

Deloitte.

Global Financial Services Industry

2006 Global Security Survey



Audit • Tax • Consulting • Financial Advisory •

Contents

Objective of the survey	4
How DTT's GFSI group designed, implemented and evaluated the survey	5
Who responded	7
Geographic segmentation observations	9
Key findings of the survey	13
Governance	19
Investment in security	24
Risk	26
Use of security technology	30
Quality of operations	33
Privacy	37
Helpful references and links	40
Acknowledgements	42
Survey development team	42

Foreword

It was the Greek dramatist Euripides, born in 480BC, who said, "Along with success comes a reputation for wisdom." With the Deloitte Touche Tohmatsu (DTT) Global Financial Services Industry (GFSI) group's fourth annual security survey, GFSI finds these words borne out. As our survey enjoys an ever-growing number of downloads and media mentions, DTT's GFSI group continues to build its reputation for first-class security knowledge and services. This result is most gratifying – and a fitting tribute to the tireless groundwork that the survey team has laid over the years.

It is particularly satisfying to note that the top priorities of survey respondents are indeed the hot topics of the industry, validating DTT GFSI group's choice of participants for this survey and illustrating, once again, that if you want to find the pulse of any industry, you go to those on the front lines.

It will come as no surprise to anyone that, according to the survey identity theft is this year's number two IT security hot button. What may come as a revelation, however, is the disturbing trend behind this topic. It seems that "big business" has moved into a domain once dominated by young, one-off hackers, operating out of their homes after school.

As annoying and illegal as these "script kiddies" were, there is now an organized, more sinister, high-stakes approach, one that necessitates a more costly and focused, effort to fight back successfully.

It has often been said that people are an organization's most valuable asset. It appears that, in the world of security breaches, they are now its most vulnerable. As an organization's fortresses continue to be strengthened against brute force attacks, criminals get smarter, waging their psychological war of deception and fraud on employees and customers through ever-evolving schemes of phishing, pharming, and spyware technologies.

Although many of the top priorities reflected in the survey this year are predictable, some are not. Even those of us in the industry who think they have seen it all are capable of having their eyes opened from time to time. I promise that this fourth annual security survey will be a compelling and thought-provoking read.

Once again, I extend my heartfelt thanks to the Chief Information Security Officers, their designates, and the security management teams from financial services industry organizations around the world, for your participation in this survey – and to the growing numbers of you who continue to join the ranks of survey participants every year. I thank you for your time and effort and for the truthful, candid information that you provide, information that is unvarnished by politics, budgets, and organizational cultures, information that allows the DTT GFSI group to present the IT security world as it really is.

Armed with information of this calibre – and by taking the appropriate action – we will pose a formidable challenge to those who would attempt to profit by undermining the bedrock of our capital markets system.



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



Objective of the survey

The goal of the 2006 Global Security Survey is to help respondents assess the state of information security within their organization relative to other comparable financial institutions around the world. Overall, the survey attempts to answer the question: **How does the information security of my organization compare to that of my counterparts?** By comparing the 2006 data with that collected for the 2003, 2004 and 2005 surveys, DTT's GFSI group can begin to determine differences and similarities, identify trends and gain an ability to ponder more 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 2003, 2004 and 2005 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.

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

The 2006 Global Security Survey reports on the outcome of focused discussions between Deloitte member firm Security and Privacy Services professionals and Information Technology (IT) executives of top global financial services institutions (FSIs).

Discussions with representatives of these organizations were designed to identify, record, and present the state of the practice of information security in the financial services industry with a particular emphasis on identifying levels of perceived risks, the types of risks with which FSIs are concerned and the resources being used to mitigate these risks. The survey also identifies which technologies are being implemented to improve security and the value FSIs are gaining from their security and privacy investments. To fulfill this objective, senior members of Deloitte member firms' Security & Privacy Services Practice 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.

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

Drafting of the questionnaire

The questionnaire was comprised of questions composed by the DTT GFSI group's survey team made up of senior Deloitte member firm 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 were to identify, record, and present the state of information security and privacy in the financial services industry. As this is the fourth 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 firms' clients and 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. Each participating region assigned responsibility to senior members of their Security & Privacy Services practice and those member firm 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. For the second consecutive year, DTT GFSI's group offered pre-selected financial institutions the ability to submit answers online using an online questionnaire managed by DeloitteDEX.

Results analysis and validation

DeloitteDEX is a DTT family of proprietary products and processes for diagnostic benchmarking applications. The DeloitteDEX US team from Deloitte & Touche LLP was responsible for analyzing and validating the data from the study. The team used a variety of research tools and information databases to provide analyses measuring financial and/or operational performance. Some basic measures of dispersion were calculated from the data sets and a resulting subset of acceptable questions and answers were incorporated into this report.

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

Benchmarking within 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.

The value of benchmarking

Financial services providers, now more than ever, recognize the importance of performance measurements and benchmarks in helping them manage complex systems and processes. The Global Security Survey is intended to enable benchmarking against comparable organizations. Benchmarking within 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, the DTT GFSI group chose to group 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, Encryption, Software Licensing.
- **Use of security technologies**
 - Technology, Knowledge Base, Trends.
- **Quality of operations**
 - Business Continuity Management, Benchmarking, Administration, Detection, Response, Privileged Users, Authentication, Controls.
- **Privacy**
 - Compliance, Ethics, Data Collection Policies, Communication Techniques, Safeguards, Personal Information Protection.

Who responded

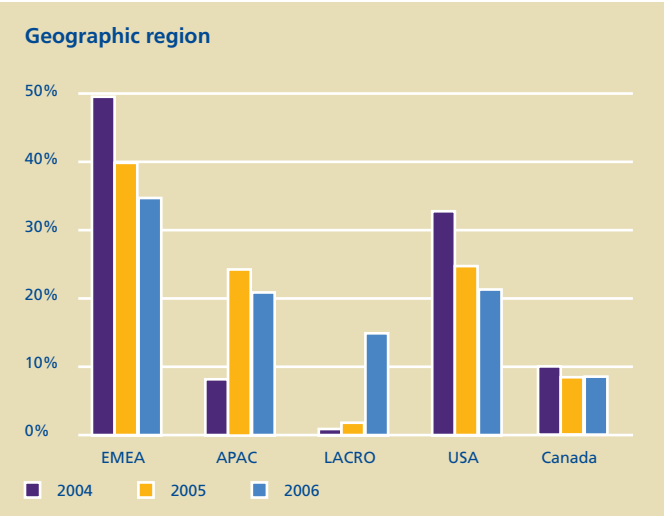
The 2006 Global Security Survey respondent data reflects current trends in security and privacy at a number of major global financial institutions. The final survey sample reflects all major financial sectors (banking, insurance, securities, payments and processors and diversified financial institutions). DTT GFSI group agreed to preserve the anonymity of the participants by not identifying their organizations. However, overall, the participants represent:

- 31% of the top 100 global financial institutions (market value).
- 34% of the top 100 global banks (2005 tier one capital).
- 16% of the top 50 global insurance companies (market value).

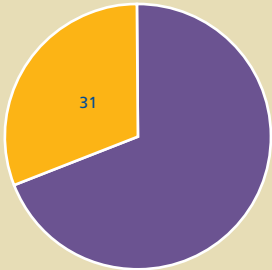
Geographic region

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

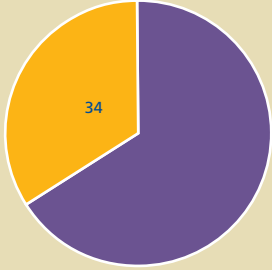
- Europe, the Middle East and Africa: 35%;
- Asia/Pacific: 21%;
- Latin America and the Caribbean: 15%; and
- North America: 29%.



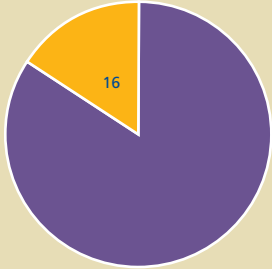
Top 100 global institutions (market value)



Top 100 global banks (2005 tier one capital)



Top 50 global insurance companies (market value)



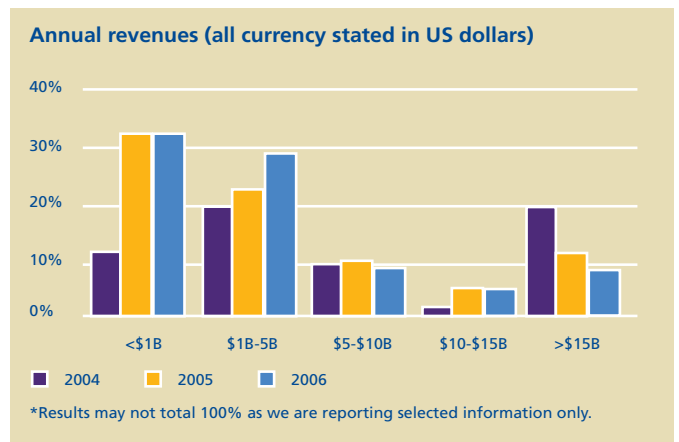
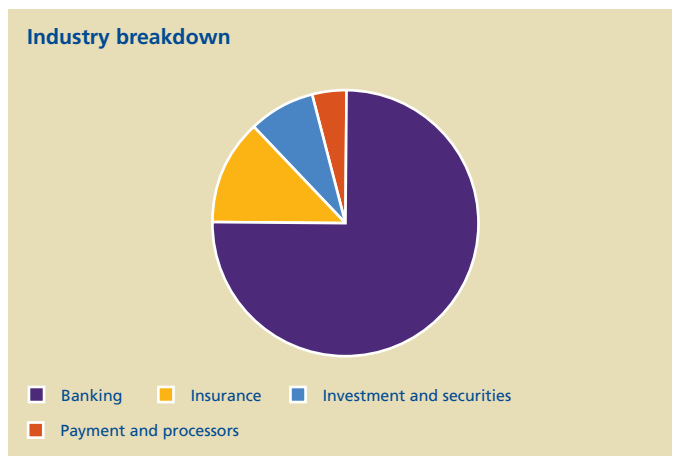
Industry breakdown

- Banking: 74%;
- Insurance: 14%;
- Investment and Securities: 8%; and
- Payment and processors: 4%.

Annual revenue

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

- <1B in annual revenue: 33%;
- \$1B-\$5B in annual revenue: 29%;
- \$5B-\$10B in annual revenue: 9%;
- \$10B-\$15B in annual revenue: 6%; and
- Greater than \$15B in annual revenue: 9%.



Geographic segmentation observations

Regional highlight	APAC (not including Japan)						
	EMEA	Japan	USA	Canada	LACRO	Global	
FSIs who have a Chief Information Security Officer (CISO)	91%	23%	74%	82%	80%	57%	75%
FSIs who feel that security has risen to the C suite or board as a critical area of business	44%	15%	56%	59%	64%	43%	47%
FSIs whose board has a clear view on the organization's major security investments from a risk and return point of view	47%	60%	85%	38%	50%	67%	53%
FSIs possessing a security strategy	64%	33%	93%	74%	36%	57%	63%
FSIs whose information security strategy is led and embraced by line and functional business leaders	67%	42%	100%	71%	75%	55%	66%
FSIs who feel they presently have both the required skills and competencies to respond effectively and efficiently	41%	0%	31%	41%	64%	32%	37%
FSIs who have security linked to their IT security employee's appraisals	43%	58%	55%	58%	55%	36%	49%
FSIs whose employees have received at least one training and awareness session on security and privacy in the last 12 months	45%	82%	90%	74%	55%	61%	63%
FSIs who feel they have both commitment and funding to address regulatory requirements	80%	62%	76%	70%	91%	90%	78%
FSIs who feel that government driven security regulations are effective in improving security posture in their industry	70%	91%	100%	76%	73%	80%	78%
FSIs who have an enterprise wide business continuity management program	88%	92%	71%	100%	100%	67%	88%
FSIs who have an executive responsible for privacy	72%	83%	100%	79%	100%	26%	74%
FSIs who have a program for managing privacy compliance	56%	85%	100%	84%	100%	25%	70%
FSIs who have experienced a breach in the last 12 months	85%	100%	32%	91%	100%	85%	82%

■ Best in class ■ Worst in class

Europe, Middle East, and Africa (EMEA)

In many instances, the issues surrounding security are dependent on a region's economic conditions. While economic downturn has affected countries within the EMEA region, the focus on security, has held steady. With the ever-present threat of terrorism, a stringent crackdown on crime by the government and increased

awareness of security issues have provided growth in this area. This year, EMEA respondents indicated that the "increasing sophistication of threats" was the number one challenge facing them (56%) while budget restraints and lack of resources (39%) and emerging technologies (37%) rounded out the top three threats they will likely encounter over the next twelve months.

When compared to last year, EMEA held steady in most areas. A key area of improvement is the increased number of respondents that now have a CISO in place in the organization (91%). Perhaps because of this, 44% of respondents indicate that the issue of security and privacy has been raised to the C-suite as a critical area of concern.

For the second consecutive year, EMEA is in last place when it comes to providing their employees awareness and education sessions in the topics of security and privacy (45%). Only 41% of respondents feel that they have both the required skills and competencies to respond effectively and efficiently to ongoing security concerns within their organizations and only 43% indicate that they have security linked to the appraisals of IT security professionals. As in most regions, the number of respondents who report having undergone the process of formulating an information security strategy is low 64% and, only 67% feel that the strategy is led and embraced by the line and functional business leaders.

With the British government using face recognition cameras installed in public places and biometric identification as a high tech means of monitoring people's movements, it was interesting to note that EMEA respondents were slightly behind those from the LACRO region as the second highest group to characterize themselves as "early adopters" of technologies (11%). The majority (57%) felt that they were "effective users of demonstrated technologies".

