

**Deloitte.**



Protecting what matters  
The 6th Annual Global  
Security Survey

# Contents

---

Foreword	1
Objective of the survey	2
The value of benchmarking	3
Who responded	4
Geographic segmentation observations	6
Key findings of the survey	9
Governance	12
What the CISO is responsible for?	14
Risk	28
Use of security technology	34
Quality of operations	38
Privacy	46
How DTT's GFSI Practice designed, implemented and evaluated the survey	50
Helpful references and links	52
Acknowledgements	54
Survey development team	54
Contributors	54
Contacts	55

---

# Foreword

Welcome to the sixth annual Deloitte Touche Tohmatsu (DTT) Global Financial Services Industry (GFSI) Practice information security survey. Every year that the DTT GFSI Practice – made up of Deloitte member firm Financial Services Industry practices – conducts the survey, we marvel at the developments that have occurred over the past year. While many of the categories and initiatives that survey respondents talk about stay the same from year to year, the face of them often changes – sometimes dramatically. There is never a dull moment!

The top two security initiatives in 2007 were “*identity and access management*” and “*security regulatory compliance*.” In 2008, they merely switched spots. While the initiatives have not changed, it seems that each year they need to be addressed with a more sophisticated and far-reaching solution.

It is no surprise that compliance with regulation and/or industry guidelines was the top initiative in 2008. The compliance initiative encompasses not just the “what” (being compliant) but also the “how” (a compliance approach that is thorough, cost-effective, and adaptable to increasing regulation). Year 2007 saw the worst credit card data breach ever and it stands as the prime example of what can ensue when an organization is exposed. The organization in question was a retail group subject to the Payment Card Industry’s Data Security Standards and had been told by its assessors that weak Wireless Encryption Protocol (WEP), missing software patches and poorly configured firewalls made them noncompliant. In a Securities and Exchange Commission filing, the retail group admitted to transmitting data to banks “without encryption.”

*Identity and access management* is one of the key initiatives on the front line of the never-ending battle between good and bad. Its face is changing constantly. It meant something last year and this year it means something entirely different. Every year, hackers’ techniques get slicker and more innovative. When a phishing/pharming attempt gets old and stale and recognized, there is another one – encompassing a whole new level of technological smarts – waiting in the wings. The innovation that powers the technology industry also causes a constant headache for those who must figure out how to protect information.

Organizations encourage their workforces to be constantly connected, more productive, and immediately responsive and the market responds with tools to help them to do this. These tools, rolled out at an increasing pace, present a whole new slew of security issues. The media adds to the urgency by revealing potential security glitches and the scenarios that might ensue, e.g., a million mobile phones simultaneously dialing a company’s head office as a result of a software glitch. As well, there is no shortage of sensationalist media coverage for high-profile events, like the rogue futures trader who contributed to losses of over US\$7 billion dollars announced by a major European financial services company.

A major focal point, people continue to be an organization’s greatest asset as well as its greatest worry. That has not changed from 2007. What has changed is the environment. The economic meltdown was not at its peak when respondents took this survey. If there was ever an environment more likely to facilitate an organization’s people being distracted, nervous, fearful, or disgruntled, this is it. To state that security vigilance is even more important at a time like this is an understatement.

Those of us in the security industry know that an organization’s best defense against internal and external breaches is not technology alone. It is a culture of security within an organization – a mindset on the part of every individual so that actions in support of information security become automatic and intuitive.

From the creation of the survey questions to the production of this document and everything in between, this undertaking requires time, effort, detailed attention and, most of all, participation. I want to thank the Chief Information Security Officers, their designates, and the security management teams from financial services institutions around the world who participated in this survey.

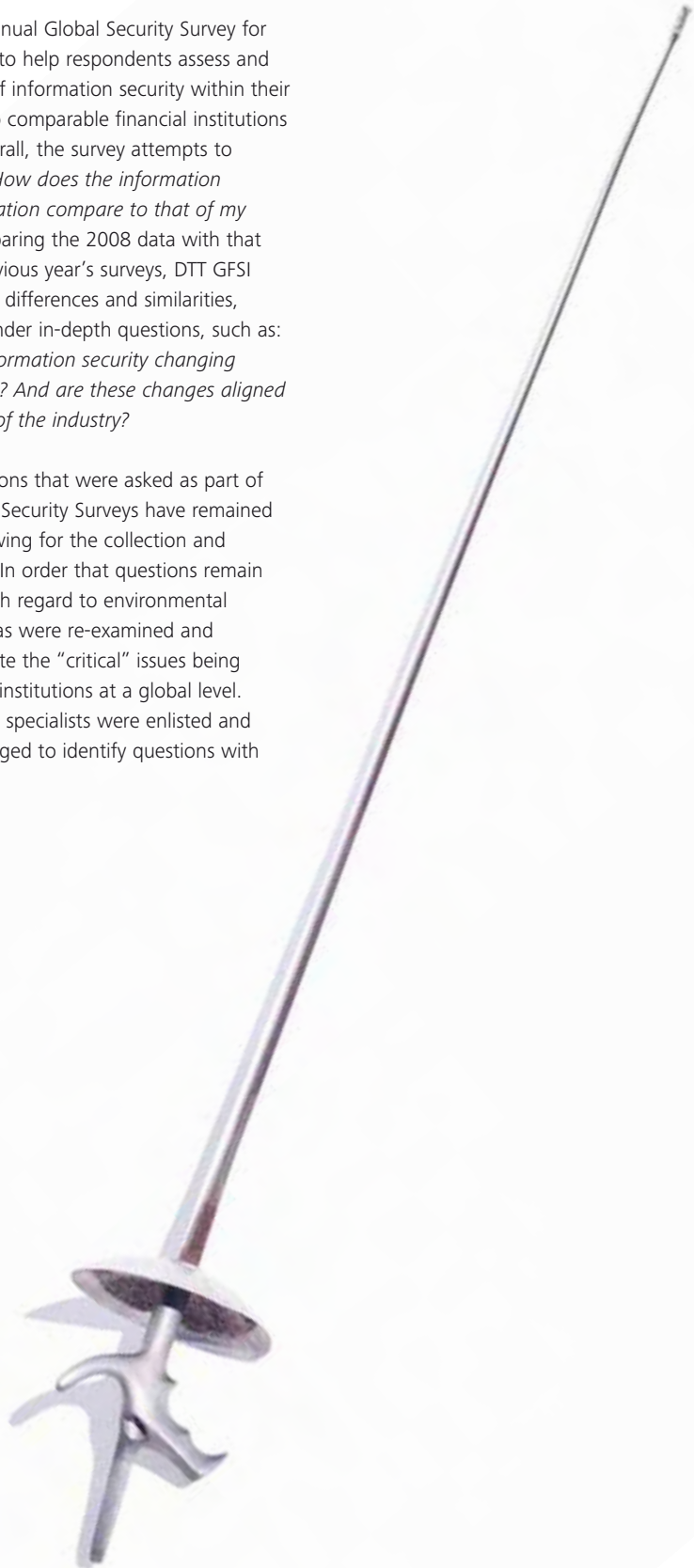


**Adel Melek** – Global Leader, Security & Privacy Services  
Global Financial Services Industry Practice  
Deloitte Touche Tohmatsu

# Objective of the survey

The goal of the 6th Annual Global Security Survey for financial institutions is to help respondents assess and understand the state of information security within their organization relative to comparable financial institutions around the world. Overall, the survey attempts to answer the question: *How does the information security of my organization compare to that of my counterparts?* By comparing the 2008 data with that collected from the previous year's surveys, DTT GFSI Practice can determine differences and similarities, identify trends and ponder in-depth questions, such as: *How is the state of information security changing within an organization? And are these changes aligned with those of the rest of the industry?*

Where possible, questions that were asked as part of the 2004-2007 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 "critical" issues being addressed by financial institutions at a global level. Deloitte subject matter specialists were enlisted and their knowledge leveraged to identify questions with these critical issues.



# The value of benchmarking

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

## Areas covered by the Survey

It is possible that an organization may excel in some areas related to information security, e.g., investment and responsiveness, and fall short in other areas, e.g., value and risk. In order to be able to pinpoint the specific areas that require attention, DTT's GFSI Practice 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.
- **Use of security technologies**  
Technology, Encryption, Knowledge Base, Trends.
- **Quality of operations**  
Business Continuity Management, Benchmarking, Administration, Prevention, Detection, Response, Privileged Users, Authentication, Controls.
- **Privacy**  
Compliance, Ethics, Data Collection Policies, Communication Techniques, Safeguards, Personal Information Protection.

## Survey scope

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

---

The Global Security Survey for financial institutions is intended to enable benchmarking against comparable organizations.

# Who responded

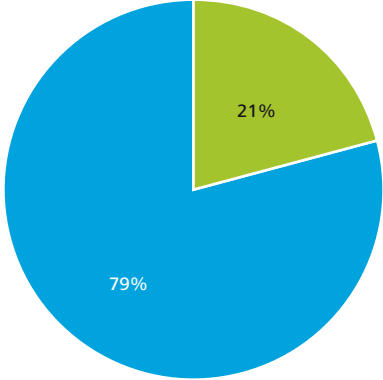
The 6th Annual Global Security Survey respondent data reflects current trends in security and privacy at a number of major global financial institutions. DTT's GFSI Practice agreed to preserve the anonymity of the participants by not identifying their organizations. However, DTT's GFSI Practice can state that, overall, the participants represent:

- Top 100 global financial institutions – 21% (based on assets value).
- Top 100 global banks – 21% (based on assets value).
- Top 50 global insurance companies – 14% (based on market value).
- Number of distinct countries represented – 32.

---

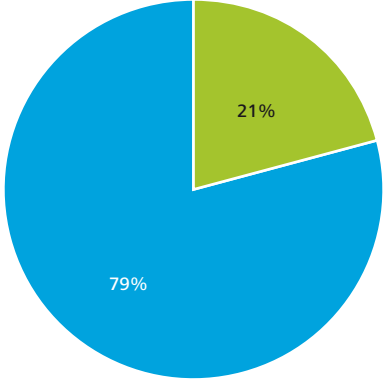
Respondent data reflects current trends in security and privacy at a number of major global financial institutions. DTT's GFSI Practice agreed to preserve the anonymity of the participants by not identifying their organizations.

**Top 100 global financial institutions (assets value)**



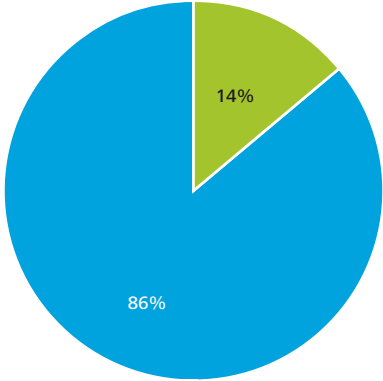
■ Top 100 global financial institutions ■ Other

**Top 100 global banks (assets value)**



■ Top 100 global banks ■ Other

**Top 50 global insurance companies (market value)**



■ Top 50 global insurance companies ■ Other

### Geographic region

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

Asia Pacific (APAC), excluding Japan	6%
Japan	9%
Europe, Middle East and Africa (EMEA)	48%
North America	18%
Latin America and the Caribbean (LACRO)	19%

### Industry breakdown

The final survey sample reflects all major financial sectors:

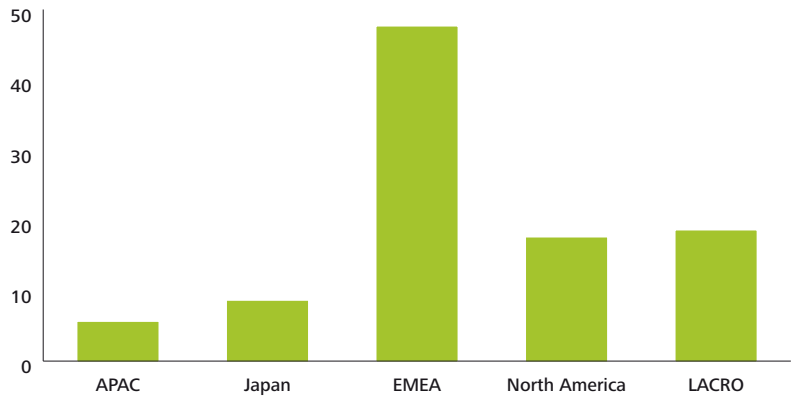
Banking	62%
Insurance	18%
Investment and securities	9%
Payments and processors	3%
Other	8%

### Annual revenue

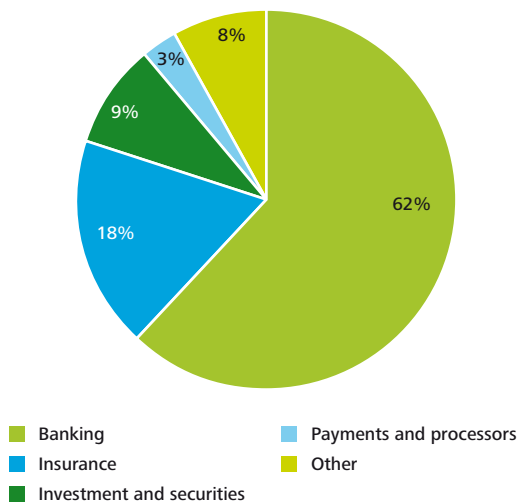
The respondent companies represent a broad spectrum based on annual revenues\*:

<\$1B in annual revenue	40%
\$1B-\$1.99B in annual revenue	7%
\$2B-\$4.99B in annual revenue	11%
\$5B-\$9.99B in annual revenue	3%
\$10B-\$14.99B in annual revenue	1%
>\$15B in annual revenue	13%

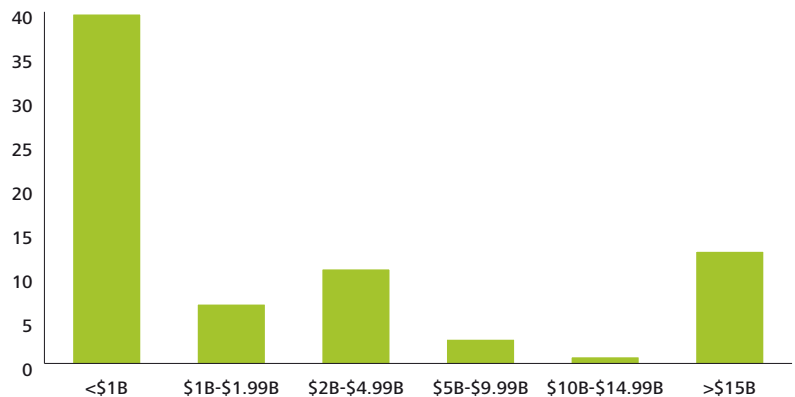
Geographic region (%)



Industry breakdown



Annual revenues (all currency stated in U.S. dollars)



\* Results may not total 100% as DTT's GFSI Practice is reporting selected information only; responses from those who decline to answer may not be included in the reported data.

# Geographic segmentation observations

Regional highlight	APAC (excl. Japan)	Japan	EMEA	North America	LACRO	Global
Respondents who feel that security has risen to executive management and/or the board as a key imperative	77%	79%	70%	63%	78%	72%
Respondents who feel they have both commitment and funding to address regulatory requirements	69%	65%	56%	58%	63%	59%
Respondents who indicated that they had a defined and formally documented information security strategy	62%	50%	64%	62%	68%	61%
Respondents who feel that information security and business initiatives are appropriately aligned	31%	30%	32%	28%	40%	32%
Respondents who indicate that their information security budget has increased	54%	25%	60%	65%	75%	60%
Respondents who indicated that their expenditures on information security were 'on plan' or 'ahead of requirements' based on the organization's current needs	31%	5%	50%	26%	59%	43%
Respondents who have incorporated application security and privacy as part of their software development lifecycle	38%	40%	26%	32%	41%	31%
Respondents who feel they presently have the required competencies to handle existing and foreseeable security requirements	23%	25%	41%	33%	33%	34%
Respondents whose employees have received at least one training and awareness session on security and privacy in the last 12 months	58%	90%	64%	82%	82%	72%
Respondents who have an executive responsible for privacy	23%	85%	58%	82%	24%	57%
Respondents who have a program for managing privacy compliance	38%	84%	43%	76%	18%	48%
Respondents who have experienced repeated internal breaches over the last 12 months	33%	17%	26%	27%	30%	27%
Respondents who have experienced repeated external breaches in the last 12 months	58%	17%	49%	51%	50%	47%

— Highest score

— Lowest score

## Introduction

In all geographic regions, we have observed that external breaches have fallen sharply over the past 12 months. This is not due to hackers giving up and finding other avenues to pursue but rather to the fact that organizations are getting more security-savvy, being less reactive and more proactive. We have said that hackers' methods are getting more sophisticated – the same is true of the technology designed to thwart them. The 2008 survey found that functional executives and business lines are more involved in the information security strategy than they did in 2007; but fewer companies are indicating that they have both the commitment and funding to address regulatory requirements. This shift may be due to the fact that executive management has a greater confidence that security initiatives are in hand and, therefore, do not warrant additional resources. There is a noticeable global decline in organizations who report that they have a program in place to manage privacy compliance (77% in 2007 has dropped to 48% in 2008).

