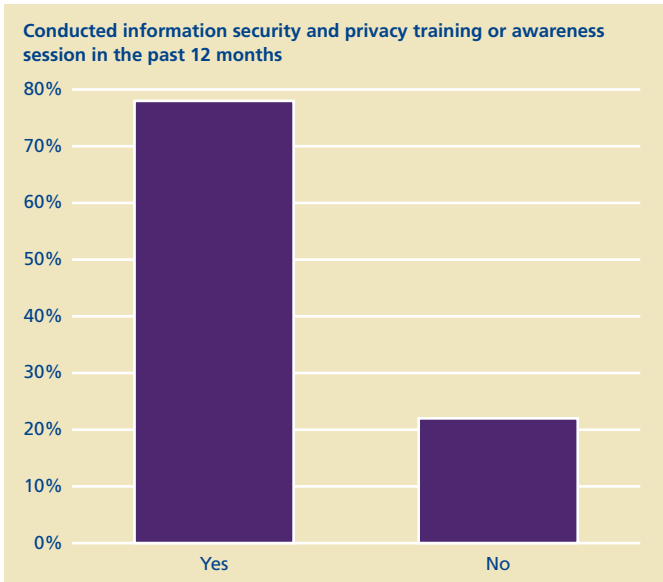
It is encouraging to note that information security professionals in 81% of organizations have defined and documented job roles and responsibilities. However, since only 50% link performance measures to performance appraisals, it raises the question of how one can effectively manage and improve that which is not measured.

A key trend, identified in last year's survey and continuing to factor into this year's findings, is that internal security threats represent a significant number of the information security incidents that impact an organization. A full 91% of this year's respondents indicate that they are concerned about employee misconduct (intentional action) and errors and omissions (unintentional action) involving their information systems. While training has limited effect on employee misconduct, it has a great deal of effect on errors and omissions, which explains why 78% provided their employees with at least one session of information security and privacy training in the last twelve months. Of those who provided training, web page and e-mail alerts (52%) were identified as the number one medium for messaging, and e-learning (46%) was the number two medium. It is interesting to note that 32% of respondents also have orientation training to help mitigate the effects of bad habits that may have been present from the first day of employment.

Concern about employee misconduct involving information systems



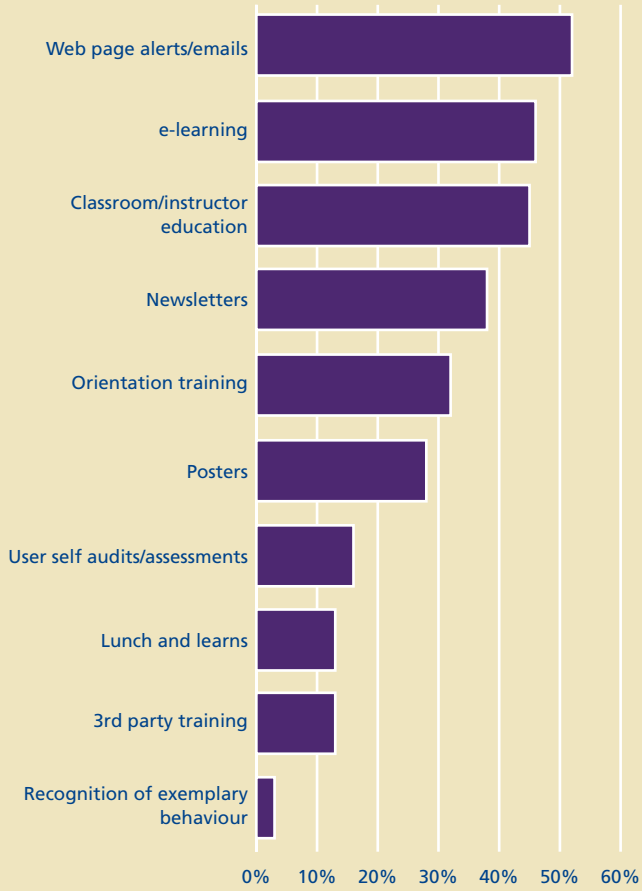
Conducted information security and privacy training or awareness session in the past 12 months



The most common mediums for security training and awareness are:

- Web page alerts/emails – 52%.
- e-Learning – 46%.
- Class room/instructor education – 45%.
- Newsletters – 38%.
- Orientation training – 32%.
- Posters – 28%.
- User self audits/assessments – 16%.
- Lunch and learns – 13%.
- 3rd party training – 13%.
- Recognition of exemplary behaviour – 3%.

Methods for delivering information security training and awareness



While the large majority of the threats to information security are due to errors and omissions (human error: 45%; operational error: 40%) rather than to malicious intent (2%), it is important to note that, of those institutions that experienced a successful internal breach, 14% of the breaches were due to theft or leakage of intellectual property (e.g., leaking of customer data).