Asia Pacific (APAC) (not including Japan)

While Japanese respondents are top of their class in most categories, the rest of APAC is at the other end of the spectrum, with the lowest level of responses in six categories. Only 23% of APAC respondents have a CISO, which may help to explain why they did not do well in many other categories. Only 15% of APAC respondents indicate that security has risen to the C-suite or board as a critical area of business and only 33% have formulated an information security strategy. Forty-two per cent feel that the strategy is led and embraced by line and functional business leaders. It is not surprising that lack of management support is rated the fourth highest (38%) challenge for APAC respondents.

Given this lack of leadership and executive support, only 62% of APAC respondents feel that they have the commitment and support to adequately address regulatory requirements, not a promising finding since privacy issues and concerns are a major challenge affecting APAC respondents (31%). On the positive side, 83% of APAC respondents have an executive in place responsible for privacy and 85% have a privacy program.

While APAC respondents indicate that they have neither the required skills nor the competencies to effectively and efficiently respond (0%), they have attempted to compensate by offering security and privacy training programs (82%) and by holding their people accountable, with security linked to their IT security staff's performance appraisals (58%).

Japan

Japanese respondents came out on top this year, taking the lead in eight different categories. While only 74% of respondents indicate that they have a CISO, 93% report that not only have they formulated an information security strategy, but 100% of those feel that it is led and embraced by line and functional business leaders.

With a finding of only 31% having both the required skills and competencies to respond effectively and efficiently, Japan has attempted to compensate for this with security and privacy training and awareness sessions – 90% of respondents held such sessions for their employees in the last year. These measures may already have proven successful – Japan has the lowest number of reported breaches (32%).

Japanese respondents indicate that their primary future challenge is that of privacy issues and concerns (70%), which might explain why Japan tied with Canada for first place in the number of respondents who had an executive for privacy in place (100%) and for those who have a program for managing privacy compliance (100%).

Japanese respondents indicate that their secondary challenge is inadequate functionality/ interoperability of security products (45%), a finding which may explain why Japan respondents are the most risk adverse, with 0% classifying themselves as early adopters of technology and 76% indicating that they are effective and efficient users.

Japanese respondents are also ahead when it comes to their privacy practices. Tied with Canadian respondents at 100%. Japanese respondents have an executive responsible for privacy and a program established managing privacy compliance.

United States of America (USA)

Natural disasters, led by the infamous Hurricane Katrina, wreaked havoc on the country, resulting in the loss of hundreds of lives and property damage of over a hundred billion dollars. The aftermath of tragedy is the ultimate educator – for the first time, the US tied with Canada for top spot in the number of respondents who claim to have an enterprise wide business continuity program (100%).

The US government has developed disaster management initiatives to deal with natural calamities. However, it is interesting to note that, despite the high-profile attention that this issue gets, US respondents are at the lower end of the spectrum among those who feel that they have the required funding and commitment to address regulatory concerns affecting them (70%). US respondents are also still on the lower end of the spectrum yet are relatively optimistic about government security regulations; 76% feel that government-driven security regulations are effective in improving security within their industry. This year, 74% of US respondents have undergone the process of formulating an information security strategy, roughly 38% greater than their northern neighbors.

As DTT's GFSI group know, a security strategy is only as good as it is perceived to be by stakeholders. Only 71% of respondents who have an information security strategy feel that it is getting the buy-in required. This finding may help to explain why the US falls near the middle of the pack when it comes to those who believe that information security is getting the attention of the C-suite. A middle-of-the-road 59% of this year's respondents feel that security has risen to the C-suite as a critical component of their business.

This year, US respondents indicate that their top threats include privacy issues and concerns (62%), increasing sophistication of attacks (59%) and emerging technologies (47%). The latter is an interesting finding, given that respondents rate themselves (3%) just above the risk-adverse Japanese as "Early adopters of technology". With regard to privacy issues and concerns, it was positive to see that 79% of US respondents have an executive responsible for privacy and 84% already have some form of program in place for managing privacy compliance.

Canada

With high-profile incidents in the news in 2005, Canada witnessed some much-needed transformation in the area of security and privacy. Notwithstanding, Canadian respondents still experienced the highest number of breaches in 2005 (100%). A surprising result is that although respondents have been under scrutiny due to the number of insider breaches (intentional or unintentional), only 64% feel that they have both the required skills and competencies and only 55% indicate that their employees received some form of training and awareness on security and privacy in the last twelve months.

When compared to other regions, respondents from Canada were top of the class in six of the categories. A surprising finding is a drop in the number of respondents who feel that they have an information security strategy (down from 70% in 2005 to 36% in 2006). Respondents rated this issue as third in importance (36%) of

the challenges they were facing in 2005. The positive news is that of the 36% who have a strategy in place, 75% feel that it is led and embraced by the line and functional business leaders. On the issue of ongoing regulation, it is positive to note that 91% of respondents have both the commitment and funding required to adequately address regulatory requirements. However, similar to findings in the US, only 73% of respondents feel that government-driven security regulations are effective in improving security in their industry. Respondents in Canada also tie for first place for the number of organizations who have an executive responsible for privacy (100%), those who indicate they have a CISO (80%) and those who have a program in place for managing business continuity management (100%) and privacy compliance (100%).

Latin America and the Caribbean (LACRO)

Increasing sophistication of threats (57%), budget constraints and lack of resources (39%) and emerging technologies (35%) are the top three challenges LACRO respondents face in today's complex and uncertain operating environment.

For the second year, LACRO respondents do not appear overly concerned with the issue of privacy. Although only 26% indicate that they have a privacy executive in place (compared to 57% who have a CISO) and only 25% indicate that they have any form of privacy program, the issue of privacy is not even one of the five challenges that LACRO respondents feel they face this year. Only 57% of respondents indicate that they have an information security strategy, an issue that is rated as number five in their top five challenges going forward (30%).

In 2006, LACRO respondents have been hard hit in terms of those who have experienced and reported a breach over the last twelve months rose to 85% from 0% in 2005. There is a startling difference between the 2005 percentage and the 2006 finding. The sharp rise in 2006 may be due to the fact that LACRO respondents did not have the tools and practices in place to detect whether they were being breached or not in 2005. The 2006 number may be explainable, in part, by the fact that only 32% of respondents feel that they have the required skills and competencies to respond effectively and efficiently and only 36% have attempted to link security to the appraisals of their IT staff.

With a lack of qualified staff, (a "bottom-of-the-pack" rating of 67%), the absence of a business continuity management program and emerging technologies as their top three challenges, it was interesting to note that LACRO respondents feel that they are leaders in adopting new technologies (15%) and as well as leaders in being late adopters of technology (30%).



Key findings of the survey

1. Sophistication of attacks and proliferation of vulnerabilities continues to dominate attention

The globalized environment in which financial institutions now operate brings with it a whole new set of challenges, challenges that push risk – from physical to fiscal – to the top of corporate agendas. This last year brought new and unique challenges to those responsible for their organization's security.

There continues to be an exponential increase in the sophistication of threats and their potential impact across an organization. When asked to rate the intensity of perceived threats over the next twelve months, 53% of respondents chose phishing and pharming while 51% chose viruses, spyware, trojans and worms. While internal threats continue to rise over previous years (employee misconduct – 20%, internal financial fraud – 19%) organizations appear to be more concerned with threats from the outside, since, in their minds, they bring a higher degree of publicity and damage to reputation.

Details of breaches publicized last year would suggest that financially motivated, targeted attacks are increasing and the criminal profile is shifting – from script kiddies and disorganized hackers to well funded organized crime rings, whose around-the-clock, across-the-globe attacks are yielding big financial payback. This trend clearly highlights that random acts of vandalism (such as the web page defacements experienced by 4% of respondents) have been replaced by purposeful, targeted acts of criminal activity (such as the successful phishing attacks experienced by 51% of respondents). The attackers are transitioning from mass virus and worm attacks to attract attention and publicity to stealthier methods to avoid detection. Illustrating the premise of Newton's third law – for every action, there is an equal and opposite reaction – organizations are now focused on ways to combat identity theft and account fraud.

As threats to financial institutions widen from technical and infrastructure threats to those affecting applications, data and people, organizations and their respective security functions necessarily evolve from IT-centric to business-centric. Robust perimeter security technology has been successful at limiting the external visibility of internal IT resources to those with only legitimate and authorized access. While the costs incurred to manage most security incidents continue to decline, the costs to manage incidents that target sensitive information continue to rise. Malicious outsiders are targeting organizations' computer systems through direct connections and unauthorized access. By taking advantage of software flaws or errors in configuration, outsiders are now able to bypass access controls to directly access applications

and data. Although it is now more difficult to get at resources using external brute force attacks, it is becoming easier to get at these same resources by exploiting social engineering attacks against the organization's people (e.g. phishing/pharming). Internal targeted attacks whereby authorized users are abusing their privileges are also on the rise. A good example is those who have access to a variety of data sources and accounts within a financial institution who attempt to account surf out of a perverse interest of well known people's financial information (e.g. politicians, professional athletes and movie stars) as opposed to normal business activity.

A significant emerging risk is one that concerns security controls applied to information assets that leave the internal environment. For obvious reasons, they are harder to control and account for. The best example of this problem is the boom in mobile and wireless technology, which puts huge pressure on an organization to try to protect users' information. Security controls have not kept pace with the proliferation of mobile technology and controls to mitigate risk are often perceived as a nuisance factor that interferes with productivity. In the future, many organizations will likely look at various encryption solutions as well as multi-factor authentication technologies for accessing information and logging onto corporate networks. The traditional approach to security – a focus on infrastructure and technical components – will likely be far less effective in the face of this technology boom. Information security controls must flow with the data and not stop at the environment's perimeter.

Looking ahead, pragmatic organizations that have the potential to be targets of choice should prepare themselves for targeted, financially motivated attacks and combine end-user and information-centric approaches by ensuring that information is protected in accordance with its value. Through the development and implementation of meaningful data classification schemes that recognize that data value changes over time and across contexts and by creating the required audit trails to allow for the reconstruction of a transaction, organizations will likely be better prepared for, and be able to help minimize the business impact of a broader range of threats.

2. Identity theft – the crime of the 21st Century

Identity theft is emerging as one of the crimes of the 21st century. It involves the deliberate stealing of another person's identifying information for criminal purposes. According to this year's survey, identity theft and account fraud are two priorities that Financial Institutions (FI) (58%) will likely be focusing on this year. To battle these ever-increasing threats, FIs around the globe will be looking

to identify and implement solutions in the areas of data privacy and information management.

The rash of high-profile data security breaches in 2005, supported by the survey respondents' admissions that 18% of them have experienced some form of data leakage, has exposed deeply rooted and long-term problems in the way FIs have been managing their sensitive customer data. Identity theft is typically associated with credit card and mail fraud. But new methods, such as spear-phishing (targeted and convincing email attacks) are constantly emerging. High-tech versions include the use of phishing and pharming (persuading people to disclose sensitive information through phony emails and web sites), malicious spyware and hacking to obtain information. Organizations also have to recognize that identity theft is not just about the technology. Low-tech forms consist of laptop, mobile device theft or social engineering techniques, such as posing as a call-centre employee or sending a fake email to obtain personal identifying information. Often the security of information is compromised by human behavior, whereby the individuals who have been entrusted with managing personal information lack adequate security qualifications, leading to an increase in release of confidential, personal identification information. Organizations that are custodians of information are struggling with how they can do a better job of securing and protecting what many would refer to as the "crown jewels" of an organization. Although some organizations have made great strides, particularly in areas such as showing consumers how to protect themselves, many fall far short in other areas, such as revoking access on a timely basis so that former employees and contractors are unable to access and abuse sensitive information.

Information security is all about protecting data from unauthorized access and unauthorized use. Effective access controls require strong enterprise identity management techniques, so it is encouraging to note that identity management was another of the respondents' top five priorities for 2006 (41%). Identity management and access control are clearly issues that are slowly making their way to the forefront of respondents' priorities, with 55% indicating that they have a fully deployed identity management solution, and another 30% piloting or planning to deploy one over the next 18 months. Whether they call it identity management or access control, these organizations are seeking a comprehensive framework that offers a robust solution to help provide simplified, automated and auditable controls over users' identities.

Over the past eighteen months, incidents involving theft and misuse of corporate information assets have captured headlines

involving mass customer database breaches to the loss of data tapes containing customer personal data. With organizations looking to all types of responses and technologies, such as encryption, to help prevent data security breaches, it is useful to remember that identity theft is not just about the technology. If organizations fail to properly implement their technology or if it is out of date, these technologies may end up increasing organizations' costs and failing to improve security. Looking to the future, those organizations who do not execute effective data security strategies will continue to struggle with the consequences of the proliferation of unstructured data and weak access controls.

Pragmatic organizations will embrace, and benefit from, the insight that data privacy can bring to organizational security. With enhanced security, operations and infrastructure, organizations can improve service delivery, strengthen consumer trust and increase their competitive advantage.

3. Planning for the unimaginable

Despite the steady proliferation of computer network viruses and attacks, it was likely the 9/11 attacks, followed by high-profile natural disasters, ranging from the Asian tsunami in 2004 to the earthquake that devastated Pakistan in 2005, that brought the concept of Business Continuity Management (BCM) to the forefront. Even the best run FIs are realizing that they were not fully prepared for a disaster or business interruption. This year, survey respondents reported hardware and software failures as the number one cause of downtime for critical business systems (70%). The ability to continue to function after a major disruption is essential for all organizations – and doubly so for those whose services include providing real-time financial information to their customers.

For the first year in the history of this survey, disaster recovery business continuity management is one of the top five priorities for respondents (49%). Even though only 24% of respondents indicate that some form of cost of continuity services has been included as part of the information security budget, it is clear that the information security function is now a key role within the organization. Survey respondents identify viruses (9%), human error (43%) and malicious acts (3%), as some of the causes of serious business interruption that they have experienced.

BCM involves a series of processes that need to be followed in the event of an emergency, governing everything from the safety of personnel to the security of essential information. This year, 12% of respondents indicate that they do not yet have a BCM plan.