## Asia Pacific (APAC) excluding Japan

Respondents from APAC indicate that they still have challenges in a number of areas and have experienced some regression from 2007. Only 7% of respondents in 2007 felt that they had the required competencies to handle existing and foreseeable security requirements. This percentage has risen to 23% in 2008, but is still the lowest response across all regions. Respondents who indicate that their employees have received at least one training and awareness session on security and privacy in the last 12 months has fallen to 58% in 2008 from 69% in 2007. This situation may also have contributed to APAC's breach track record, which is still the highest across all regions, although it has fallen from 2007. APAC respondents indicate that their organizations appear to place less emphasis on having an executive responsible for privacy – 85% had one in 2007; that number has fallen to 23% in 2008. And the obvious follow-on from this finding: while 100% of respondents felt that their organizations had a program for managing privacy compliance in 2007, only 38% feel the same in 2008. A bright spot for APAC is the fact that they have the highest confidence of respondents in all regions that they have both the commitment and funding to address regulatory requirements.

## Japan

Japan is unique when it comes to security breaches, with the lowest incidents of both internal and external breaches (17%) reported across all regions. A number of factors may contribute to this: the widespread use of strong authentication, the cultural importance of honour, the distinct language, and the culturally based reluctance to report security breaches. However, language and strong authentication alone are not responsible for the lowest amount of incidents – organizations in Japan clearly know how to protect themselves. An astounding 90% of employees have received at least one training and awareness session on security and privacy in the last 12 months. Privacy is a strong focus in Japan – respondents indicate that 85% have an executive responsible for privacy and 84% have a program for managing privacy compliance, numbers that make Japan "best in class" in this area across all regions. Security continues to rise to the executive management level – 79% in 2008 compared to 71% in 2007. But there are areas where Japan is not as strong. There has been a rather significant drop in the number of respondents who indicate the presence of a defined and formally documented information security strategy (from 75% in 2007 to 50% in 2008). Further, Japan has the lowest number of respondents across all regions (25%) indicating that their information security budget has increased and only 5% of respondents indicating that their expenditures on information security were 'on plan' or 'ahead of requirements' based on the organization's current needs. It would seem that, while respondents from Japan feel that their organizations are good at protecting the status quo, they recognize that they have a way to go as their organizations' security needs increase.

## EMEA

EMEA respondents indicate that they are confident that their security needs have been addressed – EMEA is the region that indicates the highest positive response regarding competencies to handle existing and foreseeable security requirements. However, the number of EMEA respondents whose employees have received at least one training and awareness session on security and privacy in the last 12 months (64%) is the second lowest score across all regions. This could mean that while EMEA organizations place a lot of reliance on their security staff (which accounts for the strong showing regarding competencies) they are missing an opportunity to engage their entire workforce as information security stewards by making them aware of industry best practices.

What may be a troubling indicator for EMEA for upcoming years is the finding that respondents who feel they have both commitment and funding to address regulatory requirements is, at 56%, the lowest of all regions and a rather significant drop from 77% in 2007.

EMEA respondents also indicate that 64% of their organizations have a formally documented and approved information security strategy. While this number is in line with the global average (61%), EMEA has become a crucial hub of the global financial services industry. The EU27 is the world's leading exporter of wholesale financial services, accounting for over 50% of the global total.\* One would expect that the number of organizations with an information security strategy would be much higher and that EMEA would be "best in class" of all regions.

Another finding about EMEA is that it ranks lowest of all regions in incorporating application security and privacy as part of the software development lifecycle (26% in 2008 and a drop from 33% in 2007). Also, when asked to characterize their secure application development directives, only 32% of EMEA respondents indicate that they are "well defined and practical", on par with North America (32%), but less than the global average (35%).

## North America

It appears that a focus on market conditions and the ensuing financial turmoil has forced executives in North America to start de-prioritizing security initiatives, which may well result in a downward trend in the coming years. Due to the current operating environment and shift in focus for many respondents, there is a significant drop in 2008 in the number of respondents who feel that security has risen to executive management and/or the board as a key imperative (63% in 2008 versus 84% in 2007\*\*). An organization derives real value from security and privacy initiatives when they become an integral part of the strategic plans of the organization. This finding is discouraging – and is, in fact, the lowest across all regions – because when the C-suite is no longer engaged, other areas suffer, e.g., budget, visibility. Not surprisingly, and in keeping with this finding, there is a very low perception on the part of most respondents that information security and business initiatives are aligned (again, the lowest of all regions at 28%). Surprisingly, external breaches are indicated by respondents as the second highest (51%) of all regions, even though they have fallen rather significantly from 2007 (78%\*\*\*). Where North American respondents indicate great strides – and proving they have taken notice of the fact that people are an organization's greatest asset and its greatest weakness – is in the area of internal breaches. Internal breaches have fallen to 27% in 2008 from 44% in 2007, the greatest drop across all regions but still well above Japan's "best in class" 17%.

## LACRO

LACRO is the very essence of a late bloomer. LACRO is "best in class" in five areas, topped only by Japan, and lowest in only one area. LACRO respondents indicate that their organizations are still best at having a defined security strategy (68%), but the really good news for LACRO is that everything is heading in the right direction: security budgets are increasing, security spending is on plan or ahead of requirements, and business and security initiatives are viewed as being appropriately aligned. If these trends continue, this will positively affect LACRO's information security stature. LACRO's repeated breaches are slightly higher than the global average, but if LACRO continues to do what it is doing, there is every indication that this situation will resolve itself.

\* "The Importance of Wholesale Financial Services to the EU Economy 2008", London Economics, July 2008, retrieved from <http://www.cityoflondon.gov.uk> on December 10, 2008

\*\* In the 2007 survey, we included individual findings for Canada and the U.S. This year, there is a single aggregate finding for both Canada and the U.S. defined as North America.

\*\*\* This finding is consistent with a study by the Identity Theft Resource Center (ITRC), which found that in the U.S. during 2008, data breaches were up by 47%. The ITRC study was conducted late in 2008, when the full impact of the financial crisis was being felt. Of the 656 data breaches the study reported, only 78 affected financial institutions. The ITRC confirms that the financial industry has remained the most proactive in terms of data protection.

"US financial institutions hit by 78 reported data breaches last year", Finextra.com, retrieved from <http://www.finextra.com/fullstory.asp?id=19525> on January 15, 2009.

# Key findings of the survey

## 1. Top five security initiatives: two familiar faces and a newcomer

In 2007, “identity and access management” and “security regulatory compliance,” were the top two security initiatives; in 2008 they have simply switched places. Identity and access management are tied in second place with a newcomer, “data protection and information leakage,” which was not even in the top five in 2007.

The choice of security regulatory compliance as the top priority reflects the fact that many organizations are struggling with the right way to handle the multiple legal and regulatory requirements as well as those of auditors. As budgets get tighter, the focus is on how to address compliance from a cost and risk perspective. In other words, companies are trying to figure out how to close the gaps with the highest risk, leverage solutions across multiple requirements, and streamline reporting. Clearly, the ideal solution is one that is sustainable and can accommodate increased regulation. Although being compliant does not make an organization more secure, being more secure is likely to make an organization compliant.

Given the highly profiled rogue-trading and rogue IT activities of this year, it is no surprise that identity and access management continue to be a top priority. A well regarded European financial services company, headquartered in France, announced at the beginning of 2008 that the actions of a single futures trader had led to losses of over US\$7 billion dollars. The trader in question had exceeded his authority by engaging in unauthorized trades totaling more than the bank’s entire market capitalization of US\$52.6 billion. Balancing convenient access (both for customers and employees) with strong security will be an issue that organizations must continue to deal with.

Although data protection and information leakage is a new top five initiative in our 2008 survey, it has already been front and center for months. The worst credit card breach in history (which was not public information when respondents participated in 2007 security survey) brought data protection and information leakage into the foreground and put companies on notice. As with previous years, the trend with security is less on infrastructure and perimeter-strengthening and more on preventing information from being leaked internally.

This shift reflects the effect of major media incidents, as well as the increasing proliferation of smaller yet feature-rich mobile media and the potential they present for data leakage. Since the focus of end-user technology seems to be always toward smaller, thinner, lighter, with greater capacity and processing power, the protection of information on the move will be a continuing focus for organizations. In addition, part of the increasing visibility of this issue is a result of new requirements around breaches – since organizations are now required to report breaches, they now need to have the capability to identify them within a reasonable timeframe. Data leakage protection is the second most cited technology being piloted by respondent organizations. All these factors mean that incident reporting will become more accurate, increasing visibility and heightening awareness even further.

People continue to be an organization’s greatest asset as well as its greatest risk. The economic turmoil in the U.S. – and its global repercussions – had not yet reached its peak when questions in this survey were posed to respondents. Organizations should remain aware of the effect that an unsettled financial environment can have on its workforce – employees may be disgruntled, worried, and otherwise distracted. In hard economic times, security vigilance is all-important.

Identity theft, data loss, and information leakage are now a mainstream concern. Organizations recognize, and try to offset, the human frailty of their workforces, who are more mobile, more flexible and more laden with technological tools than ever before. The focus is now on education and access control as well as leakage prevention tools.

Security infrastructure improvement moved into the top five priorities in 2008. An incident that underscores the importance of security infrastructure improvement is the recent alleged highjacking of a major U.S. city network by one of its network administrators. The administrator allegedly locked out the city from its FiberWAN network and then refused to hand over passwords to the Wide Area Network system until his demands were met.

As tempting as it is to save money in hard economic times, security infrastructure short-cuts are not the way to do it. Attacks are bound to increase when organizations let their guard down with “cost saving” measures that don’t have adequate controls built in.

## 2. The evolution of the CISO

In 2008, more organizations have a Chief Information Security Officer (CISO) than ever before (80% versus 75% in 2007), and 7% have more than one CISO. The incidence of CISOs reporting to various positions within the C-suite is an increasing trend in 2008: 33% report to the CIO (31% in 2007), 11% report to the CEO (9% in 2007) and 3% to the CSO (same as in 2007).

The CISO role is now more focused on security governance, strategy and planning, internal security awareness, and incident response (in 2007 strategy and planning was first, followed by security governance and security implementation and integration). There is greater evidence of gradual convergence via risk councils (47% combined versus 23% in 2007 report having gone through some form of convergence, 19% via risk councils). Risk councils bring together various areas of the organization to discuss security and risk issues. These factors all appear to be positive for the visibility and stature of the CISO role.

The majority of CISOs still report to the CIO (33%) or to some other technical role: IT Executive (13%), CTO (6%), CSO (3%). As much as CIOs are part of the C-suite, this reporting relationship means that security is still projected as mainly an "IT issue." It may mean that there is limited potential for greater visibility of information security outside IT, a circumstance that may support IT's desire for potential integration with other key functions.

What is interesting is that as the CISO role is becoming more focused on security governance (87%), strategy and planning (80%), internal security awareness (73%) and incident response (62%), the CISO focus moves away from traditional areas such as web customers' administration, external security awareness and disaster recovery planning, and the protection of paper-based information. In 2008, although more and more information is being created in electronic format, paper is still the most prevalent medium for information, e.g., mortgage records in branches, banking information, etc. However, that finding does not necessarily mean that the CISO is neglecting this area of responsibility – the emergence of risk councils may well mean that, although security operations may be migrating to other areas of the organization, the CISO, as part of the risk council, remains informed.

Taking its rightful spot in the top five responsibilities of the CISO is security incident response and management. "Management" of incidents means not just reporting them but also debriefing management in a post mortem or root cause analysis to answer key questions such as, *how could this have happened?* and *how could it have been avoided?*. Effective incident response and subsequent demonstration of measures to avoid reoccurrence is a sure-fire way to demonstrate alignment of security objectives with those of the business.

## 3. The evolution of the information security function

Every year the information security function continues to evolve. The increasing use of risk councils, admittedly a small step toward total convergence, is evidence of this.

It is interesting to note that respondents state that the biggest barrier to information security is "budget constraints and lack of resources." This is, no doubt, the prevailing lament of most functions, not just IT security, particularly in hard economic times. The fact that the IT security function's biggest barrier is now the universal complaint of most functions – and not the far more ominous "lack of management support", shows that the function is evolving in the right direction.

Prioritization of initiatives, having a clear business case, articulating the need for, and the impact of, security will now be reality for security functions, just as it has been for the rest of IT and the rest of the business for some time.

Another key driver of the evolution of the security function is regulation. As the Enterprise Risk Management (ERM) practices of the organization grow increasingly important – Standard & Poor's recently announced that they will review the quality of ERM as a new component in their reviews of credit ratings\*, the information security function must have a security reporting structure that reflects its importance to the compliance of the organization.

The percentage of respondents who indicate that their CISO reports to a security committee has risen in 2008 (9%) compared to 2007 (5%). Nevertheless, this percentage is still low and does not fully represent the governance potential of security committees.

\* BusinessFinanceMag.com, "S&P Rolls Out ERM Review", by John Cummings, May 13, 2008. Retrieved from <http://businessfinancemag.com/article/sp-rolls-out-erm-review-0513> on December 08, 2008.

A security committee is typically made up of representatives of functions from across the organization and allows the security function to increase its visibility across business lines and functions and better align itself with the strategic priorities of the organization.

#### 4. The information security strategy

Respondents indicate that 61% of organizations have a security strategy and 21% have one in draft form. But what is important is not just that a strategy exists in document form but rather, how the document was created and how it is being used. For example, what level of input was sought from executives and business when the document was being created? Does the organization use the document, i.e., embrace its policies? What was the quality of the input that formed it? Has the strategy translated into benefits, such as closer alignment with the business and positive feedback? Is there reporting on the effectiveness of the strategy?

As they did in 2007, companies in 2008 still appear to struggle with the definition of a security strategy and what the strategy should include. Essentially, an information security strategy is a plan as to how the organization can mitigate risks while complying with legal, statutory, contractual, and internally developed requirements. Yet only 63% of the respondents who maintain that their organizations have an information security strategy indicate that they have identified their information security strategy requirements. Only 45% have a people strategy, which is low given that many face issues with finding qualified resources. Only 40% have included metrics and performance management, which are needed to help ensure that what is being done is meeting the expectations of business. And only 63% indicate that they have aligned their strategic objectives with the organization. Until these areas are addressed, and information security strategy becomes thoroughly understood and commonplace, puzzling discrepancies will continue to surface.

#### 5. Identity and access management

"Identity and access management" was the number one initiative that respondents mentioned in 2007 survey; in 2008, it is number two. We expect that it will remain in front for years to come. The reason is because the identity and access management onslaught to the organization continues from all sides. There is increasing regulation. There are increasing industry guidelines. There are more mobile workers than ever before using more devices than ever before, such as BlackBerrys, PDAs, laptops, and iPhones. There are more suppliers, business partners, and other outsiders who need secure access to the organizations' systems.

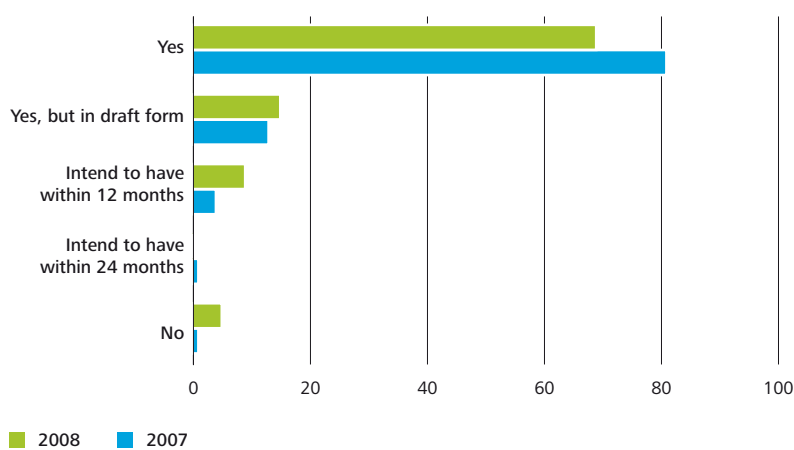
"Excessive access rights" was stated by respondents as the top "internal/external audit finding over the past 12 months." "Unauthorized access to personal information" was stated as the number one concern from a privacy perspective. Identity and access management must constantly be enhanced to reflect the state of flux. Future-state identity and access management will include enhancements such as an automated process that gives out application access and then knows immediately when an employee has left the organization and revokes that access; employee identities that are synchronized across all systems; a system that, instead of simply verifying who has a valid user name and password, also verifies whether the person needs to be accessing what they are attempting to access in the network.