Although awareness and training programs have proven to be effective in dramatically reducing problems associated with human error, it is important to address the root causes of these breaches (e.g., access control, poor information management practices, etc.). Access and Identity management (50%) and Security training and awareness (48%) were identified among the top five priorities for financial institutions in 2007. While the individual's contribution to the increase in identity theft cannot be downplayed, it is an organization's information management and security practices that are largely to blame. Many of the high—profile customer data breaches that have been the subject of headlines over the last 18 months are the result of a failure of business practices, not solely of technology. One of the business practices that often fails is the management of users' identities. Data security is all about protecting data from unauthorized access and unauthorized use **after legitimate access has been granted.**

An institution can never be prepared to completely thwart every threat it faces. Over the years, financial institutions have come to pay more attention to establishing programs of business continuity management, which allow businesses to continue their routines in the event of crisis. The utility of these programs is more pronounced when the threats are severe enough to stall business operations in their entirety. Respondents indicate the following as key drivers behind the establishment of their business continuity program.

Key drivers behind business continuity planning

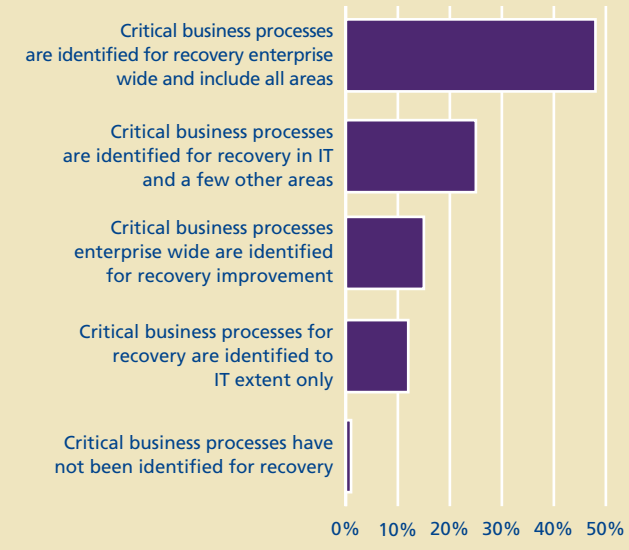
As the table below suggests, senior management's involvement in business continuity planning is not a fallacy. The fact that 32% report that their executive involvement is active and consistent in setting and driving business continuity planning is a significant finding.

Senior management's involvement in business continuity planning

Active and consistent executive involvement is setting and driving business continuity planning	32%
Senior management has approved a program of business continuity planning	23%
Senior management is aware of the importance of business continuity planning	22%
Executive committee is responsible for annual review of business continuity planning	19%
No senior management involvement	1%
N/A – do not conduct any business continuity planning efforts at this time	3%

Nearly half the respondents (47%) indicate having business continuity plans in place to recover mission-critical processes, while another 15% require these plans and have guidelines for implementing them throughout the company. This shows that respondents, in the aggregate, have an advanced state of business continuity planning.

Scope of critical business processes recovery

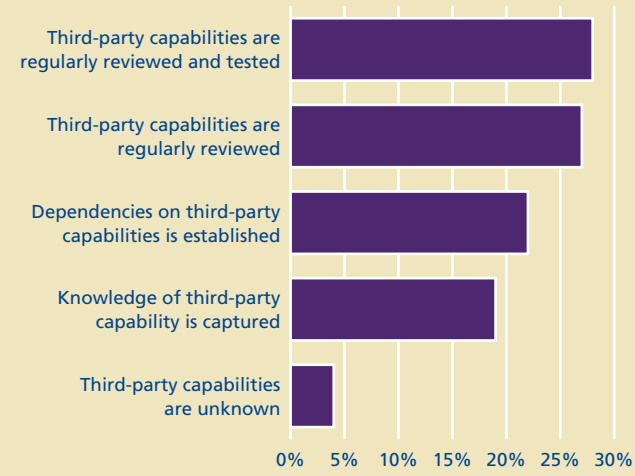


Support for this is evidenced from several findings in the study:

- While 66% of the sample has a crisis management team, 39% have their team procedures tested periodically for preparedness to handle crises.
- Critical processes are identified enterprise-wide for recovery by 63% and 15% slate them for recovery improvement.
- Third-party capabilities are regularly reviewed (27%) while some also test them (28%).
- Regular testing of all business continuity components is performed by 40% and independent facilitation of such testing, by another 7%.

A particular area of focus for financial institutions should be the application of protections to data and systems across the organization, extending as well to third-party suppliers and outsourcing partners. These third-party relationships need to be examined based on their ability to manage security risks, processing and the confidentiality of applications and data. Sixty-seven percent of respondents conduct objective independent reviews of the vendor to evaluate their security posture before engaging. While many organizations feel that they have adequately controlled their information, they may need to be reminded that many of their internal controls do not "follow" information assets once they leave the confines of the organization. Contracted or outsourced services may well have a different level of security controls, rendering the associated risks unknown and owner accountability irrelevant. To compete effectively for the business of financial institutions, outsourcers and contractors need to get used to being able to demonstrate their ability to comply with enhanced security requirements.

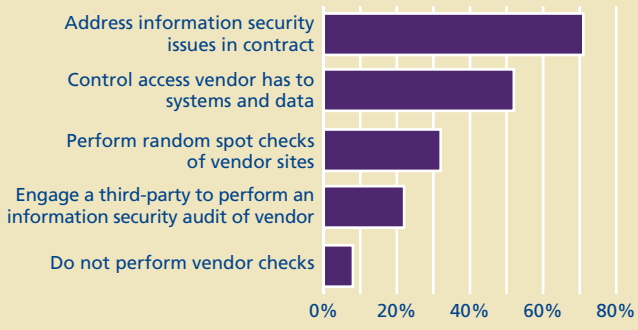
Third-party capabilities



To ensure that vendors' activities are adequate with regard to information security, the following methods are adopted:

- Address information security issues in contract – 71%.
- Control access vendor has to systems and data – 53%.
- Perform random spot checks of vendor sites – 31%.
- Engage a third party to perform an information security audit of vendor – 22%.
- Do not perform vendor checks – 8%.