While 81% of respondents indicate that they have enterprise-wide business continuity management programs, closer examination reveals that these programs may not be addressed at the enterprise level nor is the organization as prepared as it may think. A timely example of organizations' lack of readiness and resiliency is the absence of programs to address the expected avian flu pandemic. An outbreak of the flu pandemic anywhere in the world would potentially cripple supply chains, dramatically reduce available labor pools, and greatly diminish trading partner and business ability to meet scheduled obligations. However, this year's survey indicates that only 54% of respondents take into account dependencies on third parties, such as vendors and suppliers, and only 67% have plans that cover the loss of personnel.

As enterprises become more diverse and more reliant on factors outside their direct control, they expose themselves to interdependence risks, where an event potentially even at a remote location may quickly grow into a company/industry-threatening situation. External reliance outside the corporate boundaries translates to increasing vulnerabilities and new responsibilities. As a result of this trend, there are now extensive interdependencies across industries, nations, communications and trade practices that are neither well understood nor accounted for in scenario planning and risk management practices. As the level and frequency of threats, such as information warfare increase, organizations must better prepare themselves from a possible crippling of infrastructure, such as telecommunications, transportation, power grids etc.

As circumstances change, so too must the nomenclature. The way in which organizations have traditionally defined risk may not be applicable in today's operating environment. Organizations need to continually evolve, adopting a broader understanding of, and more comprehensive process for, managing risk across the extended enterprise and network of alliances. While BCM plans do not necessarily need to be addressed at the board level, the board should understand what risks the organization may be exposed to (imaginable and unimaginable).

Only then, would they be in a position to identify the risks, define the interdependencies and develop plans to prepare for events that might jeopardize revenue drivers.

In the future, in order to protect what is core business survival, organizations should continually adjust and align their strategy, their operations, their governance structure and the way in which they make decisions so that they can be proactive in identifying, and quickly adjusting to, constantly changing risks.

4. Phishing and pharming lead to Government intervention

The sophistication of the attacks on today's web applications continues to increase. The threat that respondents most anticipated over the coming year was phishing/pharming (53%), a finding no doubt bolstered by the fact that 51% of respondents have themselves experienced some form of a breach due to phishing/pharming. As a reaction to this increase, in June 2005, the Federal Deposit Insurance Corporation (FDIC) in the USA stated that financial institutions should implement some form of multi-factor authentication or layered security to protect customer data. This was later supported by The US Federal Financial Institutions Examination Council's (FFIEC), a federal inter-agency council responsible for the examination of US financial institutions. Their guidance entitled "Authentication in an Internet Banking Environment" determined that a User ID and password combination is no longer sufficient to combat increasing threats. In October, 2005, the council released a guideline endorsing two-factor authentication for web banking that is to be adopted by December 2006 citing that single factor authentication alone is inadequate for high-risk transactions such as access to customer information or the movement of funds.

An interesting question arises from this subject, one that DTT's GFSI group posed to respondents: should financial institutions be responsible for extending protection to the computers of their customers who conduct online banking? Only 29% of respondents think so and 8% are undecided. While many of the leading financial institutions are already considering additional security measures and 38% have moved beyond password authentication for online banking (with 25% intending to do so within the next 24 months) they are, at the same time, conscious of treading the fine line between making the customers' online banking experience a safe and positive one and interfering with the convenience factor, which is the key reason for banking online in the first place. Therefore, financial institutions will likely continue to be challenged with how best to protect their customers' data and yet still present an environment that is appealing for customers. Some respondents feel that if they take on the responsibility to protect their customers' computers, they will also have to share some of the liability.

While multifactor authentication adds an additional layer of security, it is not a silver bullet against risk, such as spyware, phishing and pharming. It also raises a question for those who deal with a number of financial institutions: does this mean having a key chain full of tokens and more passwords to remember? Moving forward, the industry needs to work closer together to develop solutions that not

only make it safe for customers but are still enjoyable and possibly interchangeable between providers.

Online processes have created significant cost reduction and savings opportunities for financial institutions. However, in the absence of appropriate security to protect identities online, the financial institution opens itself up to considerable reputational risk, including the erosion of user confidence in online services.

5. The value of measuring performance

While virtually all financial institutions would want to be considered “world class” when it comes to managing information security risk, most would have great difficulty living up to such a claim. According to the survey, the challenge lies with the fact that many financial institutions still do not measure the effectiveness of their information security controls – and one cannot prove what one does not measure. While reporting and measurement were identified as one of the top five security initiatives in 2005 (62%), the topic did not make the top five this year. It is difficult to determine whether those who indicated that it was a priority last year achieved their goal, or whether they simply gave up in frustration. In 2006, respondents who indicate that reporting and measurement is a top priority fell to 36%, while the number who indicate that they measure success with their information security programs fell from 34% in 2005 to 23% in 2006.

This year, 29% of respondents indicate that they have attempted to define a set of Key Performance Indicators (KPIs) that executives could use to assess and improve their information security programs. Another 30% indicate that this is in progress. However, another 26% of respondents are still struggling with how to define and measure the success of their programs.

With information security slowly making the transition from computer room to boardroom, defining and implementing an effective performance program is a major step toward improving awareness and accountability for information security and related processes. The potential benefits of an effective measurement program include the necessary executive buy-in and support for resourcing, the desired financing and a foundation from which to drive a fact-based, decision-making process. Effective measurement will likely help to identify the strengths and deficiencies of the program so that resources can be effectively applied and the program continually improved. Achievement of these end goals translates into improved infrastructure performance, information security objectives aligned with those of the business, improved cost

control and improved management of regulatory and compliance requirements. Looking ahead, organizations that measure program performance will likely be better able to identify deficiencies and risks before they become a problem.

For those who already understand the benefits associated with measuring performance, the question remains: how does one implement an effective and maintainable measurement program? Putting an effective program in place requires an integrated, comprehensive approach that allows the organization to evaluate a spectrum of internal and external metrics. Since the task of collecting, consolidating and reporting these measures is daunting, many organizations are building on technologies already deployed to feed information into a set of logic trees that move from the base of collected data or metrics to meaningful KPIs. These KPIs, and in some cases, Key Performance Indices (KPIs) (which are a summary or correlation of one or more KPIs that provide an indication of the overall performance of a defined area), need to be closely aligned with the objectives and goals of the business. In some cases, a multidisciplinary team should be established with the goal to ensure that areas important to the business are measured in order to gain buy-in from the owners of the appropriate data sources. Senior level executives will likely need to determine the appropriate information security performance objectives that also meet the goals of the organization. Once the important questions have been identified and agreed upon, they can be categorized by required performance measurement. When this has been achieved, stakeholders’ interests can be translated into strategic business objectives with the accompanying security strategies.

Through the process of dividing strategic business objectives into operational metrics and performance targets, the organization will likely be able to continually align the information security program with the goals of the institution. Organizations in the early stages of developing a measurement program should develop measures that provide a clear view of how well the organization is performing.

When defining the program targets, various categories of measurements should be considered, such as quantitative versus qualitative measures, the volume of metrics collected and analyzed as well as the process of collection and synthesis. In addition to collecting and synthesizing all metrics internally, “best in class” organizations are also attempting to calibrate them by using a variety of external measures, such as external benchmarks, external research organizations and competitor insight.

Once the program objectives and KPIs have been established, the creation of a scorecard or dashboard may be used to drive awareness and accountability. The goal of an effective information security dashboard is to define and integrate data from many sources in order to identify trends, potential exposures, inform those who are responsible for taking action, and assist in performing ongoing analysis to predict future outcomes and continually improve the information security program.

6. Convergence is not here yet

Organizations are now experiencing challenges stemming from a wide range of security initiatives, from the physical protection of their buildings, equipment and people to the security of their networks and critical information. If one adds to that mix the fact that many institutions are also dealing with an increasing number of regulatory issues, it is easy to see why the issue of security is getting the attention of the executive management team.

Historical analysis shows that most organizations have addressed security concerns from the perspective of a number of different functions within the organization and, typically, in a non-integrated fashion. This approach is due, in part, to the fact that IT security has been primarily viewed as an IT issue and that physical or corporate security has been concerned mostly with the process of keeping the “bad guys” out. Another factor in this approach has been the wide disparity between the business and IT functions in relation to competencies, compensation, inter-organizational perception and reporting structures. Only recently has the marketplace become aware of the possible benefits (e.g., cost savings, more efficient regulatory compliance and improved risk management) of bringing together these two areas of the organization.

Outside observers might question why these two groups were never merged before and why two separate departments existed in silos, rarely communicating with one another. It appears that, on an intellectual level, both groups understand the concepts of threat and risk mitigation and the importance of being able to effectively respond to an incident, as well as the economies of scale that may be achieved through the integration of technology initiatives. However, according to this year’s responses, the trend is still in its infancy, with many unresolved questions around the issue of successful organizational transformation. Overall, 24% of respondents have experienced some form of convergence within their organizations and another 7% intend to deal with the issue within the next 24 months. Regional differences are significant in the

area of convergence – APAC (48%) and EMEA (27%) have shown the strongest growth, while Canada has experienced the least (6%).

High-level examination shows that corporate and logical security share fundamentally similar internal structures and processes and, therefore, appear to be ripe for convergence. But closer examination reveals the many disparities and challenges. The difficulties do not appear to stem from a lack of rationale but rather from the cultural and structural elements of organizational architecture.

Of this year’s respondents, only 12% have an individual who is both the Corporate Security Officer and the Chief Information Security Officer. Of the organizations that have separate individuals in each position, 25% of them have a reporting structure that sees both individuals reporting to the same executive. Herein lies the problem: perception and reporting within the organization are major cultural hurdles. Other potential barriers to convergence include issues such as competencies, whereby physical security employees are viewed as either highly specialized in a niche type activity or as not having the same levels of education, training and continual education typically found on the logical side. The result is that there are major differences in areas such as compensation, another disparity that exacerbates barriers and tension between the two groups.

To converge or not to converge, that is the question. Although the trend is grabbing the attention of many, it does not appear to be a burning issue for financial institutions at the present time and looks as it may be further in the future than some speculate. Nevertheless, it will likely be an interesting topic to keep a pulse on. The issue will likely be made more immediate as organizations begin adopting technologies such as smart cards, biometrics and tokens (16%, 21%, and 10% respectively plan to have deployed, or piloted these technologies in the next 18 months) and begin integrating them with plans for corporate security offerings.

As information security and the role of the CISO continue to evolve in terms of scope of responsibility and value, and as formal risk management efforts become more integrated and cross functional, it will likely become increasingly clear that the logical and physical areas of the organization can contribute more value together than apart.



Governance

According to the survey, information security is a topic that shows no sign of fading from the corporate agendas of financial institutions. As they continue to deal with a host of security issues, including identity theft, data leakage, account fraud, phishing, and a slew of other internal and external attacks in addition to criminal activity, financial institutions have come to recognize that the topic is here to stay.

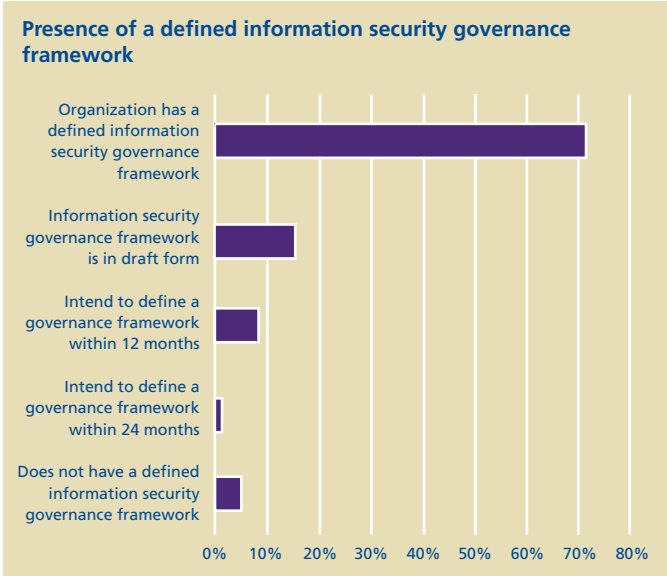
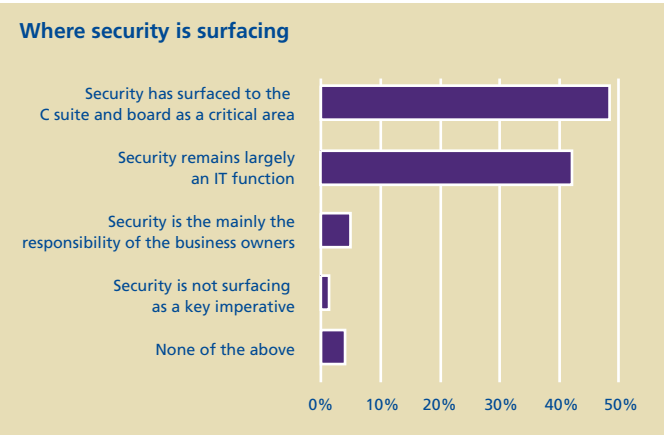
As many publications have stated – and as this year’s global security survey will support – information security continues to evolve from a technology-focused problem to one that is demanding the attention of senior-level executives and the general public. One of the survey statistics shows that 48% of respondents feel that the issue of security has risen to the board and C suite levels as a critical concern. This fact is further supported by this survey when one looks at the increasing frequency, and the nature of, reports provided to the board: those that indicate major security investments from a risk and return point of view (43%); those that deal with knowledge of information security risks (82%); and those that are issued at least quarterly (30%).

A major challenge for financial institutions is to manage information security risks, be able to prove they are being managed effectively and, at the same time, be in a position to make the appropriate business decisions and actions in order to grow the business.