Identity theft continues unabated in 2008. Those of us who believe that we are on to the tricks of identity theft scammers and already take the utmost precautions could be unpleasantly surprised by the sophistication of upcoming scams. The good news is that there is now improved communication among businesses, consumers, and law enforcement as to causes and possible solutions to reduce identity theft crimes. The level of awareness on the part of consumers grows every day. Organizations are deploying and piloting an increasing array of new technology. Security log and event management systems are, according to respondents, one of the key technologies being piloted over the next 12 months.

# Governance



Presence of a defined information governance framework (%)



## Governance framework

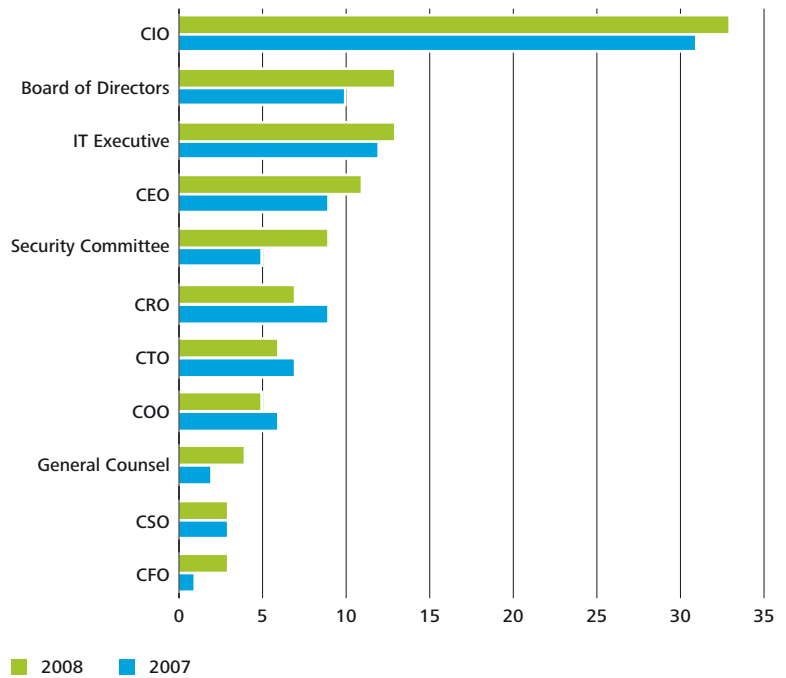
Organizations clearly recognize the link between strong security governance and effective information security – governance for security is one of the top five security initiatives in 2008. In 2007, organizations also appeared to recognize the importance of an established governance framework – 81% of respondents indicated that they had one. In 2008, however, that number dropped significantly to 69%. Does this mean that organizations are attributing less importance to the governance framework in 2008? This is unlikely, given the position of governance in the top five security initiatives. It is more probably a case of “a little knowledge is a dangerous thing.” As organizations become more security savvy and more informed, they recognize that an established governance framework is key to guiding the development and maintenance of a comprehensive information security program, and what they considered to be a framework in the past did not meet the definition of an effective governance framework.

## Reporting

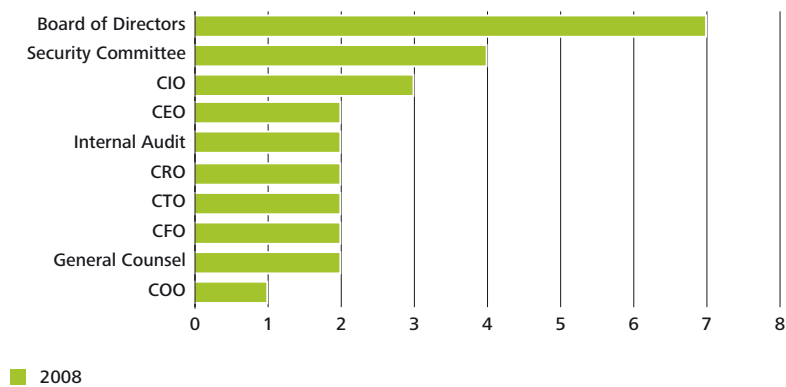
Eighty percent of respondents in 2008 indicate having a CISO or equivalent position on their corporate roster, and 7% have even more than one. The top four positions to whom the CISO reports – the CIO, the Board of Directors, IT Executive, and the CEO – either show a slight increase from 2007 or remain the same in 2008, indicating that the CISO role shows no signs of moving away from reporting to the C-suite. By far, the majority of CISOs report to the CIO, unchanged for the last three years of this survey. The CISOs still report in aggregate (50%) to predominantly IT-related positions: CIO, CTO, and IT Executive. The reality remains that the CISO position is still considered to fulfill a predominantly IT role.

In 2008, more CISOs report to a Security Committee, the fifth most-mentioned reporting line after the CIO, the Board of Directors, IT Executive, and the CEO. The greatest number of respondents indicate that the top indirect reporting position for CISOs is the Board of Directors, demonstrating that, just as it was in 2007, the issue of information security remains a C-suite and board-level concern.

Top direct reporting links (%)

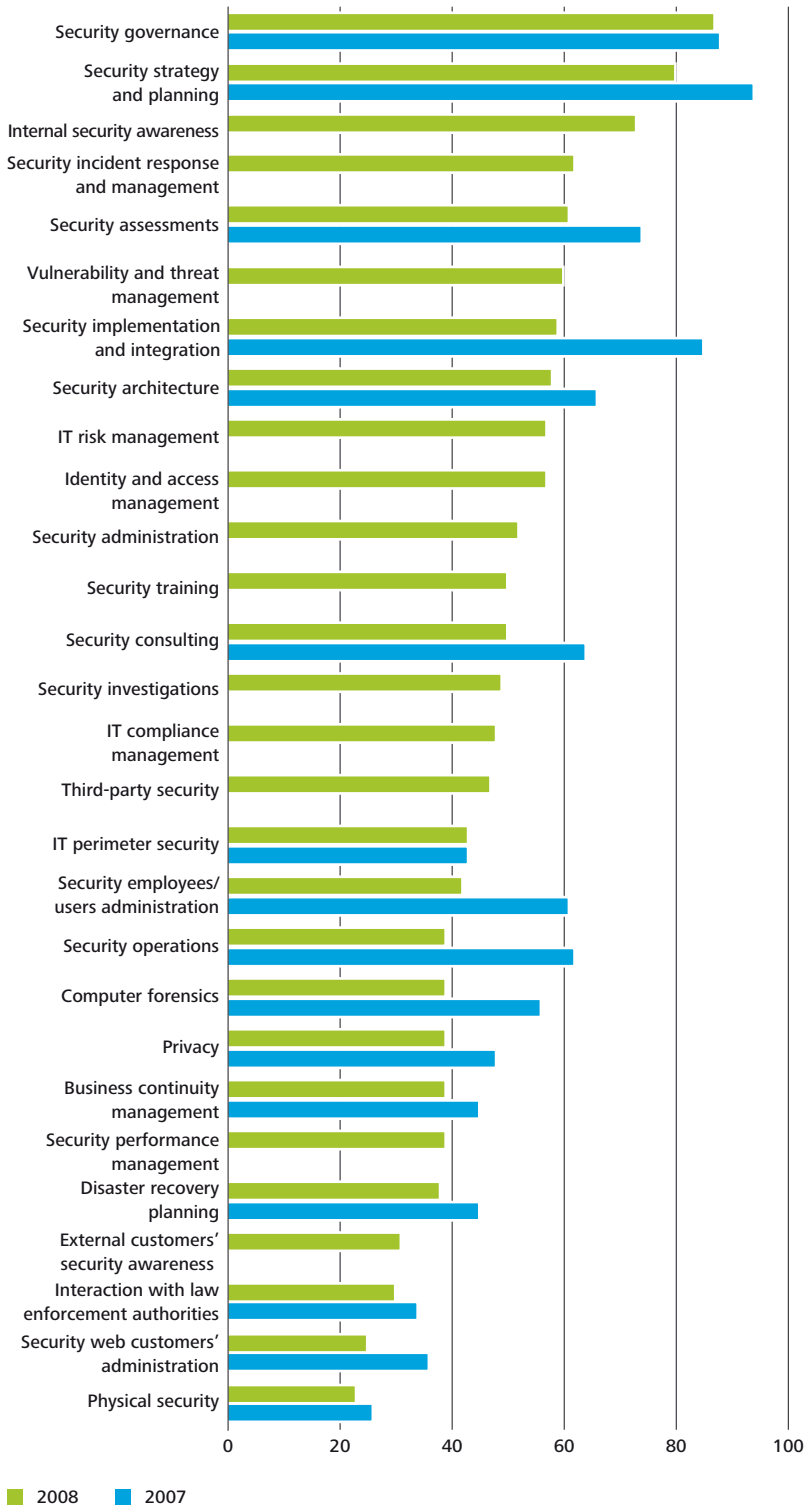


Top indirect reporting links (%)



# What the CISO is responsible for?

Top functions of CISO (%)



## Top functions

Survey respondents indicate that the CISO's primary responsibilities are security governance, strategy and planning, internal security awareness, security incident response and management, as well as security assessments (all rating at least 60%, with security governance as high as 87%). Respondents indicate that CISOs are least responsible for areas such as web customers' administration, external security awareness, disaster recovery planning, and the protection of paper-based information (all ratings less than 40%).

These findings do not mean that these latter areas are being necessarily neglected. For example, respondents indicate that the CISO is more concerned with internal security awareness (73%) than with external awareness (31%). This supports findings later in this survey that the internal workforce is an organization's biggest worry (36%) versus outsiders (13%). It is natural, then, that the CISO would focus on the areas of most concern. In addition, the emergence of risk councils may indicate that, while security operations are being handled by other areas of the organization, the CISO, as a member of the risk council, is still involved.

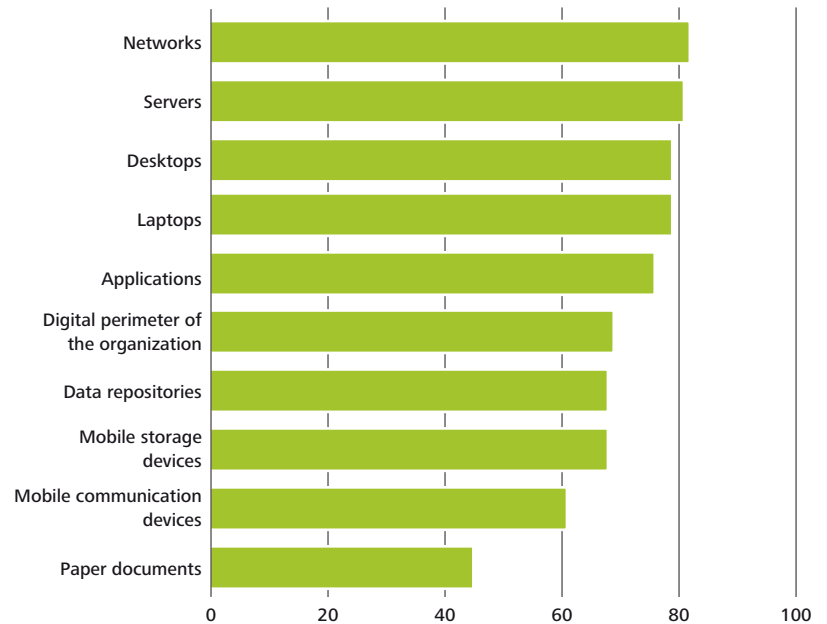
This year, respondents indicate that IT compliance management (at 48%) is part of the responsibility of the CISO. This is an important responsibility, given that organizations have identified security regulatory compliance as their primary security initiative in 2008.

Due to an expanded question set this year, responses that do not show comparisons to last year indicate that data was not collected for that question last year.

**Information assets**

Respondents indicate that the CISO’s chief responsibilities are networks, servers, desktops, and laptops. There is nothing surprising about this finding; it is the lower end of the chart that is more interesting. Only 45% of respondents include paper documents in the CISO’s mandate. Digital perimeter of the organization (69%), data repositories (68%), mobile storage devices (68%), and mobile communication devices (61%) also seem to be underrepresented. In many instances, some of these information assets (e.g., paper documents, data repositories) have not traditionally been included within the CISO’s mandate. However, as more organizations continue to expand their information security functions to include IT Risk Management, and as the respective leaders continue to adopt titles such as Information Security Officers, the question remains – are all information assets being appropriately managed?

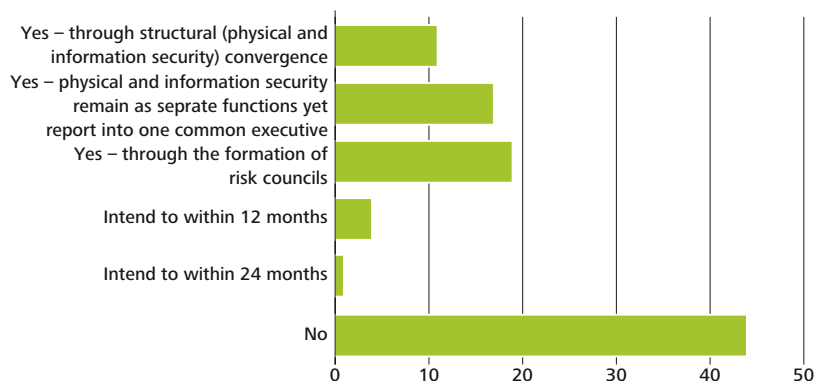
**Information assets the CISO is responsible for (%)**



**Convergence between logical and physical security**

As they did in 2007 (66%), a large number of respondents in 2008 (44%) indicate that there are no plans for their organizations to converge logical and physical security. However, convergence may typically be viewed by respondents as an “all or nothing” situation when, in fact, like any shift in thinking, small steps are required to move toward embracing the idea. These small steps were implied in the responses in 2008 and include information sharing through means such as risk councils (19%), common executives for separate functions (17%), and structural convergence for better coordination (11%), all evidence that convergence is gaining some traction. Geographically, respondents in EMEA, APAC, and Japan indicate the least resistance to convergence while those in North America and LACRO indicate the greatest. A greater number of respondents in 2008 state their intention to converge within 24 months. The reality is that while structural convergence of logical and physical security represents a radical change to the traditional structure of an organization, the survey indicates that there is a shift in thinking around the idea of convergence.

**Convergence between logical and physical security (%)**

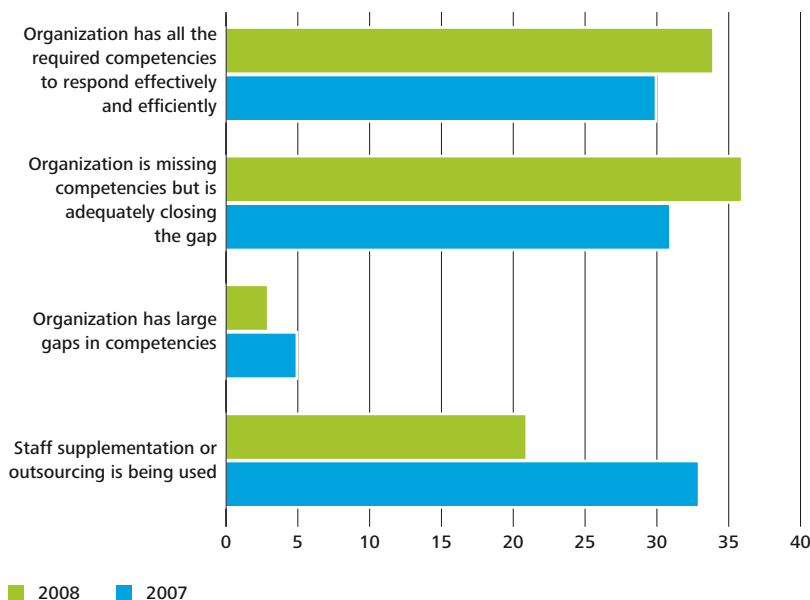


**Number of information security professionals**

FTEs* inside security function	
0	4%
1 to 50	85%
51 to 100	6%
101 to 150	2%
FTEs outside security function	
0	33%
1 to 50	50%
51 to 100	2%
101 to 150	1%
Over 400	4%
Outsourced/consultants FTEs	
0	35%
1 to 50	52%
51 to 100	2%

\*FTE – full-time employee

**Capability of security personnel (%)**



**Full-time employees**

The majority of respondents indicate that their security organizations have 1 to 50 FTEs (including all categories: internal, external, and outsourced/consultants). Thirty five percent of respondents indicate that their organizations do not have outsourced information security FTEs at all. In 2008, there is a slight increase in the number of respondents who indicate that their organizations “added resources” (45% in 2007 versus 48% in 2008). It is likely that this upward trend has been interrupted by the current economic crisis, which, at the time these questions were posed to respondents, had not reached its peak and continues to unfold.