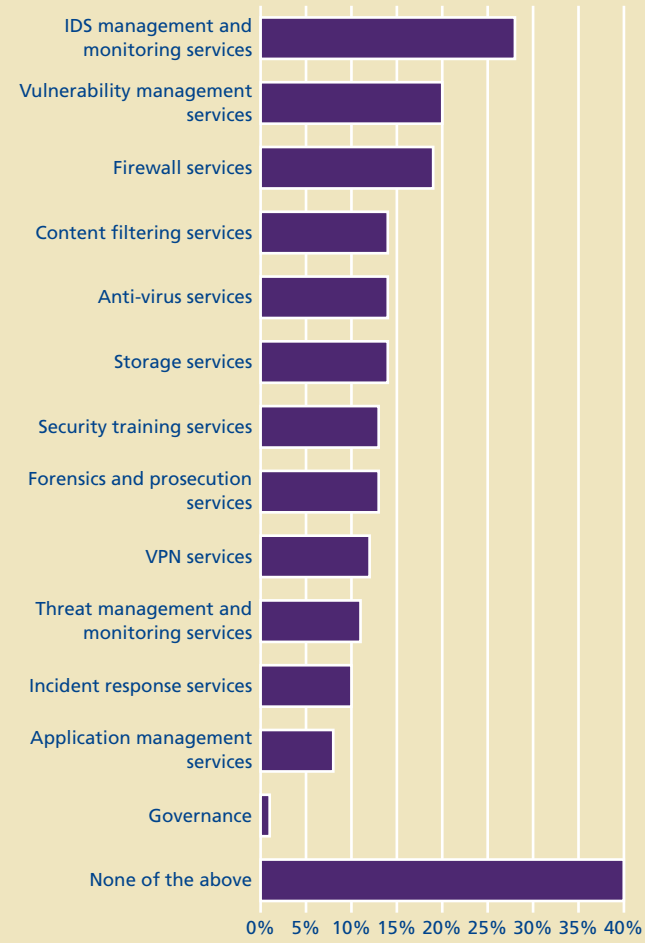
Ensuring information security with outsourcing vendors



This year, 60% of respondents indicate that they have outsourced at least one area of information security activities. Of those, IDS management and monitoring services (28%), vulnerability management (20%) and firewall services (19%) were among the top areas, while governance (1%) was the least outsourced area. Managing the risk of an outsourced arrangement can be complex and time consuming, particularly when one considers the variances among providers' cultural, legal, and security standards. As the amount of information that flows between companies, business partners and customers continues to increase, there should be a corresponding increase in safeguards, including due diligence and reviews of outsourcers' practices and procedures.

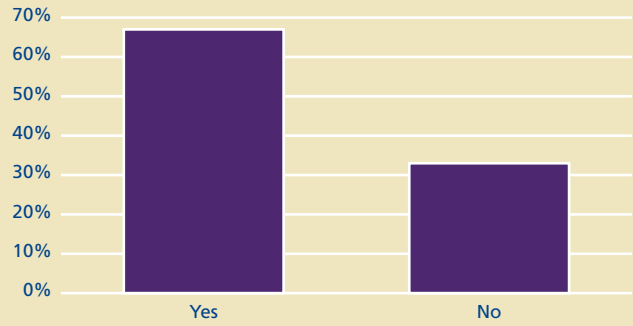
"To compete effectively for the business of financial institutions, outsourcers and contractors need to get used to being able to demonstrate their ability to comply with enhanced security requirements."

Outsourcing for information security activities



Mergers, acquisitions, and dispositions have become quite frequent in the recent past and there is every indication that this strategy will continue in the future. Financial institutions are well acquainted with mergers and acquisitions. What is the role of information security during such events? While a majority (38%) indicate that the question is not applicable in the present study, 35% indicate their role to be reactive (during negotiations) and 22% indicate their role to be proactive (prior to negotiations).

Vendor security posture evaluation before engagement



The crooks that are intent on breaching the security of an organization recognize the need to be adaptable. As infrastructure security becomes more effective, their focus shifts to application layer attacks. Web applications are no longer just software tools. In many cases, they are the organization's central nervous system. Their scope of usage continues to include the processing of customer transactions and the provision of information, both functions that are connected to critical resources and systems. As organizations acquire, outsource, implement and host applications, they must recognize and mitigate software security risks. Application security means ensuring that there is secure code, integrated at the development stage, to prevent potential vulnerabilities and that steps such as vulnerability testing, application scanning and penetration testing are part of an organization's software development lifecycle. This year, 87% of respondents feel poor software development quality is a top threat envisioned over the coming 12 months.

Respondents reported the following frequencies for these practices:

Frequency of security reviews

	Quarterly	Semi-annually	Annually	Adhoc	Never
Vulnerability scanning	38%	11%	18%	26%	7%
Penetration testing (internally)	18%	12%	26%	28%	16%
Penetration testing (externally)	16%	16%	34%	24%	10%
Application security code review	7%	1%	8%	61%	23%

"Application security means ensuring that there is secure code, integrated at the development stage, to prevent potential vulnerabilities and that steps such as vulnerability testing, application scanning and penetration testing are part of an organization's software development lifecycle."