In order to address this challenge, effective information security risk management requires coordinated and integrated action from the top down. Information Security Governance encompasses the principles and accountability framework intended to encourage

desirable behavior in the use of technology. This year, 71% of respondents indicate that they have a defined information security governance structure (e.g. defined responsibilities, policies and procedures) while 24% are in the process of establishing one. For the 21% of respondents that lacked a defined governance framework they also felt that their security initiatives were not aligned with the needs of the business.

- 71% of respondents have an information security governance framework.
- 15% of respondents have an information security governance framework in draft form.
- 9% of respondents indicated that they intend to have a defined information security governance framework within the next two years.
- Only 5% of the respondents do not have, nor intend to have, a defined information security governance framework.



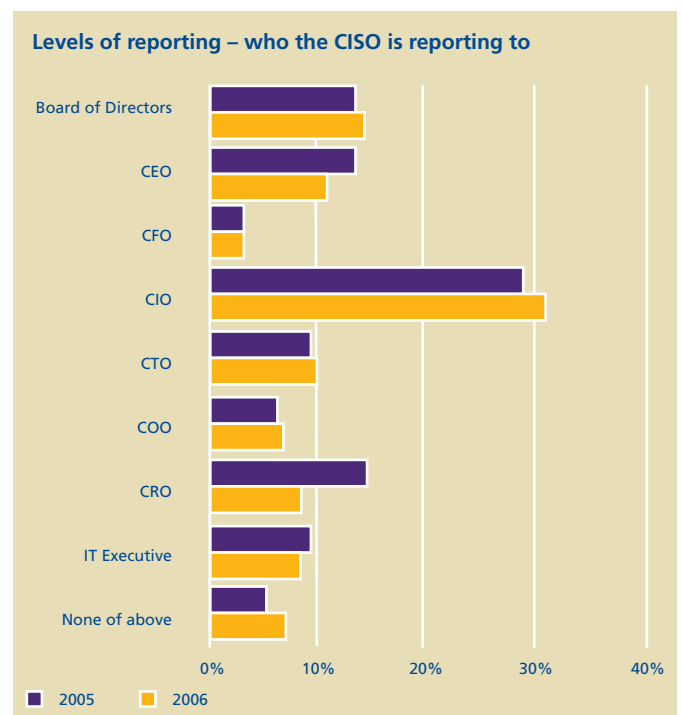
Although it is important to remember that our population of respondents change based on size, geographic dispersion and organization, from year to year, fluctuations in percentage indicate more directional movement than a static finding. An interesting statistic emerged as it related to the CISO. This year only 75% of the respondents indicated that this role was established, a decrease of 6% from 2005. On a positive note, the lifespan of the position continues to grow. While the majority of CISOs (39%) have been in the role for three to five years, the number of those who have been in the position from six to ten years increased from 13% in 2005 to 22% in 2006. Although 20% have been in the position for less than two years, a large percentage of tenured CISOs – in the position for longer than 11 years – have either departed or retired (16% in 2005 down to 10% in 2006).

Summing up the tenure of CISOs:

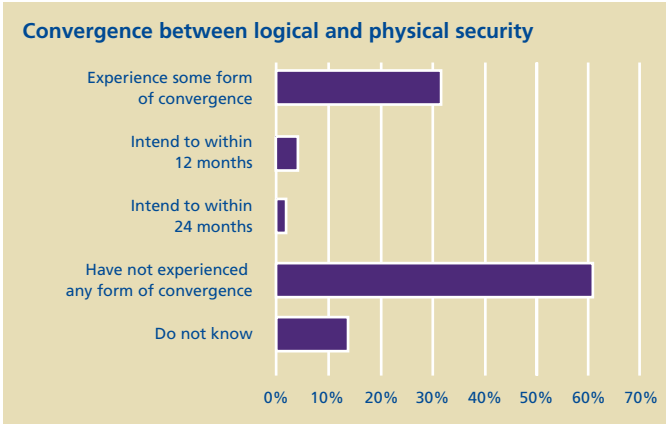
- Tenure of up to two years: 19%.
- Tenure of from three to five years: 39%.
- Tenure of from six to ten years: 22%.
- Tenure of over 11 years: 10%.

The practices of an organization detail who is involved in the governance activities, who has the authority to execute the process and who is ultimately responsible for the area. This year, 85% of the CISOs indicate that they either report to the 'C' suite level (e.g., CIO, CFO, CRO, CEO) or to the Board of Directors, with the majority (32%) reporting to the Chief Information Officer (CIO). It is interesting to note that of the organizations who believe that security has surfaced to the C suite, 74% had their CISO reporting to the C suite as well.

As the security industry matures, the role of the CISO continues to be redefined, with the scope and mandate of the CISO moving in the direction of strategic activities (84%, security and planning) and away from typical operations (55%, security operations). The trend is towards strategic responsibilities including functions of compliance and governance (44% regulatory compliance) while maintaining the bedrocks, such as implementation and integration (82%).



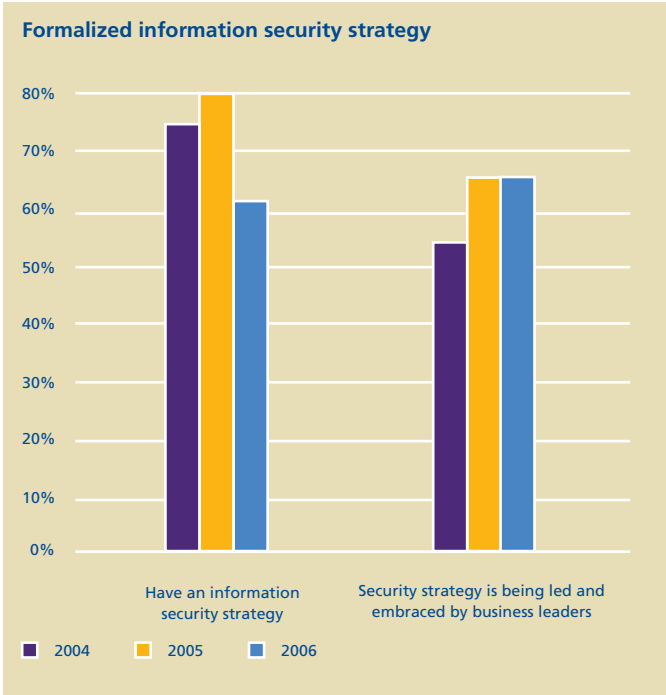
As financial institutions continue to focus their attention on compliance, and interdependencies between business functions and optimizing their security investments, there is much talk in the marketplace around the convergence of physical and logical security, either structurally where the two groups are combined together or technologically where technologies are integrated to serve a selection of needs for the organization. However, with all the hype in the marketplace, it is interesting to note that 21% of respondents have considered some form of convergence while another 4% are planning to look into it over the next 24 months. In regards to reporting structures, 50% of the respondents have a Chief Security Officer and 60% of those positions report to a different level within the organization.

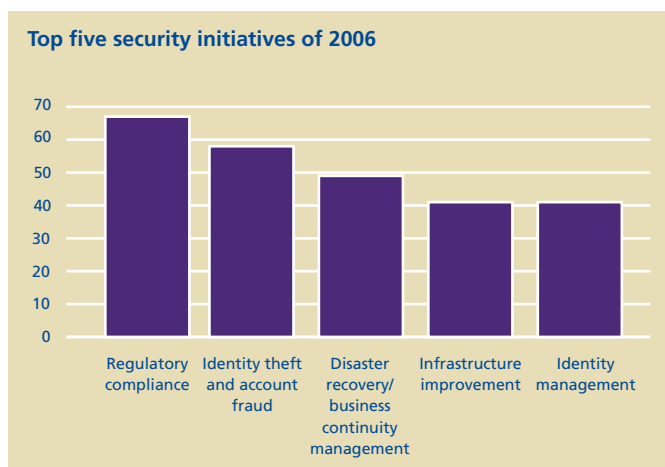


An information security strategy provides a formally defined process for translating the business objectives of a financial institution into implementable responsibilities, structures, and processes. This year, the number of financial institutions who have formulated an information security strategy has declined to 61% while another 21% indicate that they are in the process of formulating or refreshing one for their organization. Of those who respond that they have an information security strategy in place, 78% also have a CISO helping to pave the way.

The number of respondents who feel that the strategy has been led and embraced by line and functional business leaders holds steady at 66%, virtually unchanged from last year.

The information security strategy should provide a foundation for the ongoing operation and enhancement of the overall security program. The 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 drivers for information security have evolved to include the areas which are affecting and challenging financial institutions around the globe. As DTT's GFSI group indicated last year, regulation is here to stay with only more to come – which helps explain how compliance with global regulations remains as a top priority. But as more organizations experience challenges with data leakage and are blamed for poor information management practices – focus is placed on identity theft, account fraud and complementary solutions such as identity management or access control.





Organization's top five security initiatives for 2006:

- Regulatory compliance – 67%.
- Identity theft and account fraud – 58%.
- Disaster recovery and business continuity – 49%.
- Infrastructure improvement – 41%.
- Identity management – 41%.

These findings provide input to the information security strategy and the planning process as well to the specific elements that information security governance should address. The top priority areas for 2006 help to demonstrate that as the complexity and breadth of information security continues to evolve and as the cost of an ineffective program leading to a breach is clearly escalating, thus drawing unwelcome attention from senior executives, the role of the CISO continues to demand a greater focus on program management issues.

To effectively demonstrate the objectives of information security governance, it is necessary to understand and define expected outcomes, performance targets, efficiency measures and related reporting requirements. Reporting on the effectiveness of the information security program is typically provided through the collection and reporting of a selection of measures or key

performance indicators (KPI). A KPI is a measure of a particular organizational performance activity or an indicator of a precise health condition within the institution. This year, only 23% of respondents indicate that security effectiveness is tracked and monitored within their organizations and another 26% are struggling with how to define and measure the success of their security investments.

This finding supports a similar finding that 29% of respondents have defined a set of KPIs for executives to use to assess and improve their information security programs and that 29% of respondents whose security initiatives are well aligned with the needs of the business are attempting to measure the effectiveness of these initiatives. Of the rest, 30% are in the process of attempting to complete this exercise with varying degrees of success.

The following categorizes organizations that have attempted to define a set of KPIs that executives could use to assess and improve information security program management:

- Yes (29%).
- In progress (30%).
- No (35%).
- Do not know (6%).

As they go forward, organizations need to determine how their security controls and architecture align with relevant global legislation and regulations, business risk and the requirements mandated from their customers and business partners. Such a framework will provide organizations with a tool for organization-wide guidance to help ensure that information security is approached in a manner consistent with the corresponding level of risk.

One of the primary roles of the information security function is to act as a liaison between those who own the data and those who implement the controls. It is easy to see why only 33% of respondents feel that business and information security initiatives are aligned and designed based on feedback. Only 45% of respondents feel that the information security function is effective in meeting the needs of the business.



The following illustrates the extent to which business and information security technology initiatives are well aligned:

- Business priorities are appropriately aligned with security (33%).
- Business and security priorities are somewhat aligned (50%).
- Business and security priorities are not appropriately aligned (12%).
- Do not know whether business and security priorities are aligned (5%).

Financial institutions continue to operate in an environment of increasing regulation and government legislation, pushing them to invest more and more resources into compliance with global regulations. The information security program of each respondent will need to address the ongoing requirements in some form and risk management will likely remain a governance issue requiring the involvement of management and business. This fact is demonstrated in part, by the continual increase in the number of respondents (76%) who feel that senior management continues to commit the required funding and support to appropriately address regulatory and legal requirements. However, with all the focus on compliance,

organizations should not divert their attention from delivering core security needs. As DTT's GFSI group reported last year, organizations that embrace compliance and regulation and invest dollars and minds in figuring out how one regulation may overlap another may not only be in a position to implement better practices but also to develop a practice that is effective and sustainable. Today, 89% of respondents feel that legislation and regulation are driving compliance-related activities at least 'somewhat' within their organizations and that these efforts are effective and sustainable.

Legislation and regulation are driving compliance related activities and costs that are leading to sustainable and effective solutions, as follows:

- Effective (37%).
- Somewhat effective (52%).
- Not that effective (5%).
- Do not know of effectiveness (6%).