**Capability of security personnel**

In response to the statement, “the organization has all the required competencies to respond effectively and efficiently to existing and foreseeable security requirements” the number of respondents who agree (34%) is relatively low. Although it is up from 2007 (30%), the difference is perhaps too small to conclude an upward trend. There is a similar gain over 2007 when respondents rate the statement, “the organization is missing competencies but is adequately closing the gap” (36% in 2008 compared to 31% in 2007). The good news here is that, despite the increasing sophistication of security threats, the competencies required to respond effectively (or to adequately close the gap) are increasing.

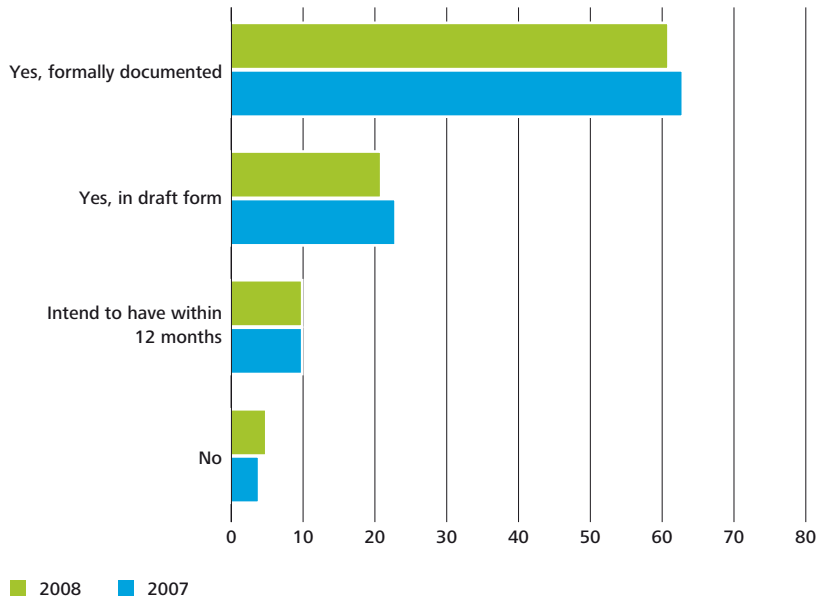
### Defined information security strategy

Respondents indicate that the presence of a defined information security strategy has not changed appreciably from last year (61% in 2008; 63% in 2007). There is also very little change in those who have one in draft form (21% in 2008; 23% in 2007) and no change in those who intend to have one in 12 months (10% both in 2008 and 2007).

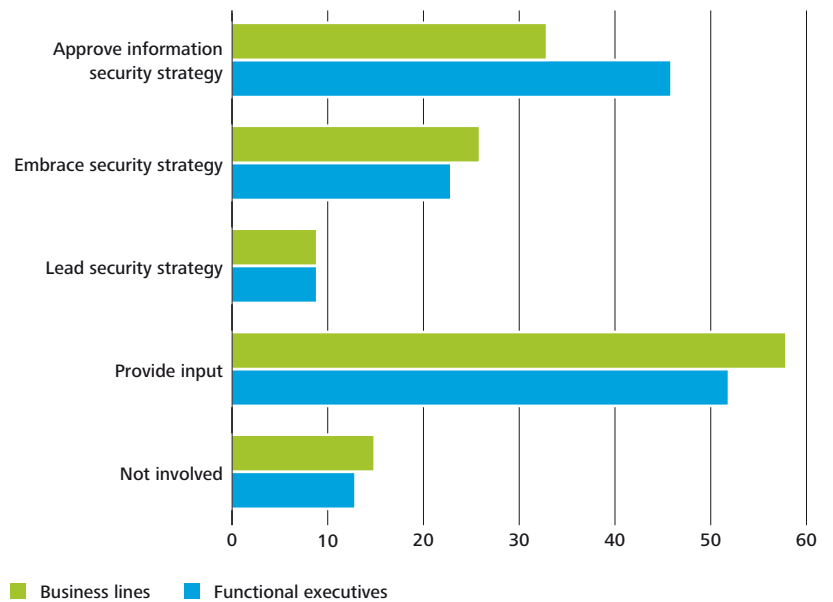
### Level of involvement in information security strategy

In just about every area regarding the information security strategy – providing input, approving it, and embracing it – functional executives and business lines have more involvement than they did in 2007. The biggest gains over last year come in the area of input to the security strategy (58% for business lines and 52% for functional executives in 2008 versus 39% combined in 2007) and in the area of buy-in or embracing it (26% and 23% in 2008 versus only 10% combined in 2007). Business lines and functional executives are now more likely to approve information for the security strategy (33% and 46% in 2008 versus 27% combined in 2007). Even though the presence of the information security strategy, either formally documented or in draft form, remains relatively unchanged from 2007, what has changed is the level of involvement with it on the part of functional executives and business lines. Why did it happen? One of the possible explanations is that functional executives and business lines are taking an extra step to correct increased perceived misalignment of business and information security initiatives. Increased executive involvement is a good thing for security function, as it is likely to increase chances of information security projects to get funding and ultimately succeed.

Presence of a defined information security strategy (%)



Level of involvement in information security strategy (%)



### Top security initiatives

It is no surprise that security regulatory compliance is the top security initiative. Organizations still grapple with how to handle legal, regulatory, and auditor requirements. There is the growing understanding that compliance and risk management processes have a direct effect on stock price. Standard & Poor's recently announced that they will review the quality of enterprise risk management (ERM) as a new component in their reviews of credit ratings for all listed companies.\* This development means a significant change in business leadership and performance management.

In 2008, data protection and information leakage – not even in the top five in 2007 – tied with the second place priority, identity and access management. This is understandable, given the incidents that have attracted media attention over the last year, including the largest hacking and identity theft case ever prosecuted by the U.S. Department of Justice. The targeted retail group admitted that some of their files were encrypted and some were not; the same applied to their data transmissions. But it would not have mattered anyway since the decryption tool was allegedly stored in the same location as the files, a common mistake according to industry analysts.

The spate of high-profile vulnerabilities in the form of high-capacity storage devices, such as USB keys or MP3 players and the growing popularity of social networking sites, such as Facebook and MySpace, continue to make data protection ever-more challenging. These mechanisms introduce opportunities to steal identities and gain access to confidential information. Since high-profile vulnerabilities will continue to proliferate, this aspect of information security will continue to grow in importance as an initiative.

### Major barriers to information security

Not surprisingly, budget constraints and the increasing sophistication of threats occupy the first two spots in 2008 (56% and 38%, respectively). Further, when the majority of questions in this survey were answered, respondents had not yet felt the full force of the current economic woes.

Surprisingly, “increasing sophistication of threats” was seen as less of a barrier in 2008 (38%) than in 2007 (49%). This result may well indicate that organizations are being better prepared to deal with them, attributable to the more widespread use of antiviruses and other security technologies. In addition, emerging technologies are also seen as less of a barrier in 2008 (27%) than they were in 2007 (36%). This may be due to the fact that as respondents become more familiar with the platforms of emerging technology, they feel that it is less of a barrier each year.

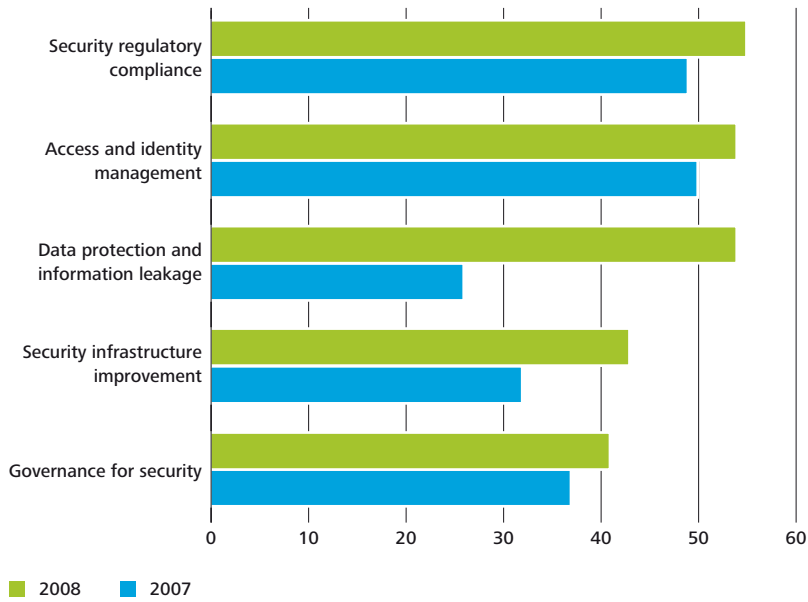
Predictably, lack of management support, a major lament in the early years of this survey, is far down the list of barriers in 2008 (only 15%).

### Return on information security investments

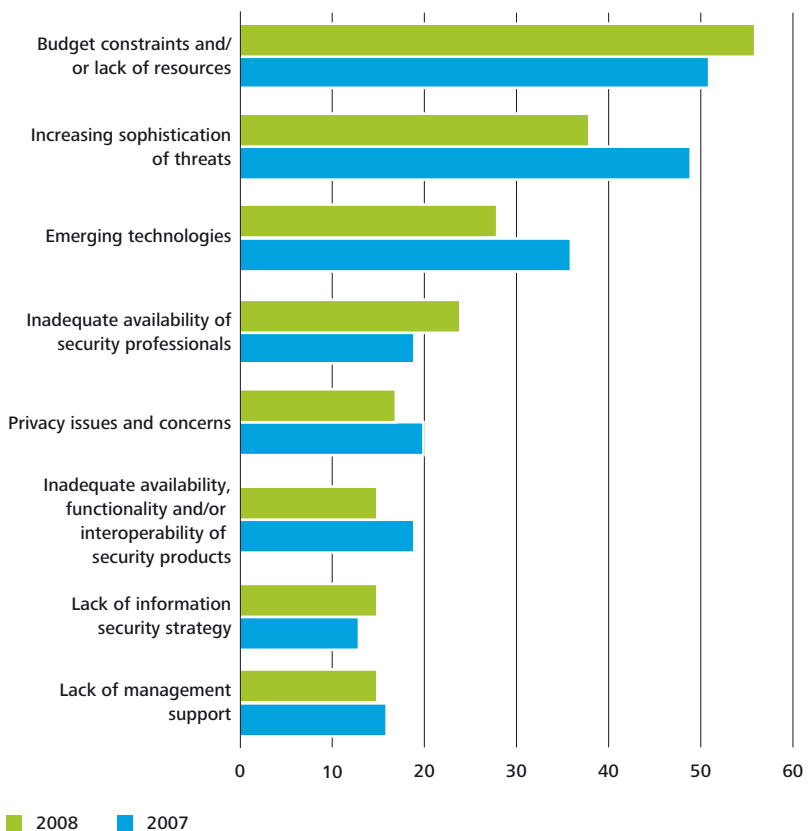
Respondents indicate that there is essentially, little, if any, measurement of return on information security investment. This may well be a factor of the speed at which information security needs to move and the agility that is required when threats warrant it. Measuring return on security investment becomes a relatively low priority when the first priority is to quickly thwart hackers at their own game and by whatever means are necessary. While 23% are working on establishing formal metrics (down from 34% in 2007), the overwhelming majority (62%) are split between “do not measure” and “little, if any, measurement.” However, the measurement of return on information security investments is a key factor in engaging C-suite executives for the necessary support and funding. Given the economic conditions, it is important to be able to justify the prioritization of initiatives.

\* BusinessFinanceMag.com, “S&P Rolls Out ERM Review”, by John Cummings, May 13, 2008. Retrieved from <http://businessfinance.com/article/sp-rolls-out-erm-review-0513> on December 08, 2008.

**Top five security initiatives of 2008 (%)**



**Major barriers in ensuring information security (%)**



### Reporting on information security status or security incidents

Respondents indicate that reporting to the Board of Directors, the Audit Committee, and the CEO is most frequently on an ad hoc basis, i.e., information reporting is not scheduled and, therefore, does not likely feed into business reporting.

A more encouraging sign would be that monthly (scheduled) reporting is in the second place for Board of Directors, CEO, and in the first place for senior and executive management. Moreover, monthly reporting to senior and executive management (at 30%) is higher than ad hoc reporting to all other areas.

#### Frequency of reporting on information security status or security incidents

	Board of Directors	Audit Committee	CEO	Senior and Executive Management
Weekly	2%	0%	2%	5%
Monthly	19%	13%	20%	30%
Quarterly	19%	19%	19%	17%
Semi-annually	7%	7%	4%	3%
Annually	11%	13%	6%	3%
Ad hoc	19%	24%	23%	24%
Never	10%	12%	9%	3%
Only when an incident occurs	9%	8%	11%	12%
Choose not to be informed	0%	0%	1%	0%

### Information security model structure

The biggest increase from 2007 in information security structure is the rise of the federated model (where a centralized group sets common standards and performs central functions while the business units maintain some control over “local” execution). The federated model is a hybrid of centralized and decentralized, employing the best characteristics of both. Twenty two percent of respondents in 2008 versus 13% in 2007 stated that they followed the federated model. In an age of increasing regulation and oversight, it is understandable that the decentralized model is losing ground. Predictably, the centralized model remains the traditional structure.

### Internal/external audit findings

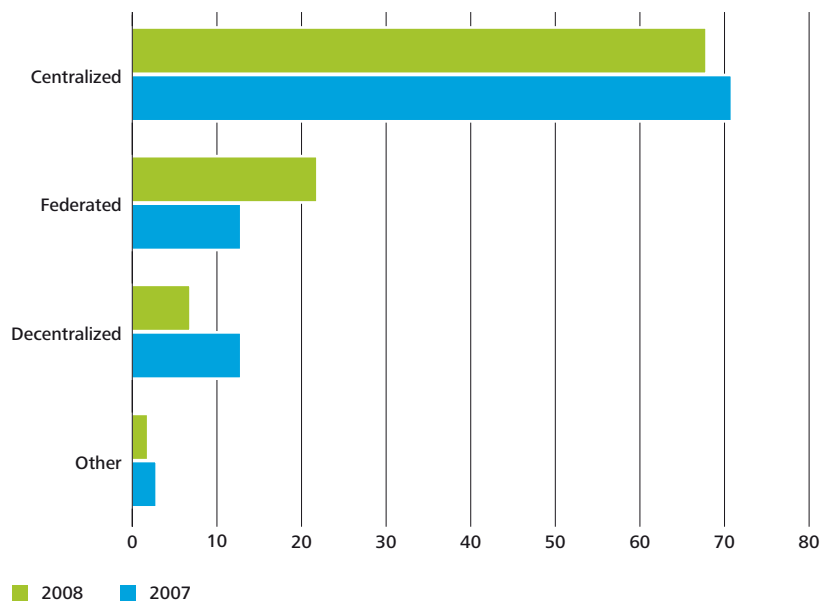
The most prevalent internal/external audit findings in the 2008 survey also reflect organizations’ top security initiatives, a good sign that there is little confusion as to what is a priority. Excessive access rights as the most prevalent audit finding, followed by access control compliance with procedures and segregation of duties, all reflect organizations’ concern about identity and access management, compliance, and data leakage protection.

These top three findings in 2008 were also the top three findings in 2007. Excessive access rights is cited by 31% of respondents, compared to 45% in 2007; access control and compliance with procedures is cited by 30% of respondents in 2008, compared to 29% in 2007; and segregation of duties ties with access control and compliance in 2008 (30%) compared to 35% in 2007.