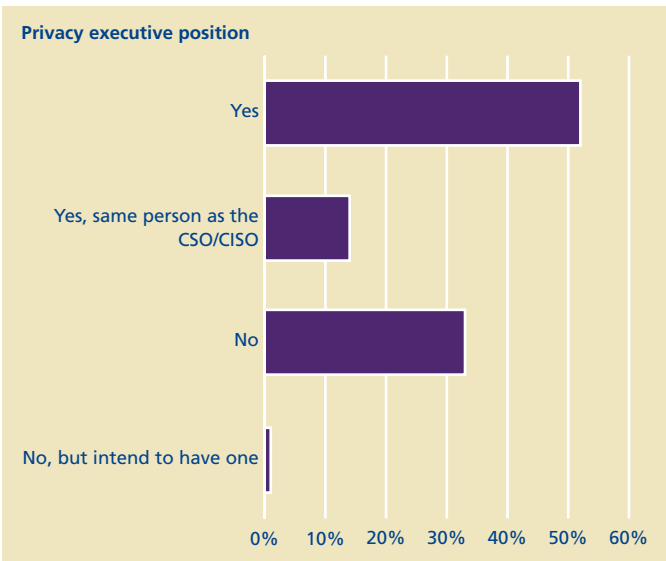
Privacy

Organizations that manage the personal information of individuals find themselves increasingly confronted with the issue of privacy, whether through legislation, industry self-regulation or customer expectations. While some countries are better prepared than others by having an executive in charge and a program established, the most cited priority of 2007 was regulatory compliance, including privacy initiatives.

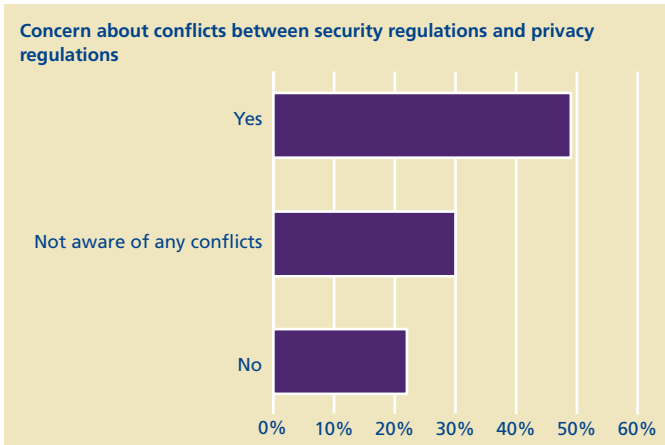
In organizations without a Chief Privacy Officer (CPO), issues such as legislative privacy requirements, privacy compliance requirements, and handling complaints from the public will present strategic and chronic vulnerabilities. It is a positive sign that 66% of respondents have an executive responsible for managing privacy programs in their organizations. In some organizations, it is not uncommon for the Chief Security Officer or the Chief Information Officer to take on a second hat – that of Chief Privacy Officer – once privacy protection becomes an issue.

This year, for 12% of respondents, the CPO is also the CISO. The wisdom of merging the CISO and CPO responsibilities is an issue still open to debate. Traditionally, the CISO tries to optimize organizational control, often from a security perimeter mentality, while the CPO tries to ensure that the individual maintains control and that authorized users do not misuse data. Both perspectives are valid and necessary; combining the roles sometimes means that the privacy perspective is often diminished or rolled into security items before issues are elevated to the attention of the CEO. The resolution of this issue is frequently thwarted by a confusing and troublesome factor: the complex and largely undefined relationship between the disciplines of information security and privacy protection. This year, 49% of respondents indicate that they are concerned with conflicts between security and privacy regulation. Another 30% were not aware of conflicts.