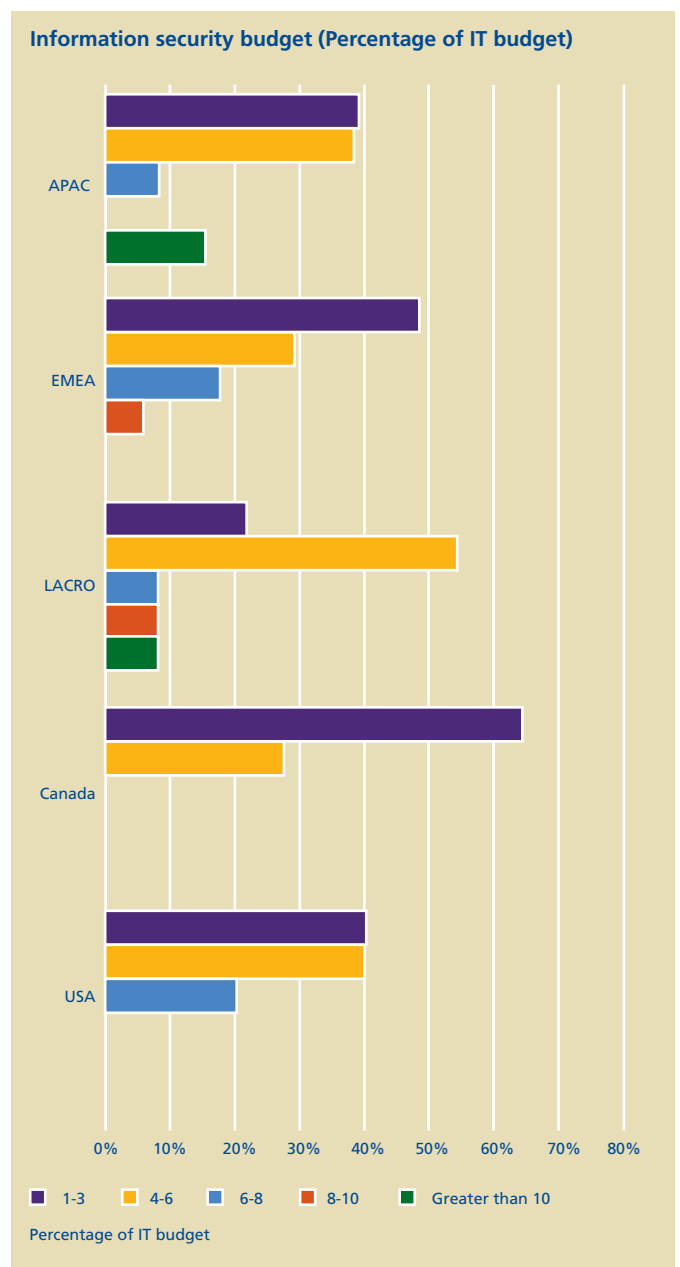
Investment in security

Spending on information security by financial institutions is very much on the rise. A full 95% of respondents indicate that they have experienced some form of growth in their information security budgets, with over 20% reporting an increase of over ten percent in 2005. However, there was a drop in one of the categories: the number of respondents whose security budgets are 1-3% of their IT budget decreased from 47% last year to 43% this year, yet still leading as the global average. The number of respondents whose security budgets are 4-6% of their IT budgets increased from 29% in 2005 to 36% in 2006 while 20% indicate that their security budgets are over 7%. These findings further demonstrate that information security is still perceived to be an IT issue with 59% of respondents indicating that they still do not have an information security budget separate from their IT budget. Outside the IT function, which accounts for 49% of the overall supplemented funding for information security, the lines of business, at 23%, represent the largest areas of supplemented funding for information security.

Security spending continues to be fueled by a variety of concerns, not the least of which is compliance with regulation, which continues to play a significant role in security spending decisions. The various trends outlined in this report are key drivers of security spending by participants. The risk tolerance of an organization might be seen to be reflected in the annual information security budget, i.e., the higher the risk tolerance, the lower the budget.

The following is a breakdown of spending within the information security budget spending:

- Logical access control products: 76%, up from 72% in 2005.
- Security consultants: 72%, up from 64% in 2005.
- Infrastructure protection devices: 69%, up from 67% in 2005.
- Physical access and control devices: 24%, down from 31% in 2005.
- Hardware and infrastructure costs: 56%, up from 55% in 2005.
- Audit and certification costs: 34%, down from 46% in 2005.

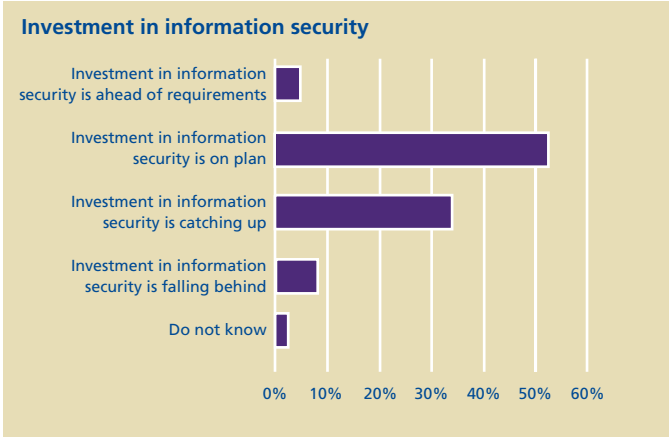
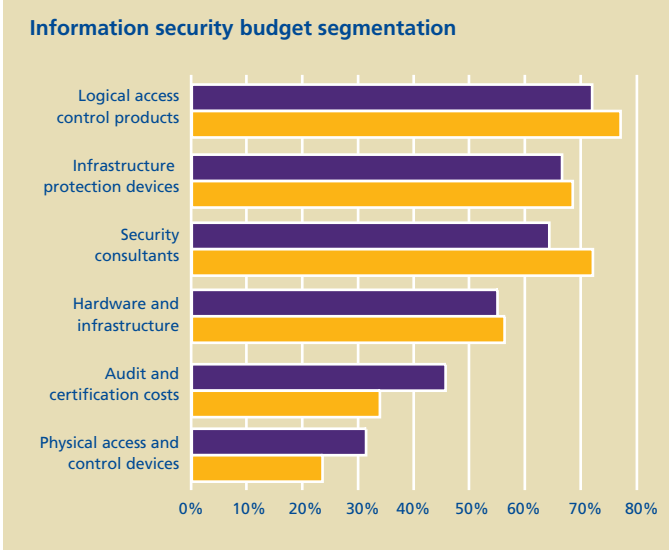


In today's environment in which organizations continue to deal with compliance, with regulations and country-specific privacy legislation, organizations respond in attempts to improve control over users' access and management as logical access control products and infrastructure protection devices top the list of the information security budget.

It seems that more and more organizations are buying into the belief 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 also an increase in respondents who now include security awareness and communication costs (employee training and embedding of the importance of security values) in their budgets.

This year, 50% of respondents indicate that their investment in information security is in line with the needs of the business, while 33% feel that they are behind and need to catch up. With greater scrutiny of budgets and increasing attention in the areas of security and compliance, the number of respondents who feel that their projects do not fail that often to deliver what they promise increased from 55% to 58%. Not surprisingly, that perennial sore spot, integration problems, remains one of the top causes of failure for 35%.

More and more organizations are buying into the belief that the human aspect of an information security program is critical to its overall success.

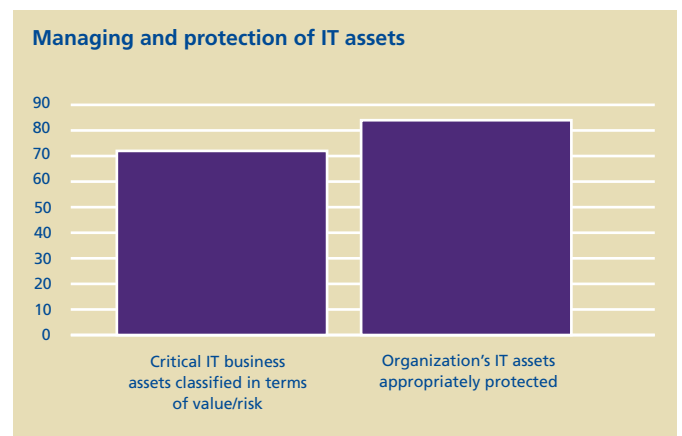


Risk

There is little doubt that IT and information security remain fundamental concerns of the financial services environment of today. Financial institutions, held to the ultimate standards of trust and security, are expected to manage risk effectively, protecting both internal and external environments from potential breaches. The information security strategy is guided by the information security vision, which in turn, is guided by the institution's approach to risk management. Risk tolerance dictates an organization's approach to managing risk in striving to reach the objectives set out by the business. For the fourth year in a row, respondents indicate that they rely on the risk appetite levels of their counterparts in the industry, with 48% of respondents indicating that they take on comparable levels of risk. This finding is in line with the number of respondents (52%) who would characterize their level of risk as effective and efficient and with those respondents (39%) who would categorize their risk practice as taking only the required risk necessary.

Risk assessment is an important aspect for finding solutions to address the various risk challenges that currently face financial institutions. In keeping with survey findings of previous years, 90% of respondents indicate that having a risk management process within their organization is either "very important" or "extremely important". Financial institutions that have a systematic approach to managing risk are more inclined to ensure an ongoing investment in information security and that the right controls are in place for the business. A risk management program will likely assist a financial institution in assessing the probability of internal, external, deliberate and accidental threats to information assets. However, while the majority of respondents indicate that such a process is very important, only 72% have gone so far as to identify and classify their critical IT business assets in terms of value to risk, while 84% of those feel that they have taken the necessary steps to effectively protect them.

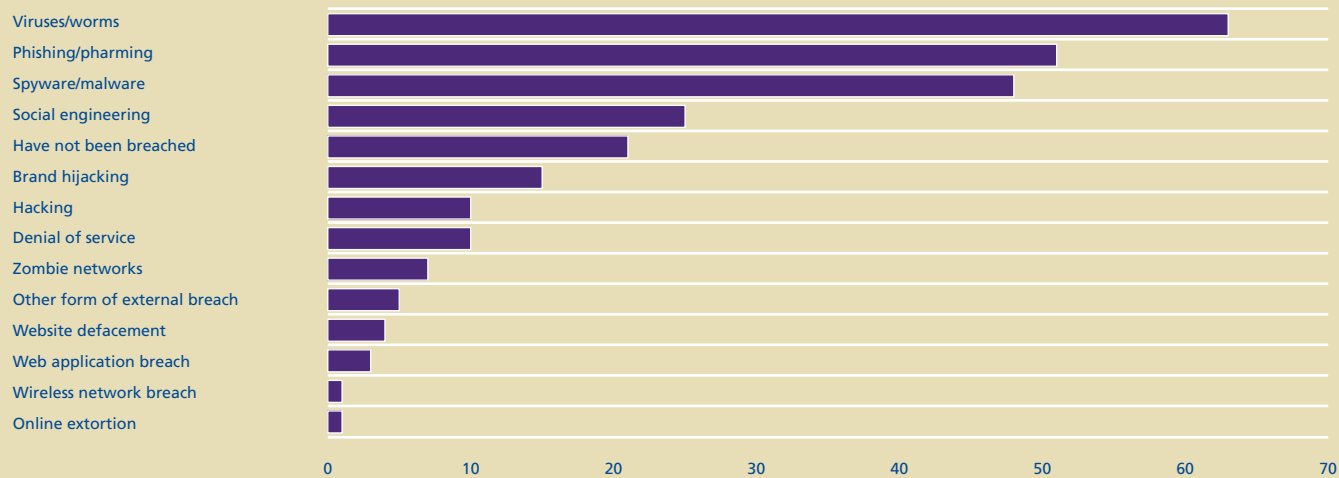
It has been said that there is no future without risk. New technology ranks right up there with one of those undertakings of greatest risk. The increasing demand for mobility, agility and interoperability being placed on the IT and security functions has led to exponential growth in a variety of communication mediums, all of which open the door to new kinds of risk. In 2004, 83% of respondents indicated that they had experienced some form of successful breach, either internally or externally. In 2005, this number decreased to 28%, based on the make up and distribution of respondents. However, as the respondent pool increases each year along with geographic distribution, so too does the risk of successful breaches. As a result, the percentage this year remains relatively unchanged (82%) from 2004.



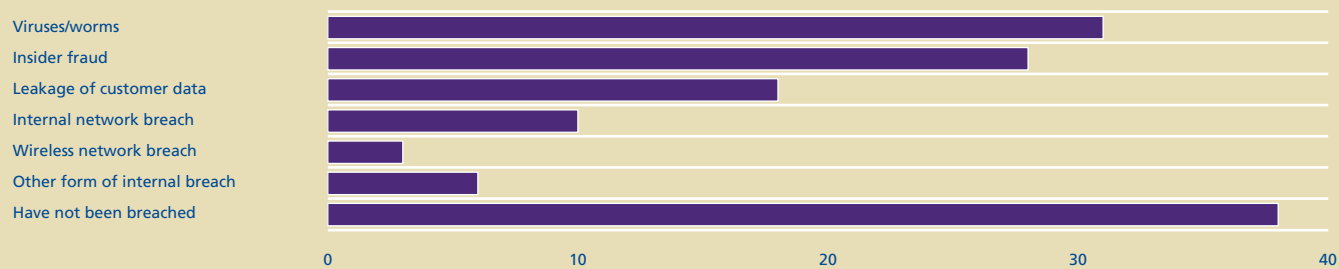
External breaches experienced included:

- Viruses/worms – 63%.
- Phishing/pharming – 51%.
- Spyware/malware – 48%.
- Social engineering – 25%.
- Brand hijacking – 15%.
- Hacking – 10%.
- Denial of service – 10%.
- Zombie networks – 7%.
- Website defacement – 4%.
- Web application breach – 3%.
- Wireless network breach – 1%.
- Online extortion – 1%.
- Other form of external breach – 5%.

External breaches over the past 12 months



Internal breaches over the past 12 months



Internal breaches included:

- Viruses/worms – 31%.
- Internal network breach – 10%.
- Wireless network breach – 3%.
- Insider fraud – 28%.
- Leakage of customer data – 18%.
- Other form of internal breach – 6%.

Of those who have experienced a breach, 78% indicate that they experienced a breach from an external attack, 49% indicate an internal attack and 44% have experienced both.

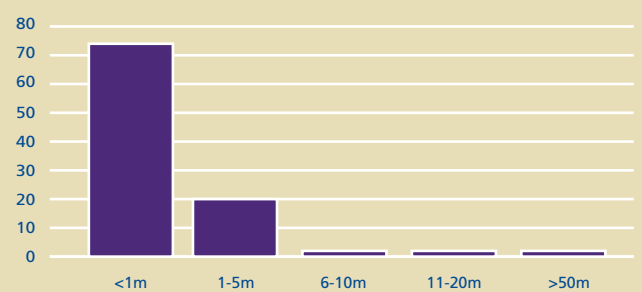
Of those respondents who had experienced a breach internally, viruses and worms originating from inside the organization were the top offenders (31%), with insider fraud at 28% and leakage of customer data at 18%.

A breach can have a major impact on the organization's image and reputation. This year, 72% of those breached indicate that the estimated amount of damage to the organization, including direct and indirect costs, was in the range of \$1 million, while 2% of those feel that the number is over \$5 million.