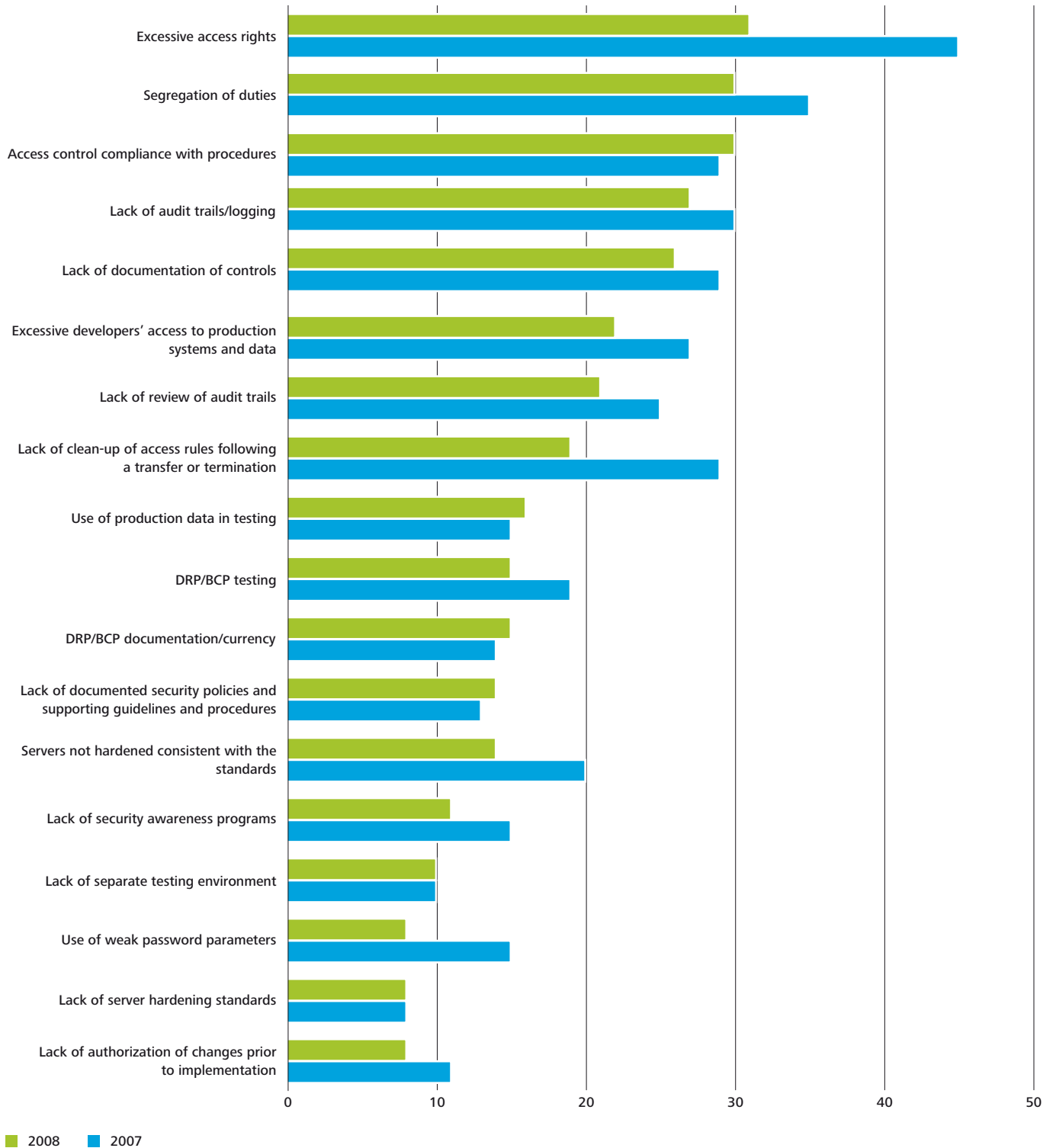
Excessive access rights is likely to be an important topic for some time. Auditors and regulators expect that individuals will have rights only to the data/information that are needed to perform their jobs. And when those rights are no longer needed to perform the job, they also expect the rights to be revoked. And “revoked” does not just mean at some point in the future – it means in a timely fashion. As simple as this sounds in theory, in practice, it is not. Given changing job responsibilities, a more mobile workforce, employee turnover, and corporate reorganizations and mergers, this is a tall order.

Access control compliance with procedures ties with segregation of duties (30%) as the second most prevalent audit finding. Access and control compliance reflects the security concern of many organizations of having controls in place to ensure users have access only to what they need to properly do their jobs. Auditors look for conflicts in segregation of duties in which one individual has access to responsibilities that are inherently in conflict with one another. To use a banking example, the same person should not accept cash, record deposits, make deposits, and reconcile the account. It is a lack of segregation of duties that allows some individuals to circumvent intended controls.

Information security model structure (%)



Top internal/external audit findings over the past 12 months (%)



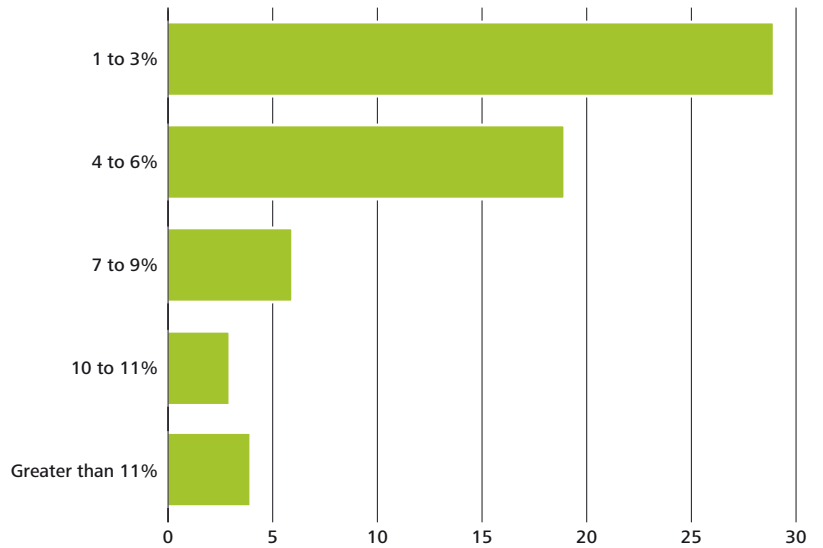
### Investment in information security

#### Percentage of IT budget dedicated to information security

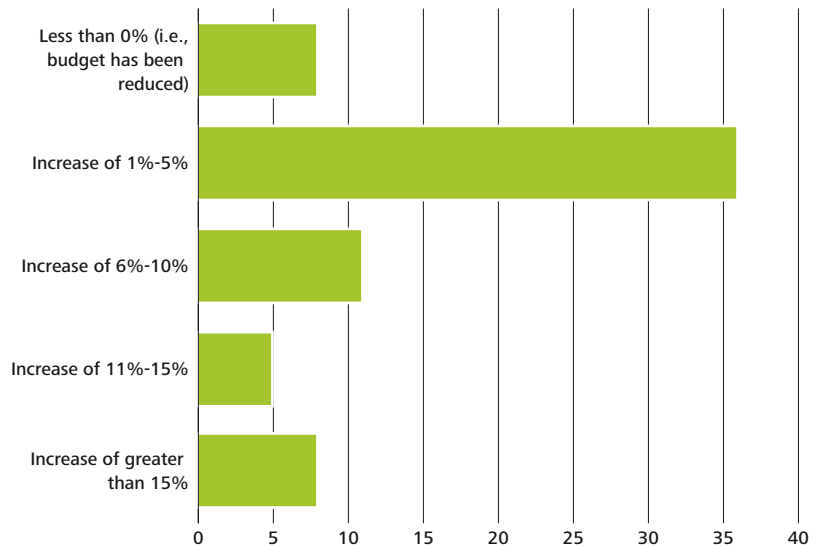
The percentage of IT budget dedicated to information security has not changed appreciably from 2007. The lowest percentage of IT budget (1% to 3%) remains the dominant category (29%). The situation is unlikely to change in the coming years – security technologies have moved into the mainstream, and all participants benefit from the effects of scale, which drive down the costs. While changes in regulations might demand new investments, keeping the infrastructure and technologies that are already in place up-to-date is a less expensive task than building everything from ground up. Increased automation will also help to ease the burden of security costs to global financial institutions.

The year-over-year trending for the security budget supports these numbers. Eight percent of respondents have had their security budgets reduced in 2008. Twenty nine percent of respondents in 2007 reported a security budget increase of over 15%; in 2008 their number dropped to 8%.

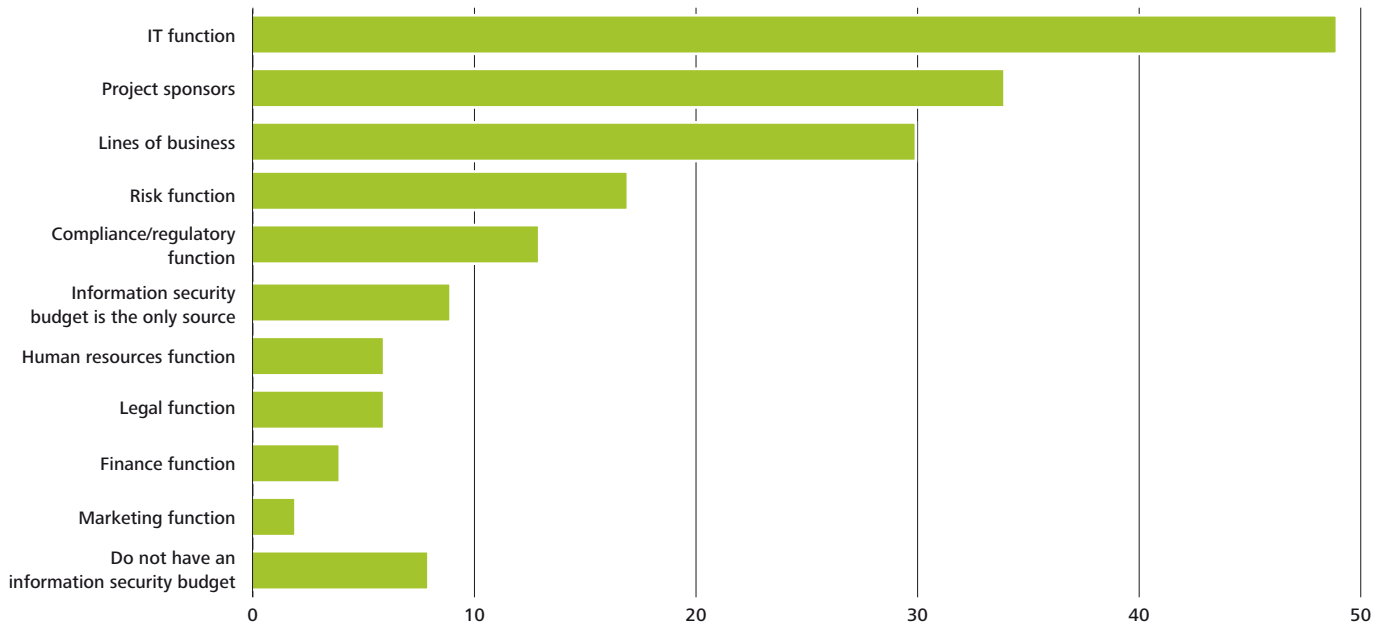
Percentage of IT budget dedicated to information security (%)



Year-over-year trending in information security budgets (%)



Additional information security funding (%)



---

By far, the biggest source of additional funding over and above the IT budget comes from the IT function (49%).

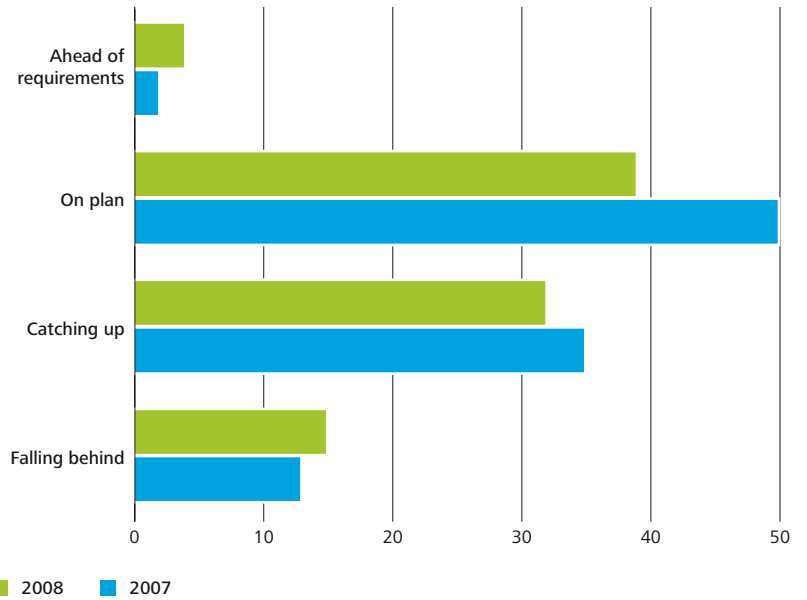
**Expenditures on information security**

Respondents in 2008 indicate a decrease in "On plan" and an increase in "Falling behind," a clear trend that projects are underfunded. This finding supports the reasons cited for "causes of project failure" (lack of resources) and "major barriers to information security" (budget constraints).

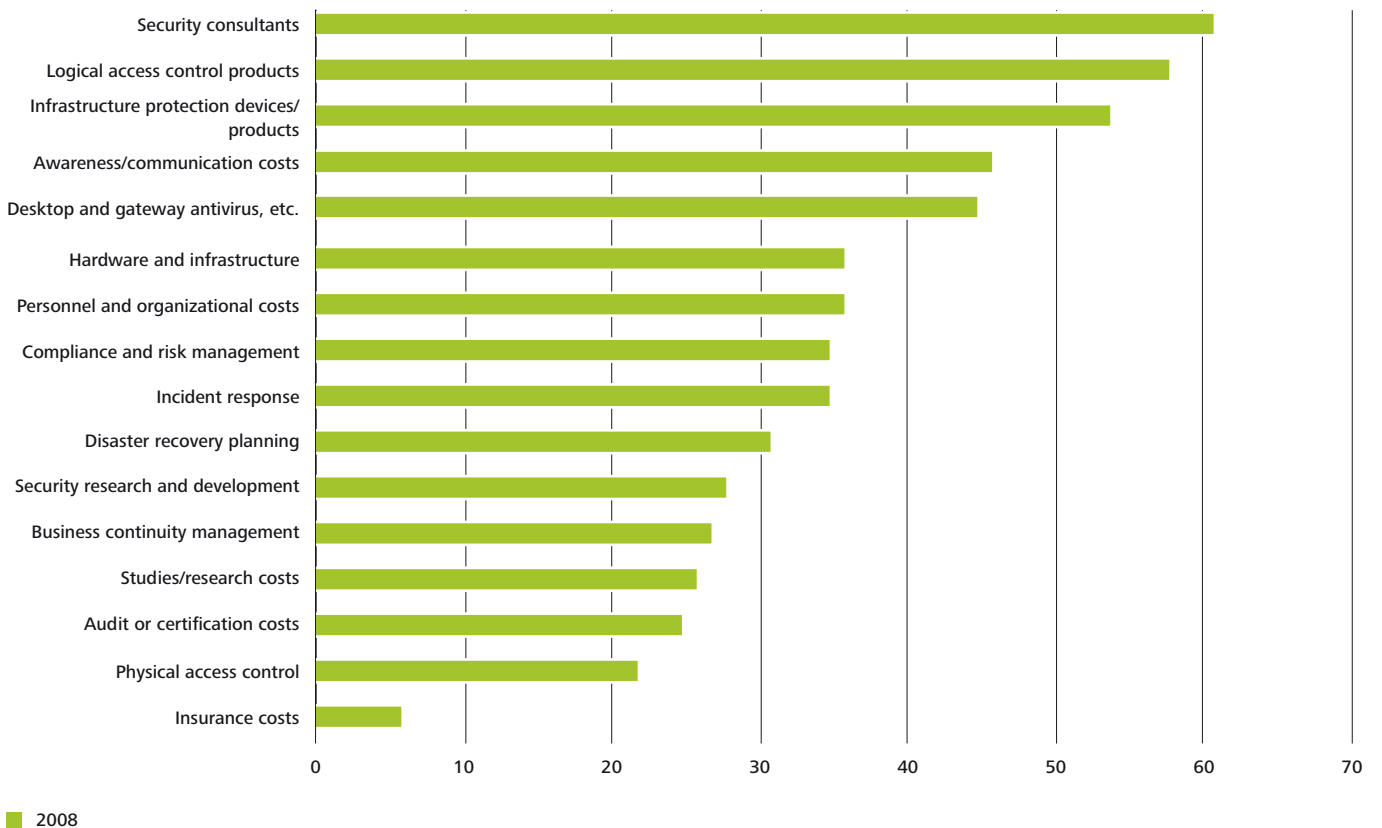
**What is covered under information security budget**

The most striking observation about what is covered under the information security budget is that key initiatives in 2007 – business continuity management and disaster recovery – have not only dropped out of the top five in 2008 but they are well down the list. They are low on the list of funding priorities as well. The top areas – consultants, access control products, and infrastructure protection devices – are all consistent with the top stated security initiatives for 2007.