Privacy executive position

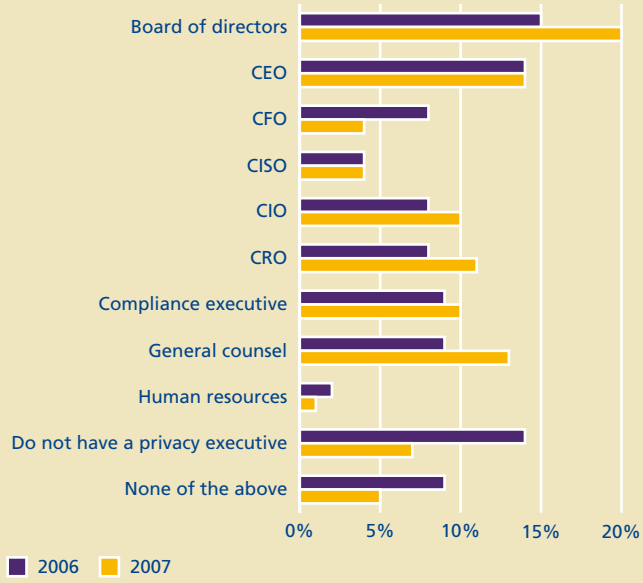


Concern about conflicts between security regulations and privacy regulations



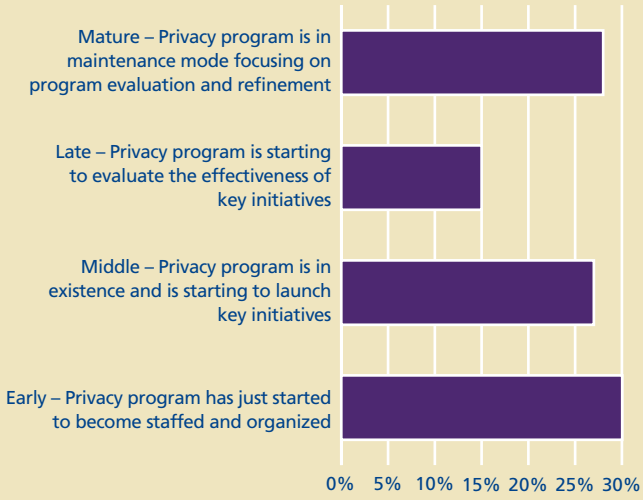
Unlike the reporting relationship of the CISO with its clear line of reporting to the CIO, the privacy executive reporting relationship is not as defined. Only 20% of respondents indicate that the role reports to the board of directors, while another 14% indicate the role reports to the CEO. Outside these two reporting relationships, the reporting structure was split between a compliance executive (10%), general counsel (13%), the CFO (4%), and the CRO (11%).

Levels of reporting – who the privacy executive is reporting to



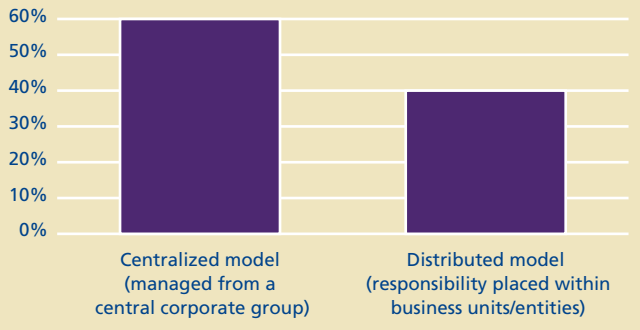
The reality remains that organizations that collect/manage personal information require some kind of program to manage privacy issues. The executive responsible for privacy needs a working knowledge of data collection, data processing, and information management. This year, 70% of respondents indicate that they have a program in place to manage privacy compliance and 37% indicate that their privacy function has been in place for over four years. When the survey examined the maturity of these programs, they found them to be characterized as "early stages", (where the privacy program is just beginning to become staffed and organized – 30%) or as "middle maturity", (where the privacy program exists and has begun to launch key initiatives – 27%), or as "mature stages or maintenance mode" (where the program has progressed enough to be focusing on program evaluation and refinement – 28%), or as "late stages", (where the privacy program's starting to evaluate the effectiveness of key initiatives – 15%).

Development stage of privacy function



The issue of structuring and managing the program varied as much as maturity. While 40% indicate that they have a distributed model (responsibility lies with the business units), 60% indicate that their program is managed from a central corporate group or in a centralized fashion.

Privacy structure

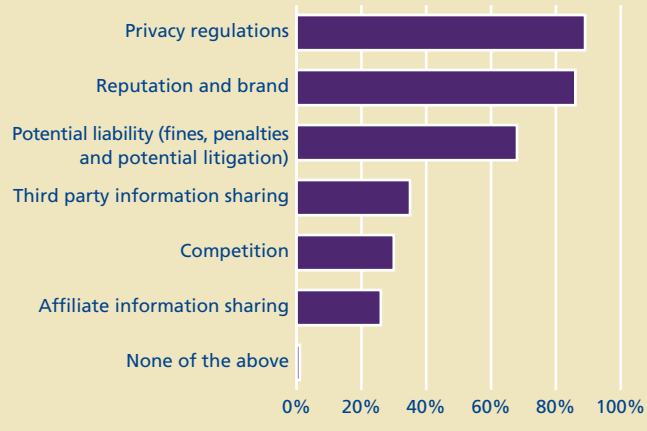


The privacy executive needs to be fully aware of the business strategy and key success drivers of the organization as well as public expectations and legislative context.

The most cited drivers from a privacy perspective include:

- Privacy regulations – 89%.
- Reputation and brand – 86%.
- Potential liability (fines, penalties and potential litigation) – 68%.
- Third party information sharing – 35%.
- Competition – 30%.
- Affiliate information sharing – 26%.