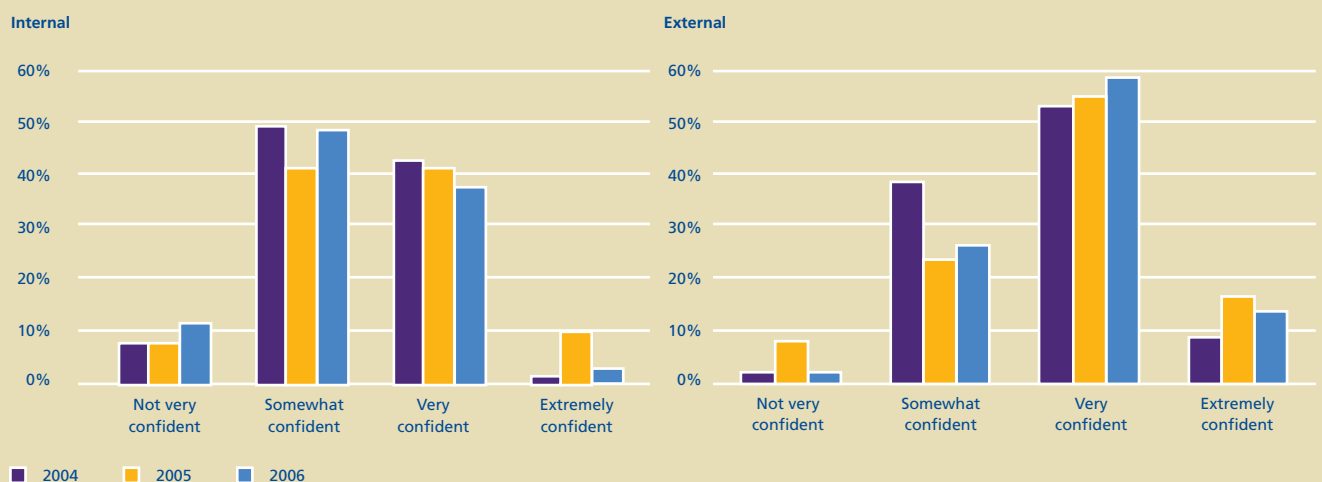
In keeping with the responses of previous years, respondents remain confident that their organization's networks are protected from attacks internally, with 41% indicating that they are either "very confident" or "extremely confident". Only 11% are not very confident at all, a surprising number since the majority of organization's experienced a successful breach and 28% of those had a breach occurring from insider fraud. When it comes to external attacks, 74% indicate that they are either "very confident" or "extremely confident", up from 69% in 2005.

A respectable 69% of institutions have classified their information assets with respect to confidentiality and privacy and 64% of those provide users with instructions, reference material and the required training.

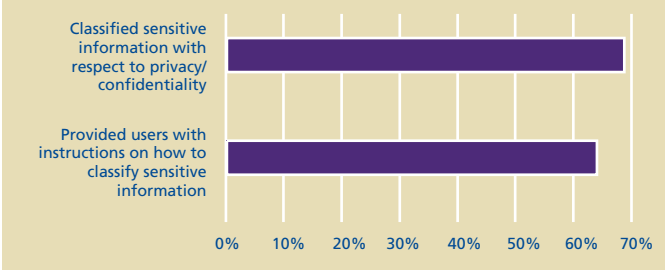
Damage sustained due to attacks (US\$)



Protection from cyber-attacks

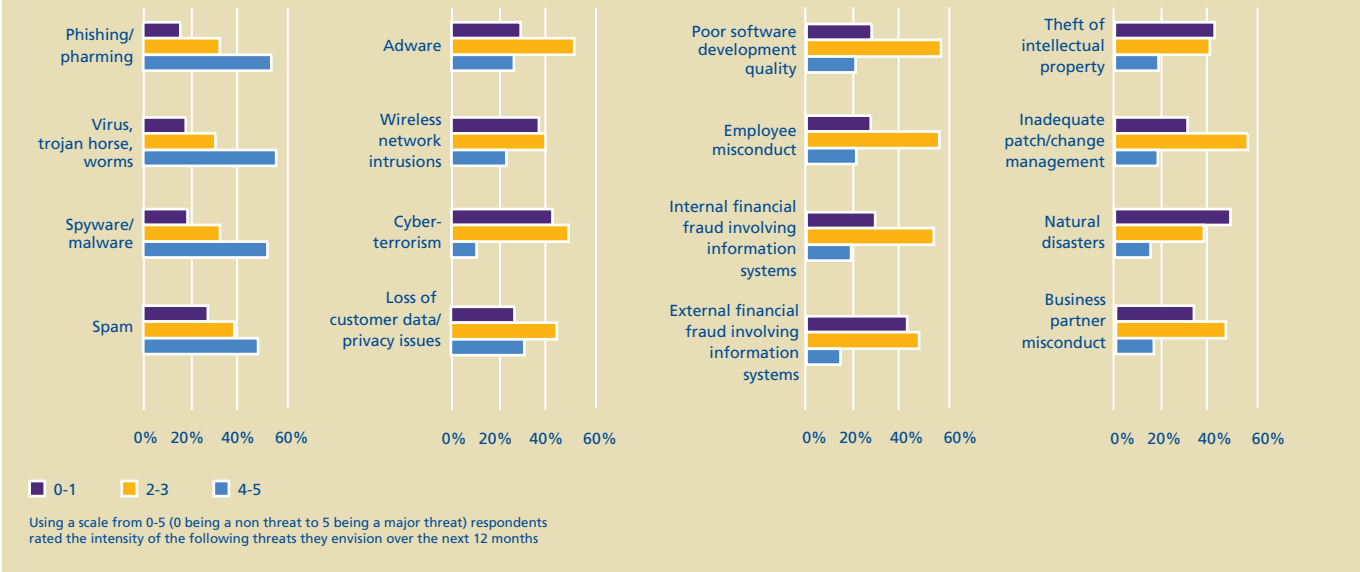


Information, identification and classification



Respondents remain confident that their organization's networks are protected from attacks internally.

Threats envisioned over the next 12 months



Use of security technology

The traditional approach to security – concentrating on infrastructure and technical components – becomes less effective as technology changes. As information security continues to evolve, so too do the business systems which are now becoming data centric rather than system or transaction-centric. Spending on security technologies is being driven by a number of concerns – regulatory compliance, identity theft, and identity management being the top three.

Financial institutions are accustomed to the concept of perimeter protection, with such methods as anti-virus protection, which 99% of the respondents indicate they use. However, as the sophistication of threats continues to evolve, respondents who indicate that this is one of their major concerns over the next twelve months (56%) find that they may not be well prepared for emerging attacks using new technology, such as spyware, malware and wireless technologies.

A layered approach to security, one that combines strong perimeter protection in addition to other forms of blocking and tackling techniques, is necessary to protect an organization's information assets. Layering is key so that a failure or circumvention of one layer, whether by error, misconfiguration or deliberate action, will likely be stopped by another layer, thus ensuring no single point of vulnerability. The layering strategy is growing in popularity, evidenced by the emergence of a number of technologies that maintain an organization's perimeter while at the same time, strengthening the inner layers to better protect the sensitive data within. This trend demonstrates the continual evolution of information security as respondents begin the transition from infrastructure protection to information protection.

In deciding whether to adopt a new technology, timing is critical. Those who invest too soon run the risk of entering into costly implementations fraught with integration difficulties. Those who wait too long run the risk of being left behind the pack, saddled with old technologies. This dilemma helps to explain the consistency of cautious attitudes around risk from one year to the next. Respondents in this year's survey (59%), classify themselves as "effective users of demonstrated technologies" with only 9% willing to take the risk associated with being an early adopter. However, it was interesting to note that some technologies which may offer substantial cost savings, such as Voice Over IP (VOIP) have been deployed at a faster rate than others in the past (VOIP 28% vs. Radio Frequency Identification (RFID) at 1%).

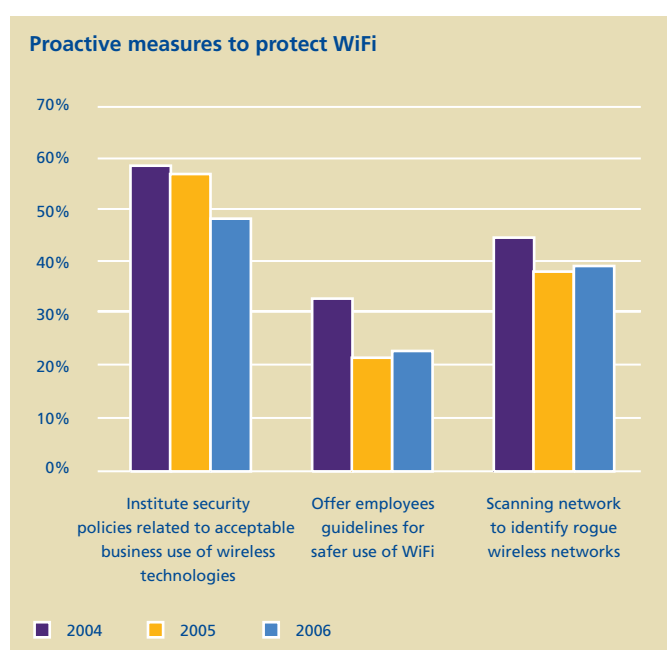
As some organizations know only too well, the unauthorized disclosure of personal information can result in not only a violation of regulatory compliance but extensive reputational damage and significant direct and indirect costs. Despite global regulation to protect information, each institution has a responsibility to ensure that contractual obligations with outsourcers, partners and contractors, and privacy policies are implemented to help monitor the risks around the flow of such data. Content monitoring and filtering technologies can help detect malicious and accidental misuse of private data and of the intellectual capital of the organization. To this end, 39% of organizations indicate that they currently track, and report publicly, loss of customer data; a full 83% have gone so far as to monitor employee use of the internet and information systems for unauthorized or inappropriate access/usage.

Technologies such as wireless networks are everywhere and the subject of much scrutiny because of the potential for breach by malicious intruders. Wireless is seen as highly risky; only 40% of respondents indicate they have deployed or are piloting wireless technologies but of those, only 64% have gone so far as to proactively protect themselves by a number of different layers.

Specifically:

- 39% have scanned the network to identify rogue networks.
- 23% offer employees guidelines for safer use of WiFi.
- 48% have security policies related to acceptable business use of wireless technologies.

Emerging technologies, such as wireless networks, will likely continue to proliferate within the work environment; as this growth continues, respondents should be adequately prepared to address the associated challenges and risks.



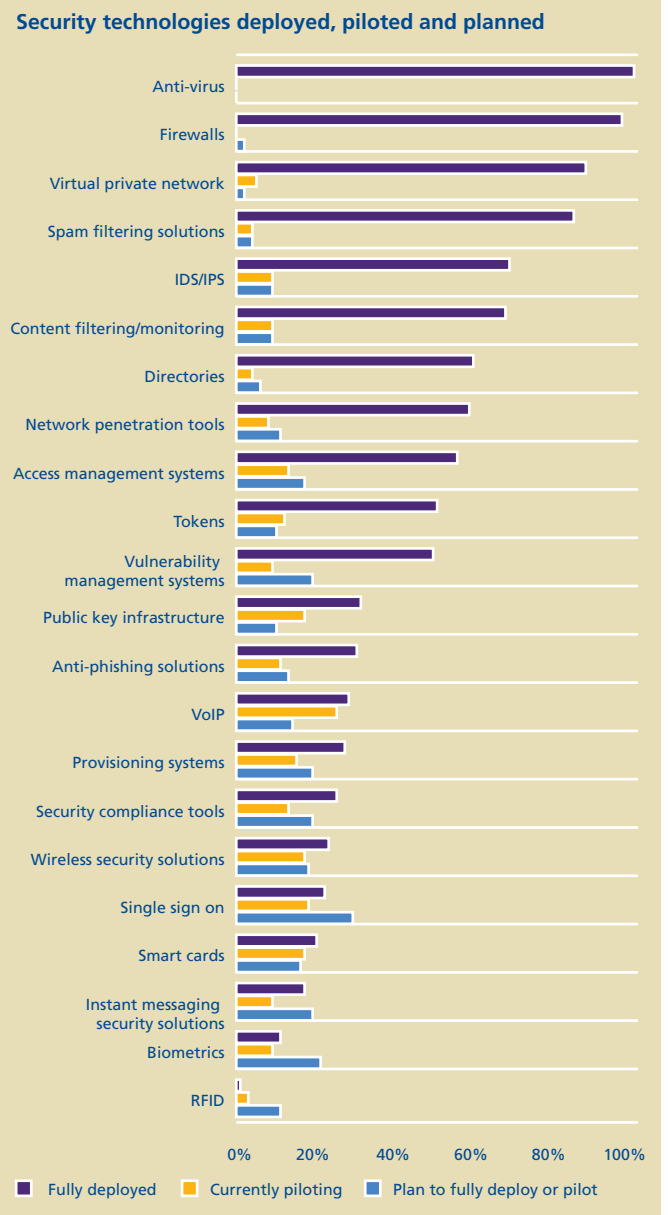
Fully deployed technologies have remained relatively consistent over the years as many technologies align with the top five identified priorities. This year, as phishing and pharming out viruses for the number one envisioned threat over the next twelve months, 30% of respondents have fully deployed anti-phishing solutions. This area of identity management 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 in an effective and efficient way for the business. This year, over half (55%) of the respondents have implemented some form of access management solution. Some organizations are experiencing ongoing difficulties with selling the business case for identity management while others are using complementary benefits to help get buy-in from various parts of the organization – such as Single Sign On (SSO) (40%). SSO would allow users to use a single password to access various resources thereby helping save the business cost in a number of areas, such as password resets.