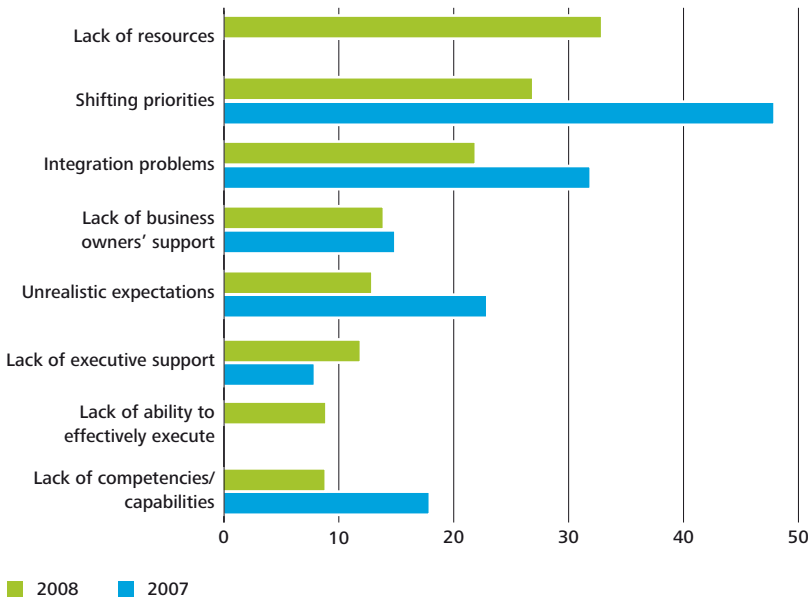
Expenditures on information security (%)



Information security budget segmentation (%)



Major causes of failure of information security projects (%)

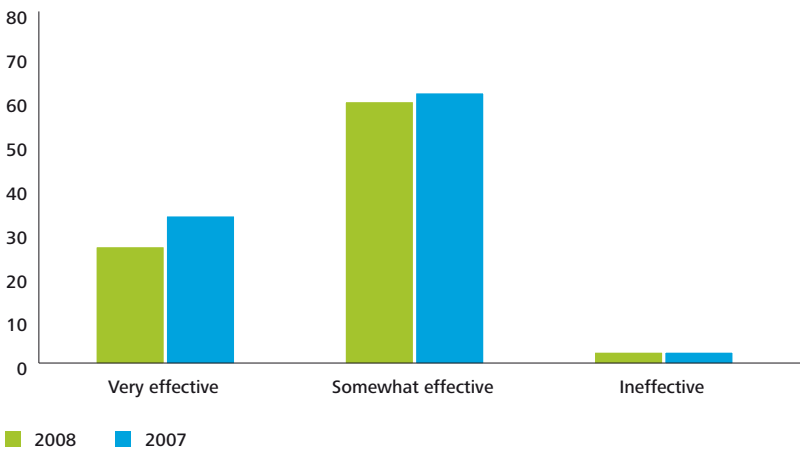


**Causes of information security project failure**

"Lack of resources" is cited as the number one cause of information security project failure. This is consistent with an earlier observation that budget restraints are the biggest barrier to information security. Despite the stated lack of resources – human nature being what it is, this will likely be an ongoing lament – there is some very good news here. "Shifting priorities" has fallen rather dramatically from the previous year (48% in 2007 to 27% in 2008) indicating that organizations are identifying, communicating, and agreeing upon priorities.

As to whether the information security function is meeting the needs of the organization, the "somewhat effective" category and the "very effective" category have both lost ground over the year. This is likely a reflection of the fact that as threats increase in sophistication (more sophisticated in 2008 than ever before), organizations struggle to keep up with them.

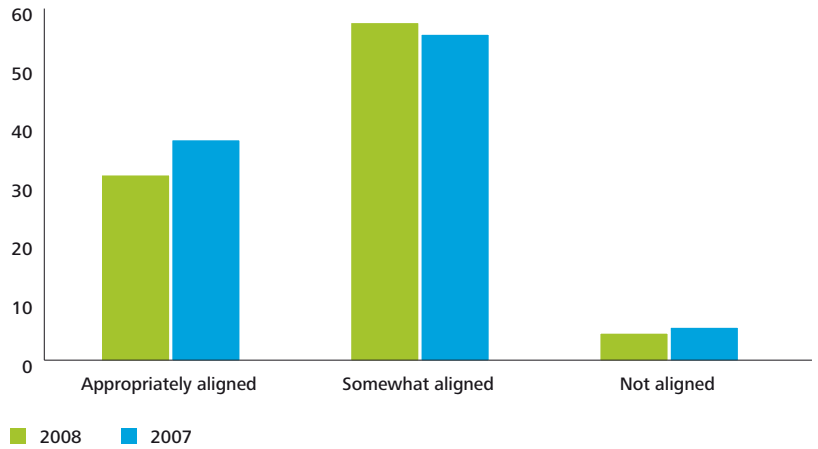
How information security meets the needs of an organization (%)



**Alignment of business and security initiatives**

Responses to this category, possibly more than any other, reflect the stature of information security within the organization, i.e., when business and security initiatives are aligned, IT security will be recognized for its true value and will have come full circle. It is somewhat discouraging that there is a slight drop from last year in the assessment that business and security initiatives are “appropriately aligned” (32% in 2008; 38% in 2007) and “not at all aligned” (5% in 2008; 6% in 2007). The good news is that the perception that business and security objectives are “somewhat aligned” appears to be growing (58% in 2008; 56% in 2007).

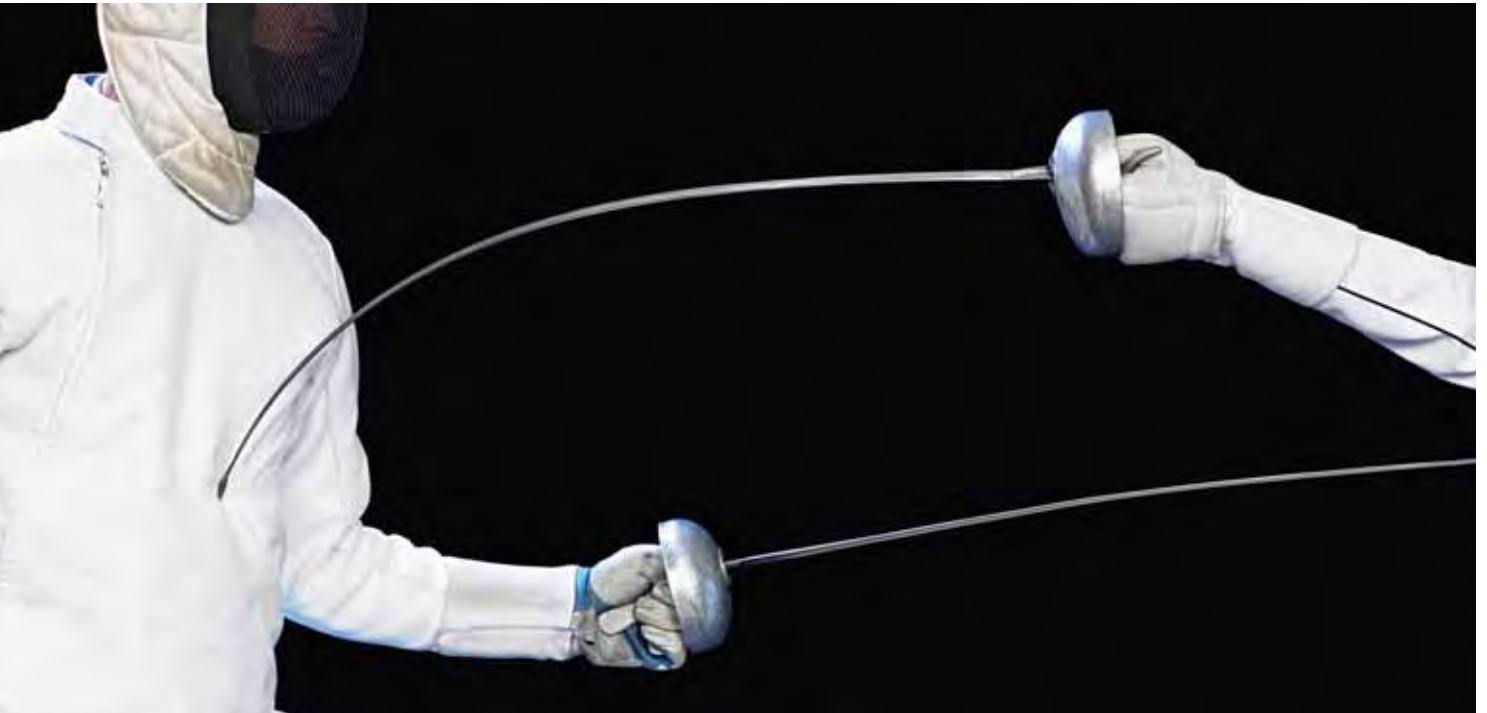
**Alignment of business and information security initiatives (%)**



---

When business and security initiatives are aligned, IT security will be recognized for its true value and will have come full circle.

# Risk



## Risk tolerance

When asked about their organization's risk tolerance, respondents indicate that their tolerance for risk may be growing. For example, in 2007, 41% of respondents indicated that they were content "to take the same risk as the rest of the industry"; in 2008, that number has fallen to 27% and the statement "...take more risk compared to the industry and have a lower cost" has grown by 5%. However, a large percentage (18% in 2008 and 19% in 2007) indicate that they "do not compare" and 10% have "no empirical data available":

- To take more risk compared to the industry and have a lower cost – 11% (6% in 2007).
- To take the same risk as the rest of the industry – 27% (41% in 2007).
- To take lesser risk compared to the industry, even at a higher cost – 24% (20% in 2007).
- We do not compare – 18% (19% in 2007).
- No empirical data available – 10% (14% in 2007).

## Application security and privacy as part of the software development lifecycle

Approximately the same number of respondents as in 2007 and the greatest percentage (46%) indicate that application security and privacy as part of the software development lifecycle varies from project to project indicating, therefore, that it is not standard procedure for all software development. While it might be reasonable for mature financial institutions to conduct their own risk-benefit analysis and determine the level of due diligence required for each particular software development project, an alarming 14% of respondents indicate that incorporating security and privacy as part of the software development life cycle is an afterthought for them:

- Incorporated in software development lifecycle – 31% (37% in 2007).
- Varies from project to project – 46% (49% in 2007).
- In most cases it is an afterthought – 14% (14% in 2007).

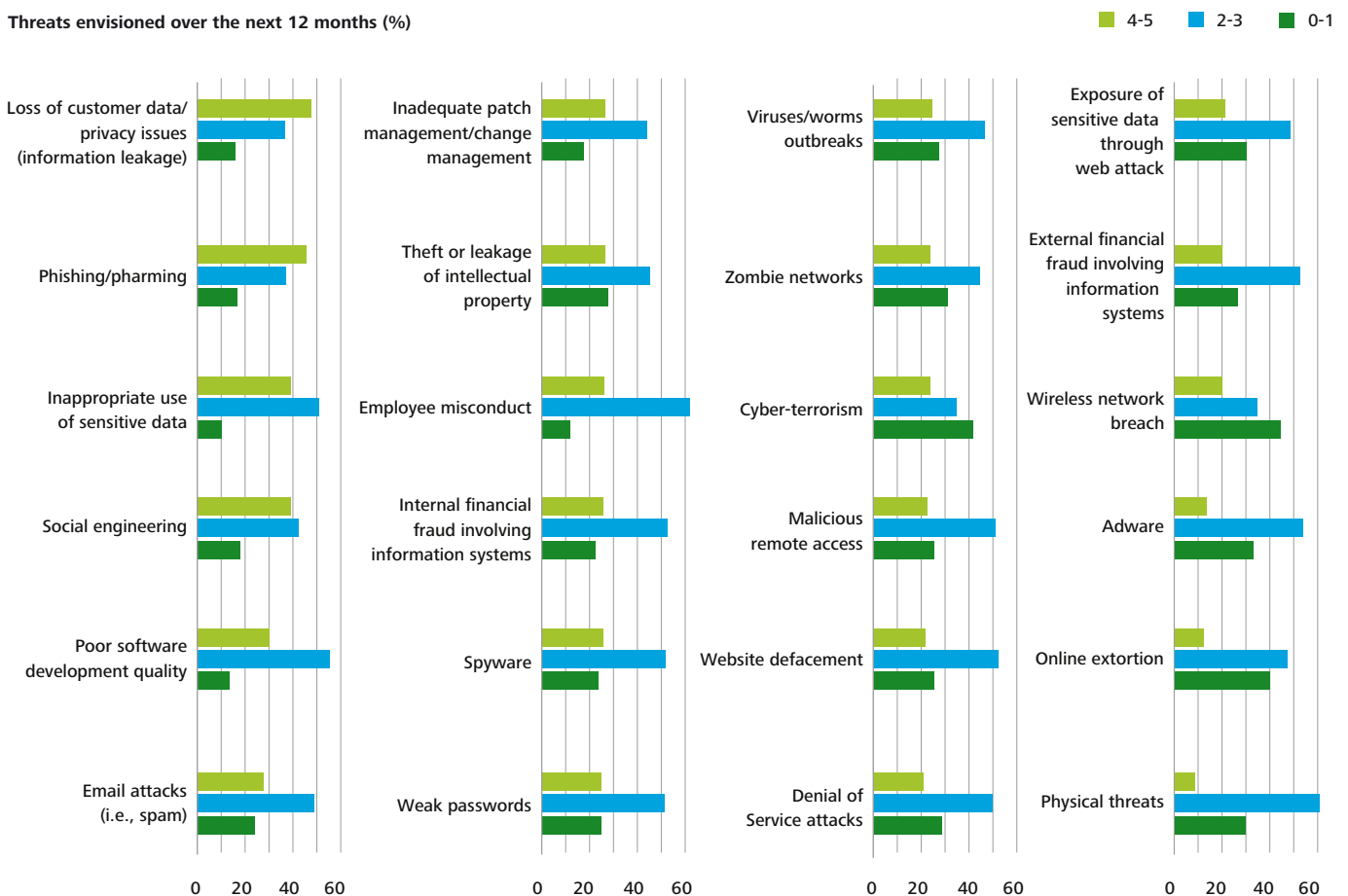
Only 35% characterize their application development directives (policies, standards, and procedures) as “well defined and practical”, with 24% indicating that they are “under development”:

- Well defined and practical – 35%.
- Well defined but impractical – 9%.
- Not well defined but practical – 17%.
- Not well defined – 10%.
- Under development – 24%.

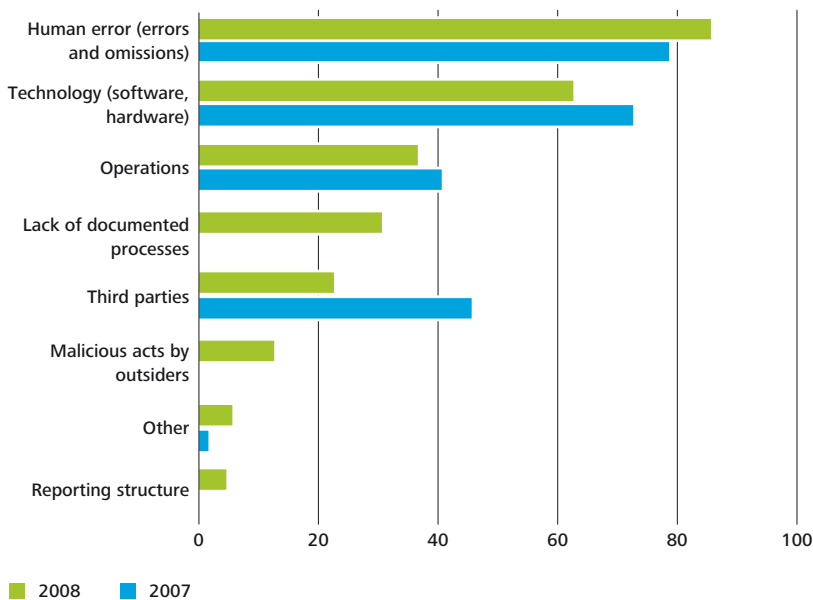
### Malicious external threats

Respondents were asked to rate their level of concern about malicious external threats on a scale of one to five (with five indicating the greatest concern). Loss of customer data/privacy issues (with 48% of respondents indicating the highest level of concern: 4 to 5) and phishing and pharming (46%) remain the most-mentioned malicious threats for the future. The phishing and pharming techniques of today look nothing like the phishing and pharming techniques of the early days – remember the amateurish email full of grammar and spelling mistakes telling you to click on a link to update your financial information? Times have changed spectacularly. One well known technique sends a Facebook message from one friend to another with a link to a YouTube video clip. The recipient clicks on the link then sees a prompt to download an updated version of the Flash player to run the clip. When the person clicks on the update, it installs malware on the computer.

Threats envisioned over the next 12 months (%)



Root causes of information systems failures (%)



**Root causes of information systems failure**

Again in 2008, as in previous years, an organization’s people (employees, customers, third parties, suppliers, etc.) are its greatest asset and its weakest link. Human error is overwhelmingly stated as the greatest weakness this year (86%), followed by technology (a distant 63%). Human error has risen from 79% in 2007, an understandable finding, given the increasing adoption of new technologies and social networking spaces that all increase the risk of errors and omissions. As human error risk rises, technology risk appears to recede – technology risk fell 10% from 2007. This could be due to the fact that technology is constantly improving to meet security demands and is therefore considered less of a threat or it could be that people have always been the concern, a fact that is becoming more acknowledged. Where only 6% separated human error from technology risk in 2007, in 2008 the gap is 23%. Unless robots replace the human work force (unlikely in the lifetime of anyone reading this report) then human error is an issue that companies will continue to deal with.