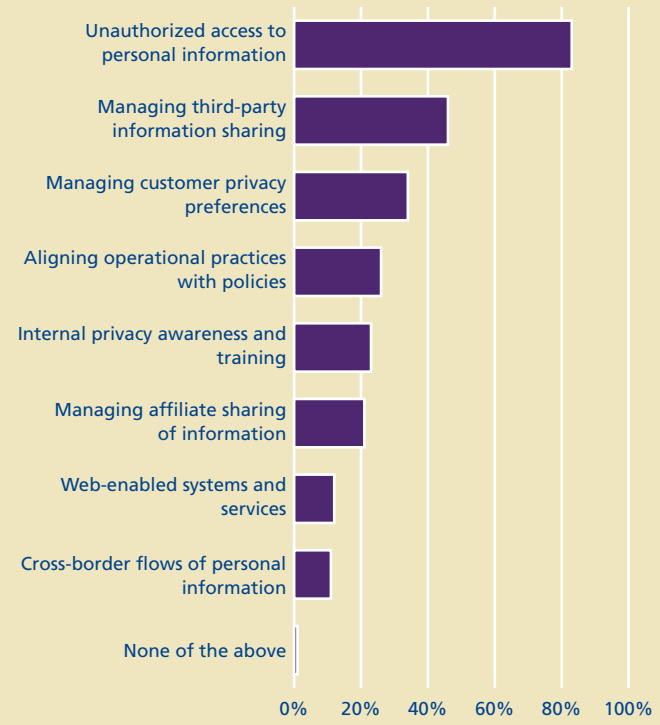
Influential drivers for privacy

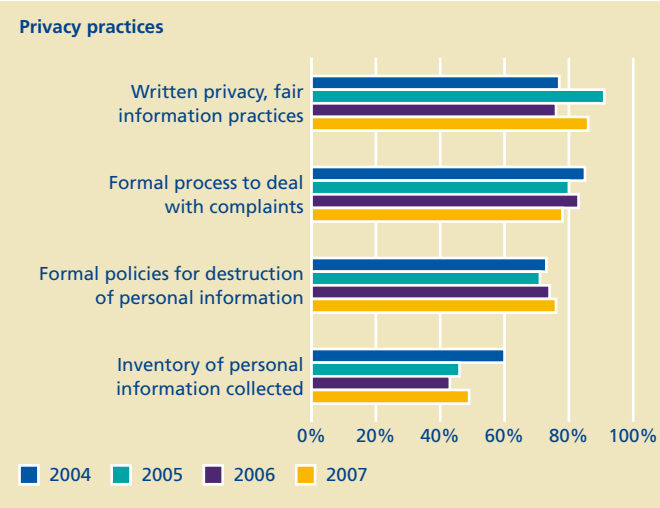


The most cited areas of concern from a privacy perspective include:

- Unauthorized access to personal information – 83% compared to 83% in 2006, 83% in 2005 and 62% in 2004.
- Managing third-party information sharing – 46% compared to 45% in 2006, 33% in 2005 and 45% in 2004.
- Managing customer privacy preferences – 34% compared to 19% in 2006, 25% in 2005 and 30% in 2004.
- Aligning operational practices with policies – 26% compared to 29% in 2006, 30% in 2005 and 19% in 2004.
- Internal privacy awareness and training – 23% compared to 22% in 2006, 22% in 2005 and 29% in 2004.
- Managing affiliate sharing of information – 21%.
- Web – enabled systems and services – 12%.
- Cross – border flows of personal information – 11%.

Areas of concern from privacy perspective





"The survey also identifies which technologies are being implemented to improve security and the value FSIs are gaining from their security and privacy investments."

Respondents indicated that they have the following privacy practices:

- Written privacy, fair information, practices or data collection policies in place – 86% compared to 76% in 2006, 91% in 2005 and 77% in 2004.
- Formal processes in place to deal with complaints about personal information management practices or policies – 78% compared to 83% in 2006, 80% in 2005 and 85% in 2004.
- Formal policies in place with respect to the destruction of personal information – 76% compared to 74% in 2006, 71% in 2005 and 73% in 2004.
- Inventory of personal information collected – 49% compared to 43% in 2006, 46% in 2005 and 60% in 2004.

How DTT's GFSI group designed, implemented and evaluated the survey

The 2007 Global Security Survey for financial institutions reports on the outcome of focused discussions between Deloitte member firms' Security & Privacy Services professionals and Information Technology executives of top global FSIs.

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

Responses of participants relating to the six areas of the questionnaire were subsequently analyzed and consolidated and are presented herein in both qualitative and quantitative formats.

Drafting of the questionnaire

The questionnaire was comprised of questions composed by the global survey team made up of senior Deloitte member firms' Security & Privacy Services professionals. Questions were selected based on their potential to reflect the most important operating dimensions of a financial institution's process 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 fifth 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 cascade around the globe. New questions were also added to reflect topics being asked about by Deloitte member firm clients and being raised by the media.

The collection process

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

Results analysis and validation

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

Once the DeloitteDEX team received the data, it was arranged by geographic origin of respondents. Some basic measures of dispersion were calculated from the data sets. Some answers to specific questions were not used in calculations to keep the analysis simple and straightforward. Not all survey respondents answered all questions; in which case, their responses were excluded from the count only for those particular questions.

Reference from the foreword:
** Sam Levenson, (1911–1980), American humourist, writer, television host and journalist.*

Helpful references and links

Global Information Security Associations

Bank for International Settlements
www.bis.org

Banking Industry Technology Secretariat (BITS)
www.bitsinfo.org

British Standards Institution (BSi): BS7799 – 2:2002
www.bsi-global.com

Business Software Alliance (BSA)
www.bsa.org

Carnegie Mellon University Software Engineering Institute
www.sei.cmu.edu

Defense Information Systems Agency (DISA)
www.disa.mil

Department of Trade and Industry: Information Security
www.dti.gov.uk/industries/information_security/European Commission (EUROPA): Data Protection
http://ec.europa.eu/justice_home/fsi/privacy/

Federal Trade Commission (FTC)
www.ftc.gov

Global Corporate Governance Forum (GCGF)
www.gcgf.org

Information Security Forum (ISF)
www.isfsecuritystandard.com

Information Systems Audit and Control Association
www.isaca.org/

Information Systems Security Association (ISSA)
www.issa.org

International Federation of Accountants
www.ifac.org

International Information Systems Security Certification Consortium (ISC)2
www.isc2.org