Following is the technology (with the corresponding percentage) that this year's respondents indicate they either deploy or pilot:

- Anti-virus – 99%.
- Firewalls – 96%.
- Virtual Private Network – 87% and 5% piloting.
- Spam Filtering Solutions – 89% and 4% piloting.
- Intrusion Detection/Penetration Systems (IDS/IPS) – 68% and 9% piloting.
- Content Filtering/Monitoring – 67% and 9% piloting.
- Directories – 59% and 4% piloting.
- Network Penetration Tools – 58% and 8% piloting.
- Access Management Systems – 55% and 13% piloting.
- Tokens – 50% and 12% piloting.
- Vulnerability Management Systems – 49% and 9% piloting.
- Public Key Infrastructure – 31% and 17% piloting.
- Anti-Phishing Solutions – 30% and 11% piloting.
- Voice over IP (VoIP) – 28% and 25% piloting.
- Provisioning Systems – 27% and 15% piloting.
- Security Compliance Tools – 25% and 13% piloting.
- Wireless Security Solutions – 23% and 17% piloting.
- Single Sign On (SSO) – 30% and 18% piloting.
- Smart Cards – 20% and 17% piloting.
- Instant Messaging Security Solutions – 17% and 9% piloting.
- Biometrics – 11% and 9% piloting.
- Radio Frequency Identification Tags – 1% and 3% piloting.

In an effort to understand how respondents believe the landscape is changing, the survey asked them which technologies they would be piloting or deploying over the next 18 months. Following are the responses with the corresponding percentages:

- Single Sign On (SSO) – 29%.
- Biometrics – 21%.
- Instant Messaging Security Solutions – 19%.
- Provisioning Systems – 19%.
- Security Compliance Tools – 19%.
- Vulnerability Management Systems – 19%.
- Wireless Security Solutions – 18%.
- Access Management Systems – 17%.
- Smart Cards – 16%.
- Voice over IP (VoIP) – 14%.
- Anti-Phishing Solutions – 13%.
- Network Penetration Tools – 11%.
- Radio Frequency Identification Tags – 11%.
- Public Key Infrastructure – 10%.
- Tokens – 10%.
- Content Filtering/Monitoring – 9%.
- Intrusion Detection/Penetration Systems (IDS/IPS) – 9%.
- Directories – 6%.
- Spam Filtering Solutions – 4%.
- Firewalls – 2%.
- Virtual Private Network – 2%.



Quality of operations

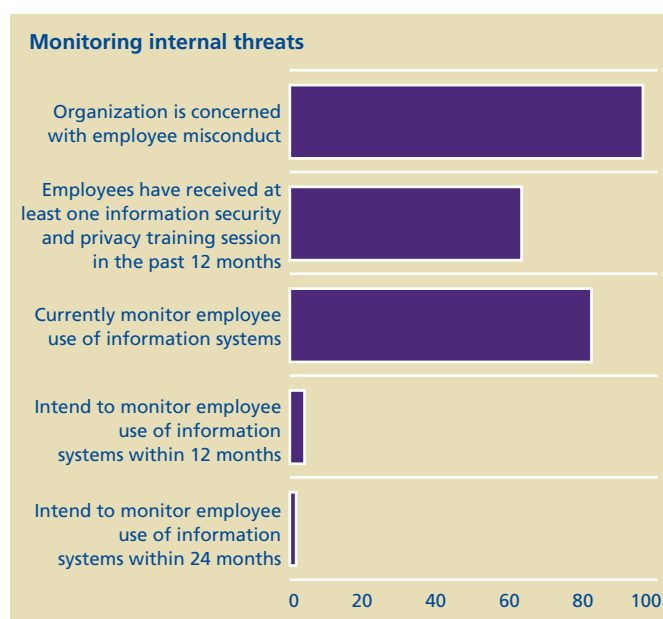
Financial institutions are aware that they must proactively work toward protecting customer data and thwarting emerging threats. The survey shows that security efforts are clearly evident in many organizations, through increasing focus on areas such as training and awareness, improved processes, and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

It is becoming clear that the scope of the information security function continues to increase into areas which are more strategic than technical. A common question is one that concerns the size of the security function: just how big should it be? The answer lies in how security is valued within the organization – whether it is considered primarily an IT risk management function or whether it is seen as contributing value to the fabric of the organization.

This year's survey indicates that the majority of respondents have less than 10 information security professionals across all functions (43%), and 6% have over 60. The majority of respondents (51%) indicate that the number of information security professionals in their organization has increased over the last twelve months, while 41% indicate that this number has stayed relatively stable. Further analysis reveals that, on average, there are two security professionals per one thousand employees in an organization and that the majority are either well prepared from a skills and competencies perspective or are quickly closing the gaps to effectively handle existing and foreseeable security requirements (35% and 37%, respectively).

Organizations are more likely to find themselves vulnerable to threats if employees are not aware of 1) relevant policies, 2) their role in helping to protect the information of the organization or 3) how to support the organization's security policies in the course of their day-to-day work efforts. It is encouraging to find that the information security professionals in 89% of respondents' organizations have defined and documented job roles and responsibilities. However, of those, only 49% link performance measures to performance appraisals, raising the issue of how you can effectively manage and improve what you do not measure.

A key trend, identified in last year's survey and continuing to play a major role in this year's findings, is that internal security threats represent a significant number of the information security incidents that impact an organization. A full 96% of this year's respondents indicate that they are concerned about employee misconduct



involving their information systems. Of those, only 34% have provided their employees with any form of information security and privacy training in the last twelve months. Of those who provided training, web page and e-mail alerts were identified as the number one medium for messaging (63%), while only 35% of respondents indicate that they have any form of orientation training to help mitigate the effects of bad habits that may have been present from the first day of employment.

The most common mediums for security training and awareness are:

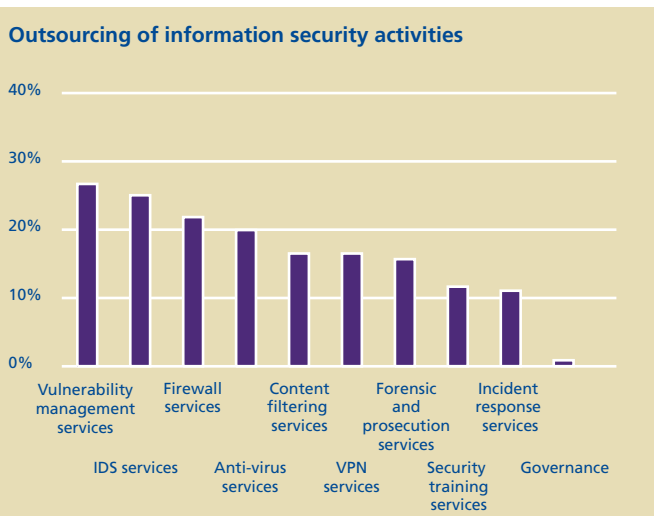
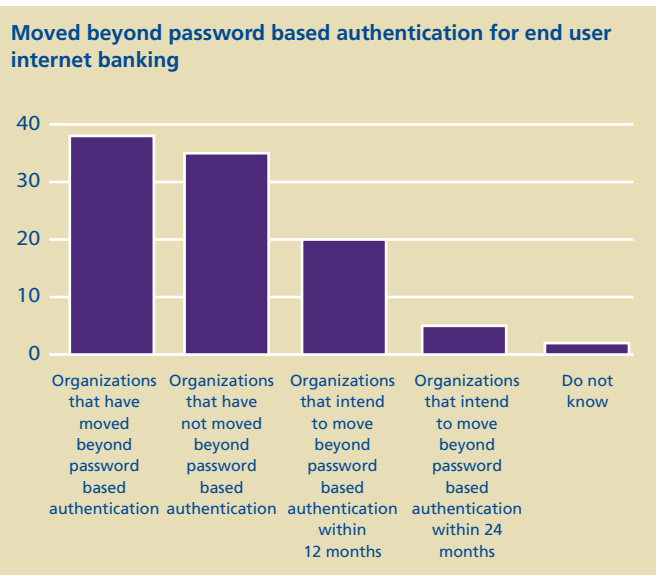
- Web page alerts and emails – 63%.
- Class room/instructor led – 48%.
- e-Learning modules – 48%.
- Newsletters – 40%.
- Orientation training – 35%.
- Posters – 32%.
- Recognition of exemplary behavior – 9%.

While the large majority of threats are due to errors and omissions (human error: 42%; operational error: 37%) rather than malicious intent, it is important to note that, of those institutions that experienced a successful internal breach, 28% were the result of experienced and intentional fraud and 18% were due to the intentional leaking of customer data.

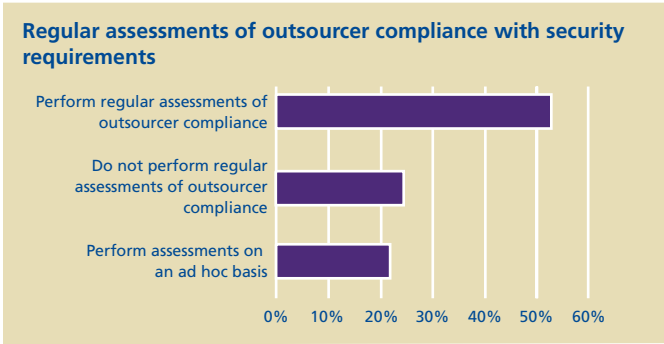
Although awareness and training programs have proven to be effective in dramatically reducing problems associated with human error, it is important that the root causes of these breaches are addressed, (e.g., access control, poor information management practices, etc.) Security training and awareness was identified as one of the top five priorities for financial institutions in 2005; this year, it fell out of the top five and was overtaken by identity theft/account fraud and identity management. While individuals most certainly contribute to the increase in identity theft, 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 these business practices that often fails is the effective and efficient management of users' identities. Data security is all about protecting data from unauthorized access and unauthorized use.

Effective access controls require good enterprise identity management techniques, a realization that is clearly dawning on respondents as 55% of them indicate that they have a fully deployed access management solution. Another 30% are either piloting or plan to deploy one over the next 18 months. Organizations that do not effectively address data security strategies will continue to struggle with the proliferation of unstructured data and weak access control.

This year, close to 70% of respondents indicate that they have outsourced at least one area of information security activities. Of those, vulnerability management (27%) and intrusion detection (25%) were among the top areas, with governance (1%), 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.



A particular area of focus should be the application of protections to data and systems across the organization, extending to third-party suppliers and outsourcing partners. These third-party relationships should be examined based on their management of security risks, processing and the confidentiality of applications and data. Only 53% of respondents regularly assess their outsourcers' compliance with the organization's information security policies



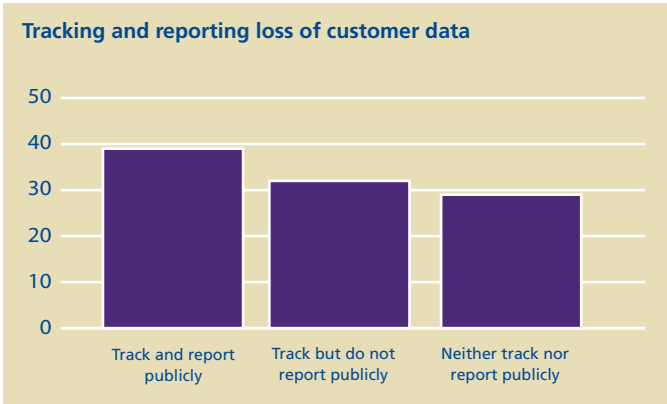
and requirements. While many organizations feel that they have adequately controlled their information, they may need to be reminded that many of their internal controls do not “follow” information assets once they leave the confines of the organization. Contracted or outsourced services may well have 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 will likely need to get used to the necessity to demonstrate their ability to comply with enhanced security requirements.

The crooks 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, 26% of respondents indicate that application security is a top priority within their organization, while 56% feel that poor software development quality poses an above-average threat over the coming 12 months.

Respondents reported the following frequencies for these practices:

Investment in information security

Practice	Quarterly	Semi-Annually	Annually	Adhoc	Never
Vulnerability scanning	40%	10%	14%	32%	4%
Penetration testing (internal)	24%	8%	26%	30%	12%
Penetration testing (external)	19%	16%	33%	28%	4%
Application security code Review	7%	2%	13%	65%	13%





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, according to the survey the most cited priority of 2006 was regulatory compliance, including privacy initiatives.

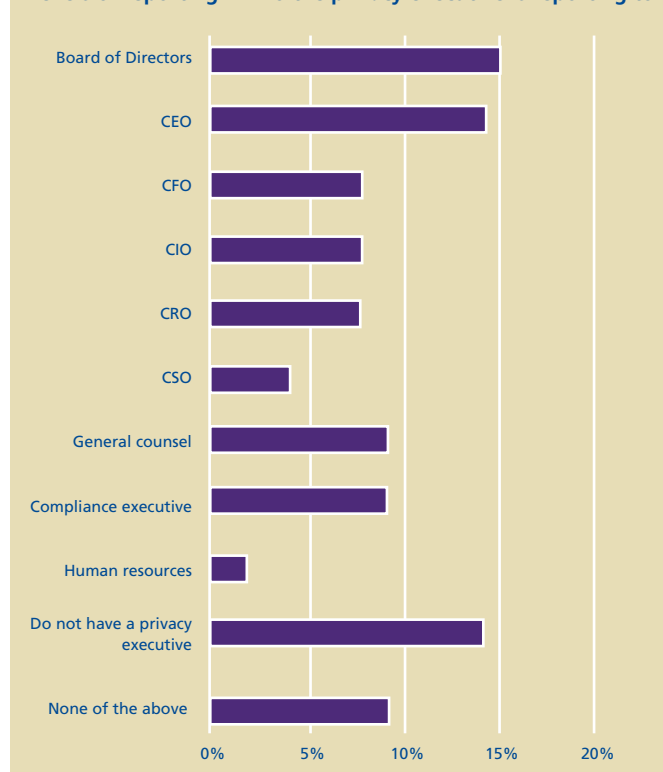
In organizations without a Chief Privacy Officer (CPO), the issues of legislative privacy requirements, privacy compliance requirements, and handling complaints from the public all present strategic and chronic vulnerabilities. It is a positive sign that 59% of respondents have an executive responsible 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 wear 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 often means that the privacy perspective is diminished or rolled into security items before issues are elevated to the attention of the CEO. Resolution of this issue is frequently thwarted by a confusing and troublesome issue: the complex and largely undefined relationship between the disciplines of information security and privacy protection. This year, 44% of respondents indicate that they are concerned with conflicts between security and privacy regulation. Although 21% indicate that, at this time, they are not concerned, another 32% were not sure.