**External breach experience**

Viruses and worms, email attacks, and phishing/pharming are cited by respondents as the primary cause of repeated occurrences of external breaches. Last year, respondents cited the same three as the top causes of repeated external breaches. Repeated occurrences of these three types of breaches have fallen dramatically from last year: viruses/worms: 15% in 2008, 43% in 2007; email attacks: 24% in 2008, 57% in 2007; phishing/pharming: 7% in 2008, 38% in 2007.

Interestingly, in the case of viruses and worms, there is not a big difference in 2008 between those who had one occurrence (11%) and those who had repeated occurrences (15%) indicating that, after the first occurrence, many companies were able to deal with the issue to prevent repeated occurrences. However, email attacks are not as easy to deal with because they come in so many different forms and shutting down email is not an option (10% of respondents indicate that they have had at least one occurrence, with 24% indicating that they have had repeated occurrences).

The same is true for phishing and pharming, which also takes many forms, often appearing on internet sites as well as in e-mail (22% of respondents indicate repeated occurrences).

In addition, new threats are increasingly leading to vulnerabilities exploiting in new Web developments, such as social networking sites. Organizations need to continue to figure out ways to thwart these threats if the Internet is to be a trusted communications medium.

#### External breach experience

	One occurrence (%)	Repeated occurrences (%)
Viruses/worms outbreaks	11%	15%
Email attacks (i.e., spam)	10%	24%
Spyware	7%	11%
Zombie networks	4%	3%
Denial of service	6%	2%
Website defacement	5%	1%
Malicious remote access	2%	2%
Online extortion	2%	1%
Wireless network breach	3%	1%
Phishing/pharming	7%	22%
Social engineering	5%	7%
Employee misconduct	11%	11%
Theft of intellectual property	6%	1%
External financial fraud involving information systems	4%	10%
Exposure of sensitive data through web attack	4%	2%
Physical threats	7%	6%
Accidental instances	8%	5%
Other forms of external breach	4%	2%
No, have not been breached through an external attack	20%	7%

### Internal breach experience

Viruses and worms, loss of customer data and accidental instances are cited by respondents as the greatest causes of both one-time and repeated occurrences of internal breaches. The media speculated that a recent worm attack, acknowledged by the U.S. Department of Defense (DoD), may have been linked to thumb drives after the DoD subsequently banned them. Devices that allow information to be copied and moved freely are a constant source of worry for organizations.

Loss of customer data is a primary internal breach concern in the aftermath of the the largest retail breach incident, with almost the same percentage of respondents in 2008 as in 2007 citing both one-time and repeated occurrences. Accidental instances are cited as a main concern – these may include an error on the job because of a lack of documented procedure which causes the information to be compromised.

#### Internal breach experience

	One occurrence (%)	Repeated occurrences (%)
Viruses/worms outbreaks	11%	9%
Wireless network breach	3%	1%
Loss of customer data/privacy issues (information leakage)	8%	9%
Internal financial fraud involving information systems	6%	6%
Theft of intellectual property	4%	1%
Accidental instances	9%	10%
Other forms of internal breach	5%	3%
No, have not been breached through an internal attack	30%	8%

---

Viruses and worms, loss of customer data and accidental instances are cited by respondents as the greatest causes of both one-time and repeated occurrences of internal breaches.

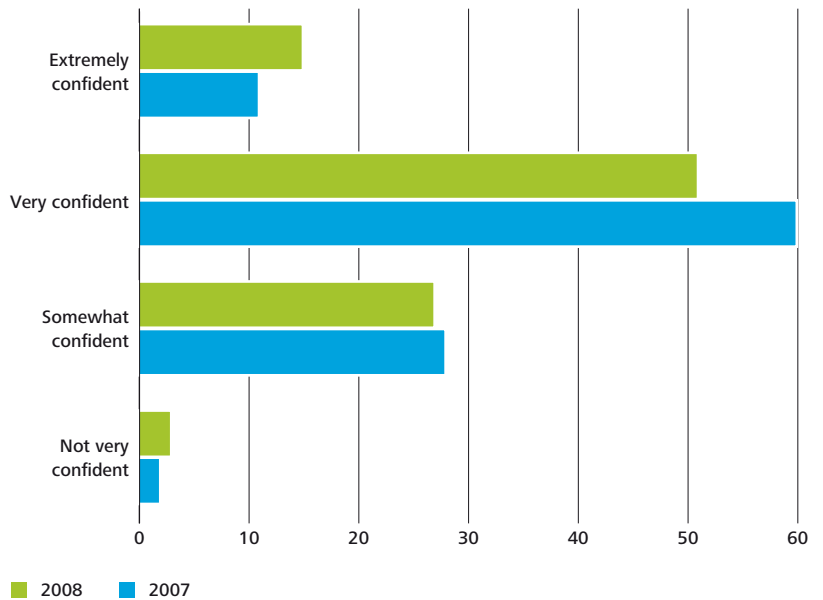
**Protection from cyber attacks**

Consistent with previous years, respondents’ perception of how well they are protected from cyber attacks shows that the majority (66%) are either very confident or extremely confident of their ability to prevent and/or block external attacks.

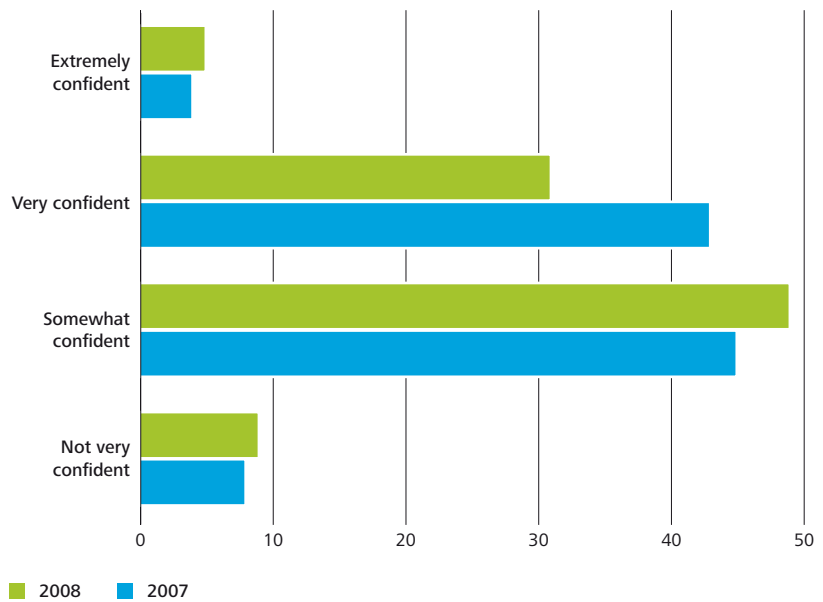
Internal cyber attacks, however, present a much more challenging issue – only 36% say they are extremely confident or very confident, while the majority of respondents (49%) allow themselves some doubt, saying they are somewhat confident in their ability to protect themselves from internal threats.

Perhaps reflecting the expanding security issues to deal with – the increasing sophistication of threats, the ever-expanding array of tools for the workforce and the increasing popularity of social networking sites – respondents indicate that less of them feel “very confident” in 2008 – for external attacks, 60% in 2007 has dropped to 51% in 2008 and for internal attacks, 43% in 2007 has dropped to 31% in 2008.

**Protection from cyber attacks – External (%)**



**Protection from cyber attacks – Internal (%)**



# Use of security technology



## Security technology

The majority of organizations have recognized the risk inherent in wireless LANs, social networking technologies, and instant messaging technologies and have restricted their use (55%, 53%, and 58%, respectively). However, most organizations do not prohibit the use of storage devices and mobile devices because such a practice may well interfere with productivity.

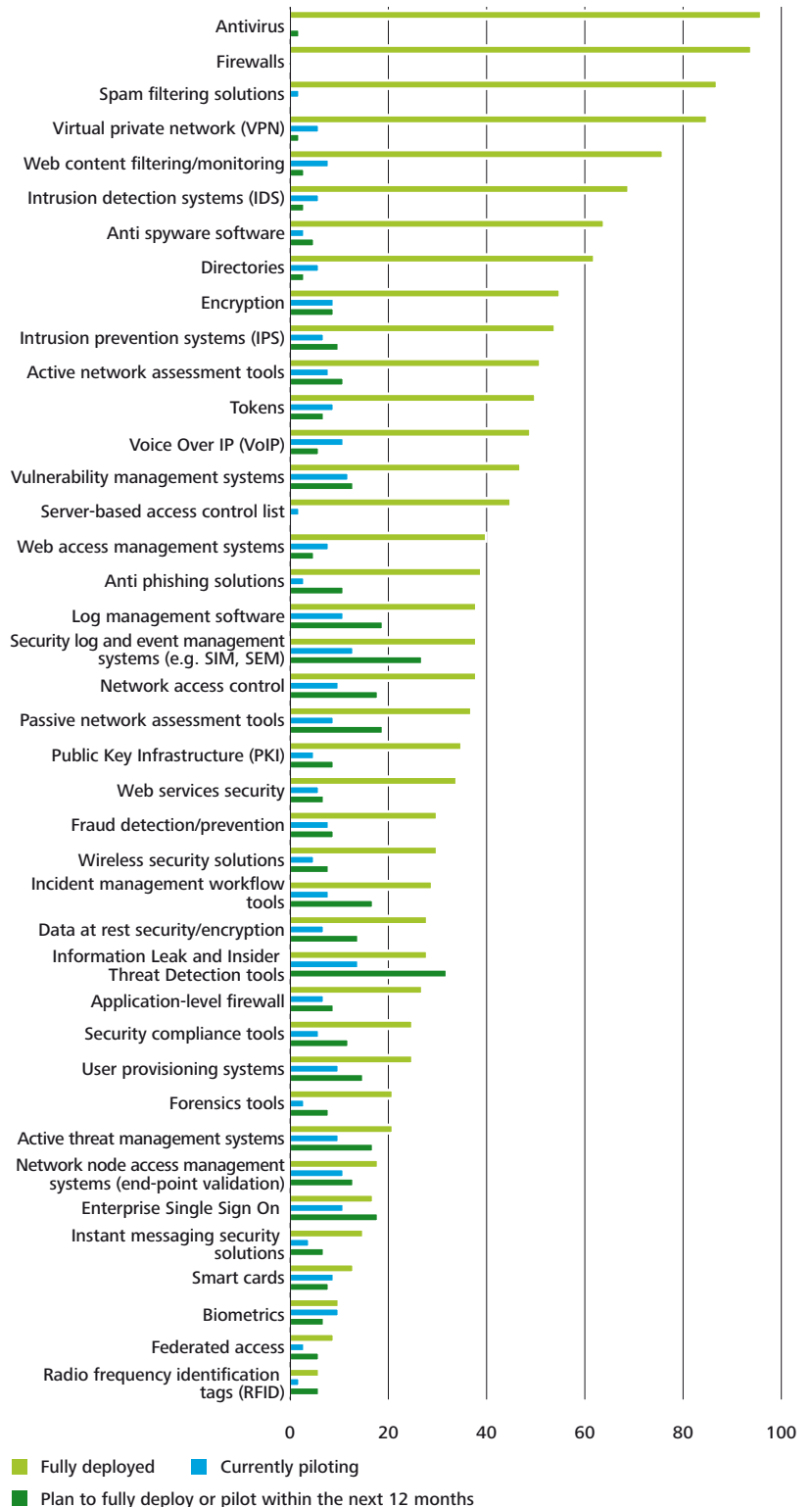
For these two technologies (storage devices and mobile devices), respondents indicate that their organizations offer employee guidelines (31% and 38%, respectively), publish policies on acceptable use (39% and 42%, respectively) and implement and encourage the use of secure technologies (23% and 30%, respectively). An example of this latter category would be encrypted USB storage keys issued by the organization that require a password to access the information on them.

## Organizations' handling of technologies

	Prohibit the use of	Offer employee guidelines on secure use	Publish policies on acceptable business use	Implement and encourage use of secured technologies
Wireless LAN capability	55%	13%	19%	18%
Storage devices (e.g., USB drives, portable media players, etc.)	27%	31%	39%	23%
Mobile devices (i.e., PDAs, Blackberries)	10%	38%	42%	30%
Social networking technologies (e.g., Facebook, blogs)	53%	17%	11%	4%
Instant messaging technologies	58%	13%	12%	14%

Predictably, an overwhelming majority of respondents indicate that their organizations employ antivirus (96%), firewalls (94%), spam-filtering solutions (87%), and virtual private networks (85%). Radio frequency identification (RFID) is the least frequently deployed technology (6%), according to the survey respondents. RFID is a chip technology that can be implanted in almost anything where the data is transmitted to a reader via radio waves. The technology that most organizations are piloting (13%) is security log and event management systems; it is also the technology most likely to be deployed within the next 12 months (27%). This technology helps organizations to convert security data into management reports to meet the demands of regulatory compliance. This finding is consistent with the issue that most organizations indicate to be their top initiative, security regulatory compliance.

**Security technologies deployed, piloted, and planned (%)**



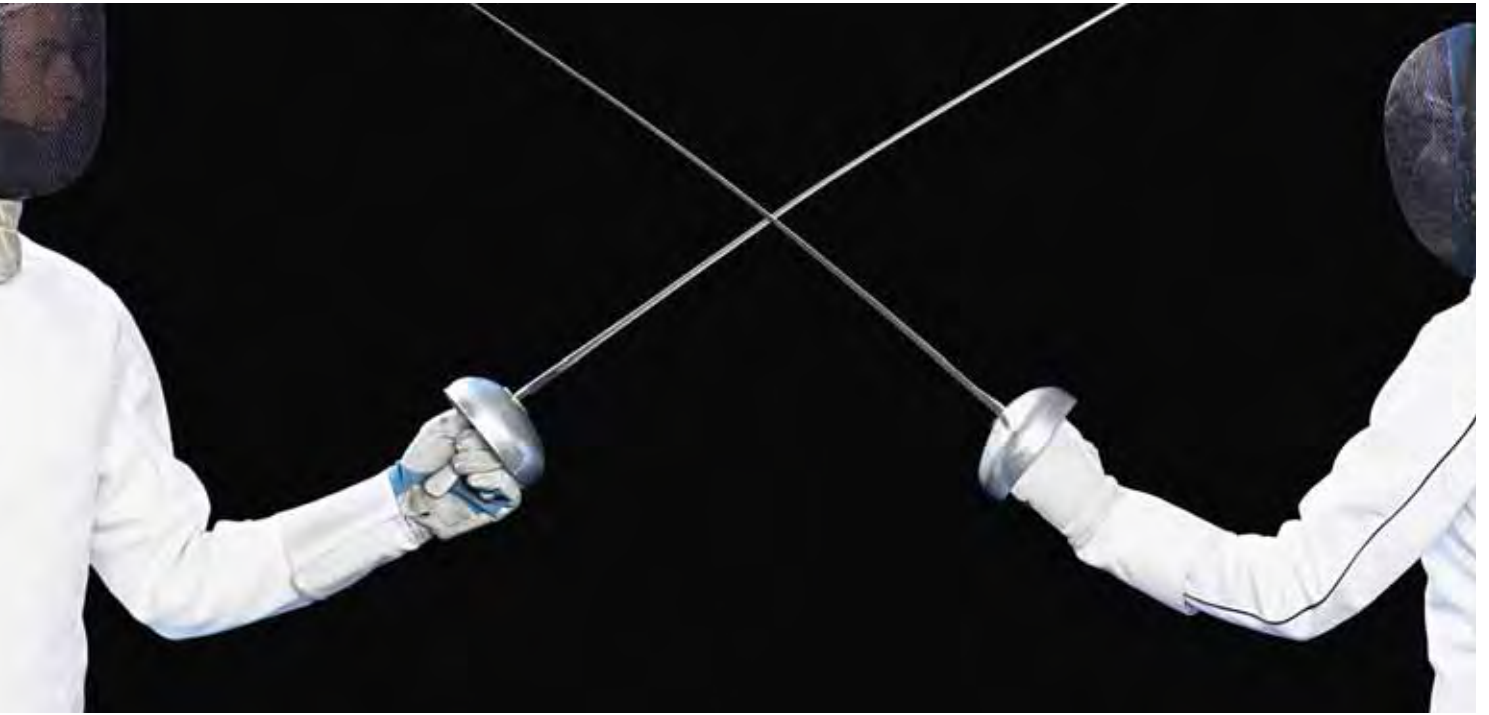
### Security testing

In the five types of testing, from vulnerability scanning to application security code review, over the five frequencies of testing intervals, from monthly to never, the numbers are relatively consistent with one exception: the ad hoc application of security code review has dropped from 61% in 2007 to 41% in 2008. At the same time, there is a relatively high number of respondents who state that they never undertake application security code reviews (29%), internal penetration testing (14%), external penetration testing (10%), penetration testing by a third-party (10%) and vulnerability scanning (6%).