International Standards Organization (ISO): ISO 17799 – 2000
www.iso.org

IT Governance Institute (ITGI)
www.itgi.org

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

National Security Agency (NSA)
www.nsa.gov

OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security
www.oecd.org

Systems Administration, Audit and Network Security Institute (SANS)
www.sans.org

VISA International Account Information Security (AIS): Payment Card Industry (PCI) Data Security Standard
http://corporate.visa.com/pd/security/main.jsp

Industry Responses to Identity Theft

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

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

Identity Theft Assistance Center (ITAC)
www.identitytheftassistance.org

Infragard
www.infragard.net

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

Australia's National Computer Emergency Response Team (AusCERT)
www.auscert.org.au

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

Corporate Governance Japan
http://www.rieti.go.jp/cgj/en/index.htm

Japan Computer Emergency Response Team Coordination Center (JPCERT)
http://www.jpcert.or.jp/english/

EMEA
African-Union
www.africa-union.org

Austrian Working Group for Corporate Governance
www.corporate-governance.at

European Corporate Governance Institute (ECGI)
www.ecgi.de/codes

Institute of Chartered Accountants in England and Wales
www.icaew.co.uk

French Business Confederation (MEDEF)
www.medef.fr

CERT-Bund (Germany)
www.bsi.bund.de/certbund

German Accounting Standards Committee
http://www.standardsetter.de/drsc/news/news_eng.php

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

LACRO
Seguridad en Computo
www.seguridad.unam.mx

b:Secure
http://bsecure.com.mx

Grupo de Seguridad de Red CUDI
http://seguridad.internet2.ulsa.mx/

DoDoMex Internet Security Portal
http://www.dodomex.com/

Seguridad en Internet
http://www.e-mexico.gob.mx/wb2/eMex/eMex_Seguridad_en_Internet

Seguridad UMSNH
http://seguridad.umich.mx/North America

North America
North American Electric Reliability Council (NERC)
www.nerc.com

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

Department of Homeland Security (DHS)
www.dhs.gov

Public Company Accounting Oversight Board (PCAOB)
www.pcaobus.org

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

Canada's Computer Emergency Response Team (canCERT)
www.cancert.ca

Canadian Institute of Chartered Accountants (CICA)
www.cica.ca

Acknowledgements

We wish to thank all of the professionals of the financial institutions who responded to the 2007 DTT GFSI Group Security 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. The DTT GFSI Group extend its heartfelt thanks for the time and effort that respondents devoted to this project.

Survey development team

Authors

Adel Melek
+1 416 601 6524
amelek@deloitte.ca

Marc MacKinnon
+1 416 601 5993
mmackinnon@deloitte.ca

Prasad Kantamneni
+1 615 718 5981
pkantamneni@deloitte.com

Data analysis and editing

Clare Galloway
+1 416 601 6357
clgalloway@deloitte.ca

Sreehari Gangisett
+1 615 718 5696
sgangisetty@deloitte.com

Methodology and survey development

DeloitteDEX:
Olivier Curet
+1 216 589 5448
ocuret@deloitte.com

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

Marketing support

Chris Patterson
+1 212 436 2779
chrpatterson@deloitte.com

Sephron Da Silva
+1 416 874 4336
sdasilva@deloitte.ca

Contributors

The following individuals made significant contributions to the development of this publication:

Mike Bronson
Glen Bruce
Elizabeth Callahan
James Chung
Ross Couldrey
Mark Fernandes
Nick Galletto
Kaan Gunay
Simon Ho
Adam Jolicoeur
Michael Hortobagyi
Reza Kopaee
Richard Maurice
Ryan Li
Donald Mccoll
Oliver Ng
Jonquil Peel
Daniel Poliquin
Steve Rampado

Contacts

Jack Ribeiro
Managing Partner
Global Financial Services
Industry (GFSI) Practice
United States
Deloitte & Touche LLP
+1 212 436 2573
jribeiro@deloitte.com

Leon Bloom
Deputy Managing Partner
Global Financial Services
Industry (GFSI) Practice
Canada
Deloitte & Touche
+1 416 601 6244
lebloom@deloitte.ca

Adel Melek
Partner, Global Leader IT Risk
Management & Security Services
Global Financial Services
Industry (GFSI) Practice
Canada
Deloitte & Touche LLP
+1 416 601 6524
amelek@deloitte.ca

Mark Layton
Global Enterprise Risk Leader
United States
Deloitte & Touche LLP
+1 214 840 7979
mlayton@deloitte.com

Regional leaders

Adel Melek	Canada – Toronto	Deloitte & Touche LLP	+1 416 601 6524	amelek@deloitte.ca
Christopher Lee	USA – San Jose	Deloitte & Touche LLP	+1 408 704 4314	chrislee@deloitte.com
Simon Owen	EMEA – London, UK	Deloitte & Touche LLP UK	+44 20 7303 7219	sxowen@deloitte.co.uk
Uantchern Loh	APAC – Kuala Lumpur, Malaysia	Deloitte KassimChan	+65 6216 3282	uloh@deloitte.com
Bruce Daly	Japan – Tokyo, Japan	Deloitte Touche Tohmatsu	+81 (3) 4218 7284	brdaly@deloitte.com