Unlike the reporting relationship of the CISO position with its clear line of reporting to the CIO, the privacy executive reporting relationship is not as defined. Only 15% 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 (9%), general counsel (9%), the CFO (8%), and the CRO (8%).

The reality remains that organizations that collect or manage personal information require some kind of program to manage privacy issues. The executive responsible for privacy needs a working

Levels of reporting – who the privacy executive is reporting to



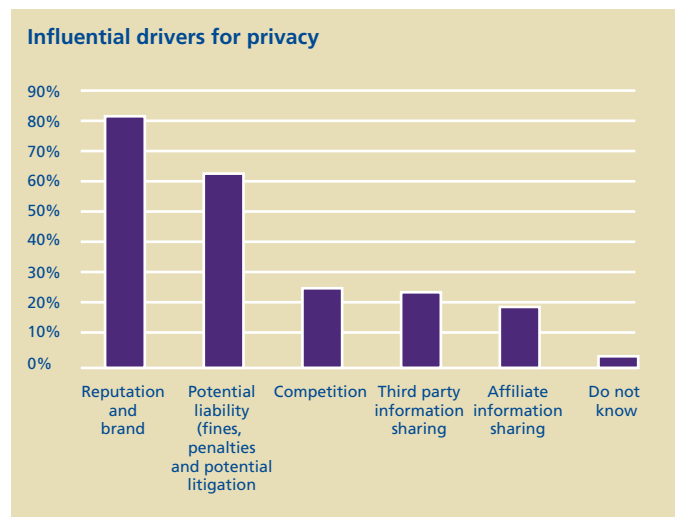
knowledge of data collection, data processing, and information management. This year, 65% of respondents indicate that they have a program in place to manage privacy compliance and 34% indicate that their programs have been in place for over four years. When DTT's GFSI group examines the maturity of these programs, they are characterized as "early stages", where the privacy program is just beginning to become staffed and organized (29%), or as "middle maturity" where the privacy program exists and has begun to launch key initiatives (27%), or by "mature stages or maintenance mode" where the program has progressed enough to be focusing on program evaluation and refinement (30%).

The issue of structuring and managing the program varied as much as its maturity. While 46% indicate that they have a distributive model, whereby responsibility lies with the business units, 42% indicate that their program is managed from a central corporate group or in a centralized fashion.

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 are:

- Privacy regulations – 88%.
- Reputation and brand – 82%.
- Potential liability (fines, penalties etc.) – 62%.
- Competition – 24%.
- Third party information sharing – 22%.

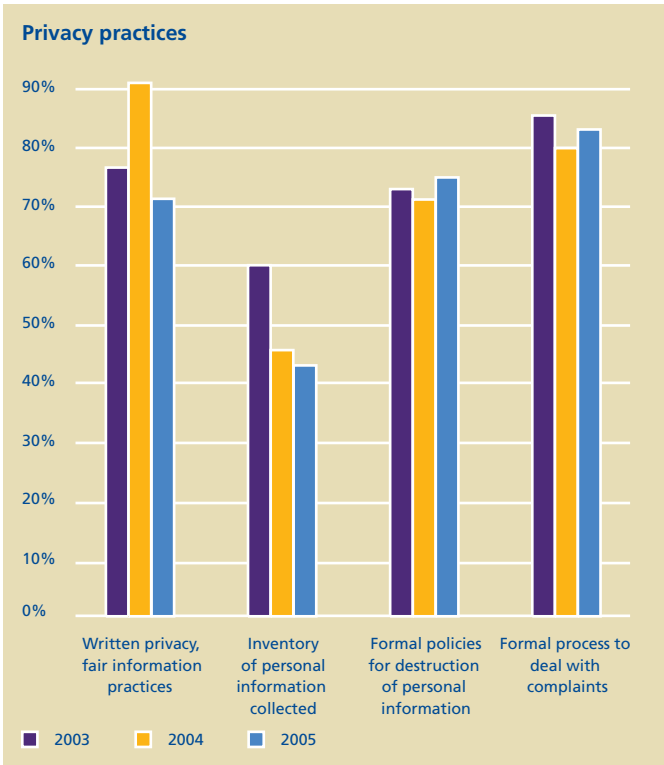
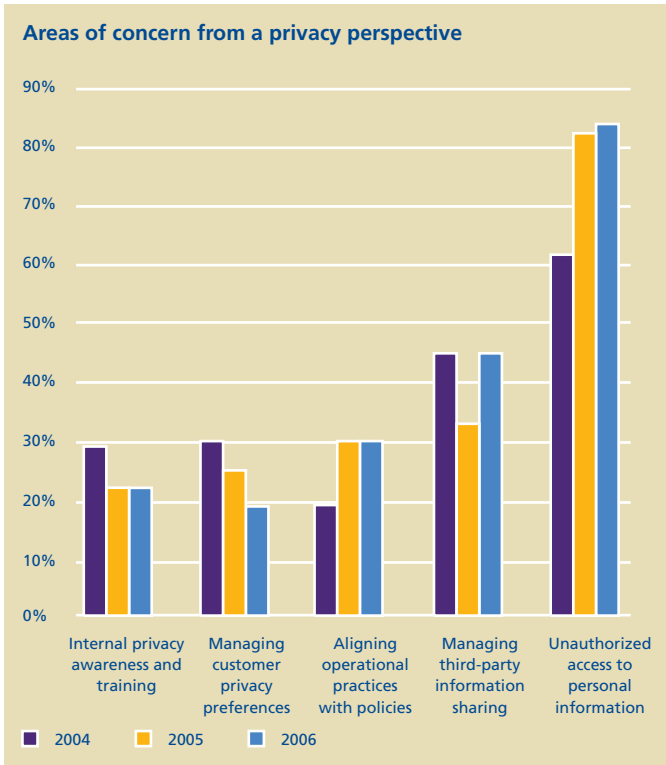


The most cited areas of concern from a privacy perspective include:

- Unauthorized access to personal information – 84%, compared to 83% in 2005 and 62% in 2004.
- Managing third party information sharing – 45%, compared to 33% in 2005 and 45% in 2004.
- Aligning operational practices with policies – 30%, compared to 30% in 2005 and 19% in 2004.
- Internal privacy awareness and training – 22%, compared to 22% in 2005 and 29% in 2004.
- Managing customer privacy preferences – 19%, compared to 25% in 2005 and 30% in 2004.

The most cited additional areas of concern from a privacy perspective are:

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



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://europa.eu.int/comm/internal_market/privacy/index_en.htm

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
www.visa.com/_gds_mod/fb/merchants/gds/main.html

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

Belgian Directors Institute (BDI)
www.ivb-ida.com

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

Ministerio da Ciencia e Tecnologia: Policy for Information Security
 Management (Brazil)
www.mct.gov.br

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

DTT's GFSI group would like to thank all of the professionals of the financial institutions who responded to the survey and who allowed us to further correspond with them over the course of this project. Without such participation and commitment, DTT could not produce surveys such as this. DTT's GFSI group extends our heartfelt thanks for the time and effort that respondents devoted to this project.

Survey Development Team

Authors

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

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

Data Analysis and Editing

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

Shiv Sengupta
1(416) 643 8380
shisengupta@deloitte.ca

Methodology and Survey Development

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

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

Marketing Support

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

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

Contacts

Jack Ribeiro

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

Leon Bloom

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

Adel Melek

Global Leader IT Risk Management
& Security Services
Global Financial Services
Industry Group
Canada
+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

Christopher Lee	USA – San Jose, USA	Deloitte & Touche LLP	+1 408 704 4314	chrislee@deloitte.com
Mike White	EMEA – Johannesburg, South Africa	Deloitte Touche Tohmatsu	+27 11 806 5899	mikwhite@deloitte.co.za
Simon Owen	UK – London, UK	Deloitte & Touche LLP	+44 20 7303 7219	sxowen@deloitte.co.uk
Uantchern Loh	APAC - Kuala Lumpur, Malaysia	Deloitte KassimChan	+65 6216 3282	uloh@deloitte.com
Mitsuhiko Maruyama	Japan – Tokyo, Japan	Deloitte Touche Tohmatsu	+81 (3) 6213-1112	mitsuhiko.maruyama@tohmatsu.co.jp
Martin Carmuega	LACRO – Buenos Aires, Argentina	Deloitte Touche Tohmatsu	+54 11 4320 4003	mcarmuega@deloitte.com

Contacts

Kim Altern	New York, USA	Deloitte & Touche LLP	+212 436 3634	kaltern@deloitte.com
Ricardo Balkins	São Paulo, Brazil	Deloitte Touche Tohmatsu	+55 11 5186 1559	rbalkins@deloitte.com
John Clark	Chicago, U.S.A.	Deloitte & Touche LLP	+1 312 486 3985	johclark@deloitte.com
Bruce Daly	Tokyo, Japan	Deloitte Touche Tohmatsu	+81 3 4218 7284	brdaly@deloitte.com
Kenneth DeJarnette	San Francisco, U.S.A.	Deloitte & Touche LLP	+1 415 783 4316	kdejarnette@deloitte.com
Gerry Fitzpatrick	Dublin, Ireland	Deloitte & Touche, Ireland	+353 1 417 2645	gfitzpatrick@deloitte.com
Valerie Flament	Paris, France	Deloitte & Associés	+33 1 40 88 2464	vflament@deloitte.fr
Abhay Gupte	Mumbai, India	Deloitte Haskins & Sells	+91 22 5667 9405	agupte@deloitte.com
Marcel Labelle	Montreal, Canada	Deloitte & Touche LLP	+1 514 393 5472	marlabelle@deloitte.ca
Danny Lau	Hong Kong, China	Deloitte Touche Tohmatsu	+852 2852 1015	danlau@deloitte.com
Donald McColl	Toronto, Canada	Deloitte & Touche LLP	+1 416 601 6373	dmccoll@deloitte.ca
Alfonso Mur	Madrid, Spain	Deloitte Touche Tohmatsu	+34 91 514 5000 x2103	amur@deloitte.es
David J. Pike	Zurich, Switzerland	Deloitte AG	+41 44 421 6401	djpike@deloitte.com
Juan Miguel Ramos	Madrid, Spain	Deloitte, S.L.	+34 91 514 5000 x2107	juramos@deloitte.es
Francois Renault	Paris, France	Deloitte & Associés	+33 1 55 61 61 22	frenault@deloitte.fr
Ted DeZabala	New York, U.S.A.	Deloitte & Touche LLP	+212 436 2957	tdezabala@deloitte.com
Rob Stout	Amsterdam, Netherlands	Deloitte Touche Tohmatsu	+31 20 582 4040	Rstout@deloitte.nl
Ioannis Tzanos	Athens, Greece	Deloitte Touche Tohmatsu	+30 210 678 1100	itzanos@deloitte.gr
Chris Verdonck	Brussels, Belgium	Deloitte Touche Tohmatsu	+32 2 800 2420	cverdonck@deloitte.com
Julie Priest	Sydney, Australia	Deloitte Touche Tohmatsu	+61 2 9322 7171	tfviljoen@deloitte.com.au
Stefan Weiss	Frankfurt, Germany	Deloitte & Touche GmbH	+49 40 320 804 674	stefanweiss@deloitte.de
Mike Maddison	London, UK	Deloitte & Touche LLP	+44 20 7303 0017	mmaddison@deloitte.co.uk

The scope of this survey was global, and, as such, encompassed financial institutions with worldwide presence with head office operations in one of the following geographic regions: North America; Europe, Middle East, Africa (EMEA); Asia Pacific (APAC); and Latin America and the Caribbean (LACRO). Attributes such as size, global presence, and market share were taken into consideration. Due to the diverse focus of institutions surveyed and the qualitative format of our research, the results reported herein may not be representative of each identified region.

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

Deloitte Touche Tohmatsu makes no representation as to the sufficiency of these survey results for your purposes. Reported survey findings should not be viewed as a substitute for other forms of analysis that management should undertake, and is not intended to constitute legal accounting, tax, investment, consulting or other professional advice or services. Prior to making decisions or taking action that might affect your business; you should consult a qualified professional advisor. Your use of these survey results and information contained herein is at your own risk.

Deloitte Touche Tohmatsu will not be liable for any direct, indirect, incidental, consequential, punitive damages or other damages, whether in an action of contract, statute, tort (including, without limitation, negligence) or otherwise, relating to the use of these survey results or information contained herein. These survey results and the information contained in this report are provided "as is," and Deloitte Touche Tohmatsu makes no express or implied representations or warranties regarding the results or the information.

For more information on the Global Security Survey, please contact your local Deloitte Touche Tohmatsu professional listed on the inside back cover of this publication.

About the Global Financial Services Industry Group

Deloitte Touche Tohmatsu's Global Financial Services Industry group consist of the Financial Services practices organized in the various Deloitte member firms. There are dedicated Financial Services member firm practices in more than 40 countries, employing over 1,500 partners and 17,500 financial services professionals between them. For more information on the Global Financial Services Industry group, visit www.deloitte.com/gfsi.

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 150 countries.

With access to the deep intellectual capital of 120,000 people worldwide, Deloitte delivers services in four professional areas-audit, tax, consulting, and financial advisory services-and serves more than one-half of the world's largest companies, as well as large national enterprises, public institutions, locally important clients, and successful, fast-growing global growth 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.

© Deloitte Touche Tohmatsu 2006. All rights reserved.

Designed and produced by The Creative Studio at Deloitte, London. 15014B.

Item # 6108