Contacts

APAC
Abhay Gupte
Mumbai, India
Deloitte Touche Tohmatsu India Pvt Ltd.
+91 22 5667 9405
agupte@deloitte.com

Danny Lau
Hong Kong
Deloitte Touche Tohmatsu
+852 2852 1015
danlau@deloitte.com.hk

Julie Priest
Sydney, Australia
Deloitte Touche Tohmatsu
+61 2 9322 7171
jpriest@deloitte.com.au

Canada
Marcel Labelle
Montreal, Canada
Deloitte & Touche LLP
+1 514 393 5472
marlabelle@deloitte.ca

Donald McColl
Toronto, Canada
Deloitte & Touche LLP
+1 416 601 6373
dmccoll@deloitte.ca

CIS
Valery Zaichenko
Moscow, Russia
Deloitte Touche Tohmatsu
+7 495 787 0600
vzaichenko@deloitte.ru

Wayne Brandt
Moscow, Russia
Deloitte Touche Tohmatsu
+7 495 787 0600
wbrandt@deloitte.ru

EMEA
Carlo Schupp
Brussels, Belgium
Deloitte & Touche
+32 32 2 800 20 77
cschupp@deloitte.com

Francois Renault
Paris, France
Deloitte Conseil
+33 1 55 61 61 22
frenault@deloitte.fr

Sven Hesselbach
Frankfurt, Germany
Deloitte & Touche GmbH
+49 69 75695 6449
shesselbach@deloitte.de

Ed Van Essen
Amsterdam, Netherlands
Deloitte Touche Tohmatsu
+31 (0) 20 4547606
evanessen@deloitte.nl

Kris Budnik
Johannesburg, South Africa
Deloitte Touche Tohmatsu
+27 (0) 11 806 5224
kbudnick@deloitte.co.za

Luis Carro
Madrid, Spain
Deloitte Touche Tohmatsu
+34 91 514 50 00
lcarro@deloitte.es

Mark Carter
Zurich, Switzerland
Deloitte AG
+41 44 421 6289
markjcarter@deloitte.ch

Mike Maddison
London, UK
Deloitte & Touche LLP UK
+44 20 7303 0017
mmaddison@deloitte.co.uk

LACRO
Robson Calil Chaar
Sau Paulo, Brazil
Deloitte Touche Tohmatsu
+ 55 11 5186 6209
rchaar@deloitte.com

USA
Kim Altern
New York, USA
Deloitte & Touche LLP
+212 436 3634
kaltern@deloitte.com

John Clark
Chicago, USA
Deloitte & Touche LLP
+1 312 486 3985
johclark@deloitte.com

Kenneth DeJarnette
San Francisco, USA
Deloitte & Touche LLP
+1 415 783 4316
kdejarnette@deloitte.com

Ted DeZabala
New York, USA
Deloitte & Touche LLP
+1 212 436 2957
tdezabala@deloitte.com

Rich Baich
Charlotte, USA
Deloitte & Touche LLP
+1 704 887 1563
jbaich@deloitte.com

For more information on the Global Security Survey, please contact your local DTT or Deloitte member firm professional listed on the inside back cover of this publication.

Disclaimer
The information contained herein is provided by Deloitte Touche Tohmatsu and is intended to provide general information on a particular subject or subjects and is not an exhaustive treatment of such subject(s). Accordingly, the information is not intended to constitute accounting, tax, legal, investment, consulting or other professional advice or services. The information is not intended to be relied upon as the sole basis for any decision which may affect you or your business. Before making any decision or taking any action that might affect your personal finances or business, you should consult a qualified professional adviser.

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

The information is provided as is, and Deloitte Touche Tohmatsu makes no express or implied representations or warranties regarding the information. Without limiting the foregoing, Deloitte Touche Tohmatsu does not warrant that the information will be error-free or will meet any particular criteria of performance or quality. Deloitte Touche Tohmatsu expressly disclaims all implied warranties, including, without limitation, warranties of merchantability, title, fitness for a particular purpose, non-infringement, compatibility, security, and accuracy.

Your use of the information is at your own risk and you assume full responsibility and risk of loss resulting from the use thereof. Deloitte Touche Tohmatsu will not be liable for any direct, indirect, special, incidental, consequential, or punitive damages or any other damages whatsoever, whether in an action of contract, statute, tort (including, without limitation, negligence), or otherwise, relating to the use of the information.

If any of the foregoing is not fully enforceable for any reason, the remainder shall nonetheless continue to apply.

About Deloitte
Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, its member firms, and their respective subsidiaries and affiliates. Deloitte Touche Tohmatsu is an organization of member firms around the world devoted to excellence in providing professional services and advice, focused on client service through a global strategy executed locally in nearly 140 countries. With access to the deep intellectual capital of approximately 150,000 people worldwide, Deloitte delivers services in four professional areas – audit, tax, consulting, and financial advisory services – and serves more than 80 percent of the world's largest companies, as well as large national enterprises, public institutions, locally important clients, and successful, fast-growing global companies. Services are not provided by the Deloitte Touche Tohmatsu Verein, and, for regulatory and other reasons, certain member firms do not provide services in all four professional areas.

As a Swiss Verein (association), 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.

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

Item # 7182

Deloitte
Touche
Tohmatsu