#### Frequency of security reviews

	Quarterly	Semi-annually	Annually	Ad hoc	Never
Vulnerability scanning	43%	9%	13%	27%	6%
Internal penetration testing	16%	12%	23%	33%	14%
External penetration testing	19%	13%	33%	24%	10%
Penetration testing conducted by third-party	13%	14%	34%	26%	10%
Application security code review	6%	5%	8%	41%	29%

# Quality of operations



---

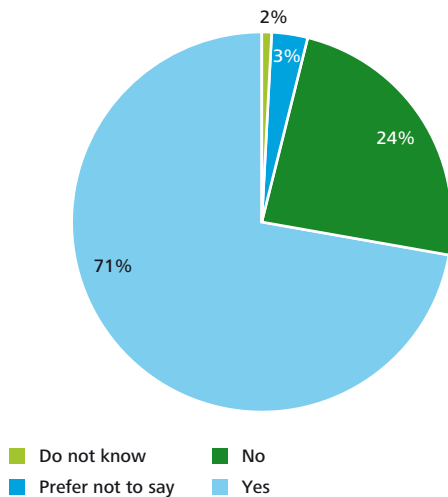
While a large number of respondents (38%) indicate an equal concern for the misconduct of both internal and external people, it is clear that internal people alone are the biggest worry – 36% versus only 13% for external people. Organizations clearly recognize that internal people, the machine that makes the business run, are a concern.

**Internal and external misconduct related to information security systems**

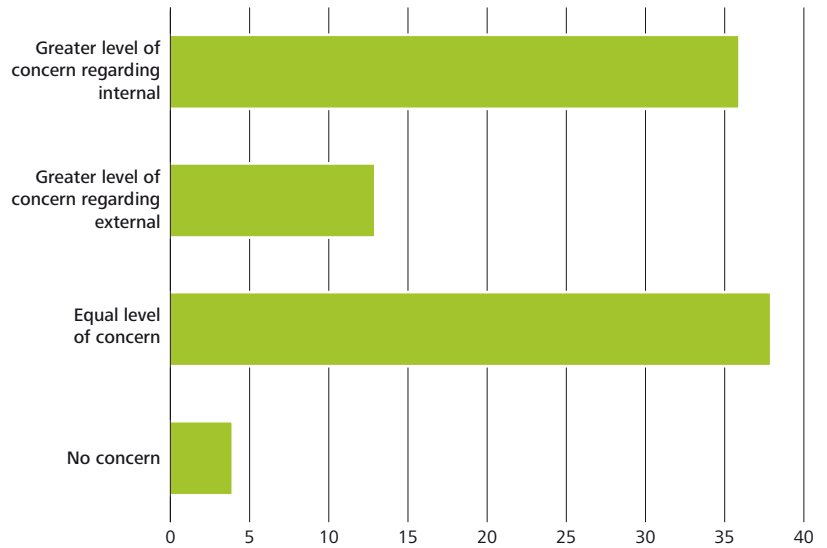
While a large number of respondents (38%) indicate an equal concern for the misconduct of both internal and external people, it is clear that internal people alone are the biggest worry – 36% versus only 13% for external people. Organizations clearly recognize that internal people, the machine that makes the business run, are a concern.

Respondents indicate that a full 71% of companies have provided training on identification and reporting of suspicious activities to their employees and 56% of companies combined chose to provide an awareness session on information security and privacy issues to all or at least a segment of their online customers. However, when respondents were asked to name their top security initiatives earlier in this report, security training and awareness ranked 7th on a list of 15, with only 36% listing it as a priority in 2008, compared to 48% in 2007.

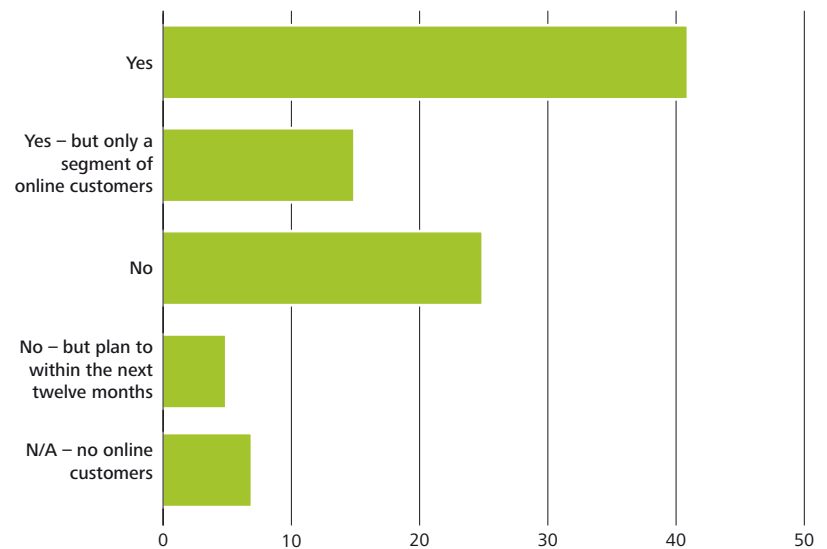
**Train employees on identification and reporting of suspicious activities**



**Level of concern regarding internal/external people's misconduct involving IS (%)**



**Offered online customers an awareness session on information security and privacy issues in the past 12 months (%)**

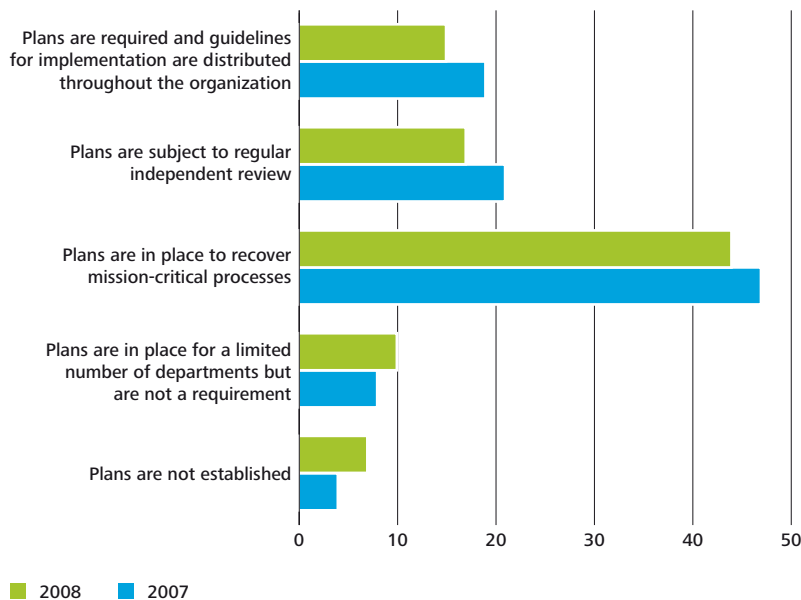


Customized job training is sporadic, with the highest focus of both regular and ad hoc training on systems administrators. Predictably, contractors, who become even more of a risk during hard economic times when companies increasingly outsource rather than hire, had the lowest percentage of both regular and ad hoc training.

**Customized training by job role and function offered**

	Yes – regularly	Yes – ad hoc	No	N/A – No training offered
Executives	21%	28%	34%	6%
People handling sensitive information	29%	32%	26%	5%
IT application developers and programmers	28%	34%	25%	6%
Systems administrators	30%	38%	22%	5%
IT infrastructure	29%	35%	23%	5%
Contractors	15%	21%	37%	13%

**State of business continuity planning (%)**

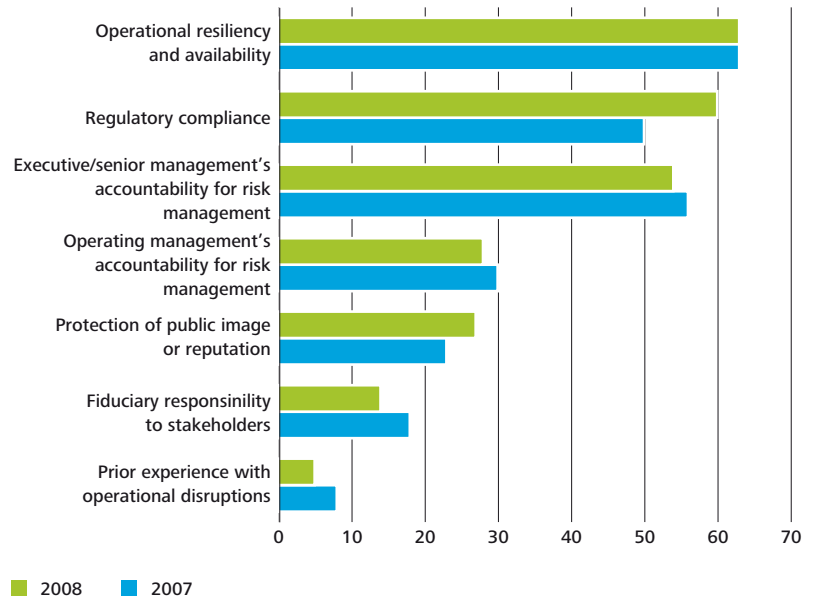


**Business continuity planning**

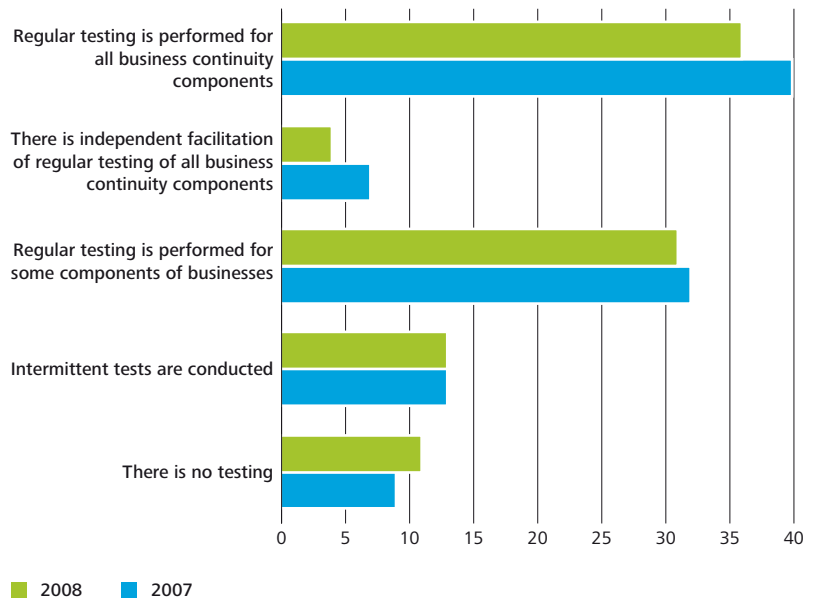
It seemed that every kind of natural and man-made disaster was perpetrated on humanity in the first decade of 2000. War, 9/11, SARS, terrorist attacks, tsunamis, earthquakes, etc. all wreaked havoc with lives, property, and commerce. As terrible as it all was, the experience they afforded organizations in terms of business continuity planning was invaluable. It seemed that, if an organization could get through that time with their mission-critical applications intact, they could get through anything. Organizations appear to have done a good job of prioritizing and dealing with their mission-critical applications – 44% indicate that plans are in place to recover mission-critical processes, just slightly down from 47% in 2007. The percentage of respondents who indicate that “plans are required and guidelines for implementation are distributed throughout the organization” remains relatively unchanged from last year as well (15% in 2008, 19% in 2007).

In keeping with the top priorities, the key drivers of business continuity planning are operational resiliency and availability (good access, low risk) (unchanged from 2007 at 63%) and regulatory compliance (moving into the majority with 60% in 2008; 50% in 2007). While “regular testing is performed for all business continuity components” is the statement chosen by the highest percentage of respondents (36%), this is still a relatively low number and remains virtually unchanged from 2007 (40%).

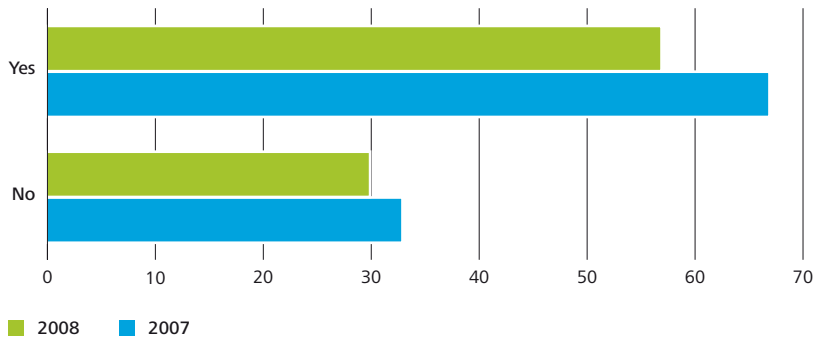
**Key drivers behind business continuity planning (%)**



**Frequency of business continuity testing (%)**



**Vendor security evaluation before engagement (%)**

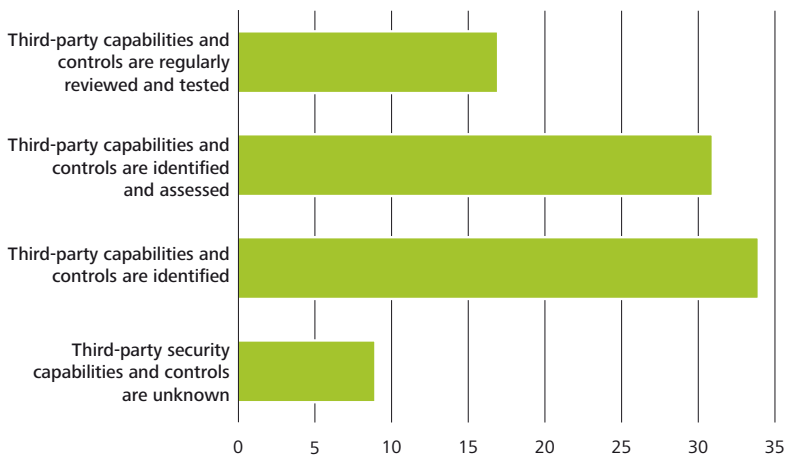


**Third-party controls and vendor reviews**

Fifty-seven percent of respondents indicate that their organizations conduct an objective, independent review of the security of their vendors before engagement.

However, while most respondents state that their organizations *identify* the security capabilities, controls and organizational dependencies of third parties (34%), fewer (31%) actually identify *and* assess their suitability.

**Third-party capabilities, controls, and organizational dependencies (%)**

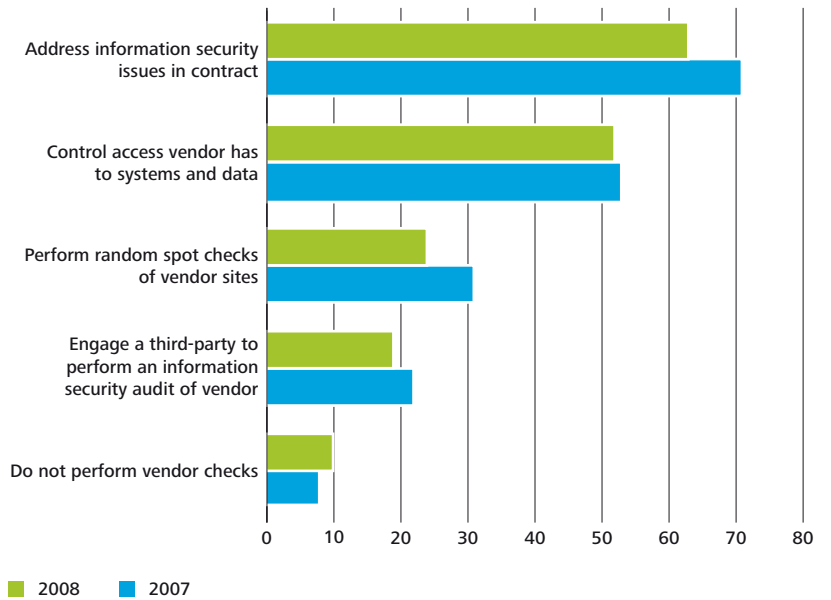


The most common way that organizations ensure the adequacy of the information security of their vendors once they are engaged is through a contract (63%) and by restricting their vendors' access to their systems (52%). These are relatively benign controls but the vendor/organization relationship is no doubt bolstered by the understanding that vendors would be better off by being very cautious with the access to the data that they have been granted. However, as we know, breaches are as much a result of inadvertent and careless behavior as they are of malicious intent.

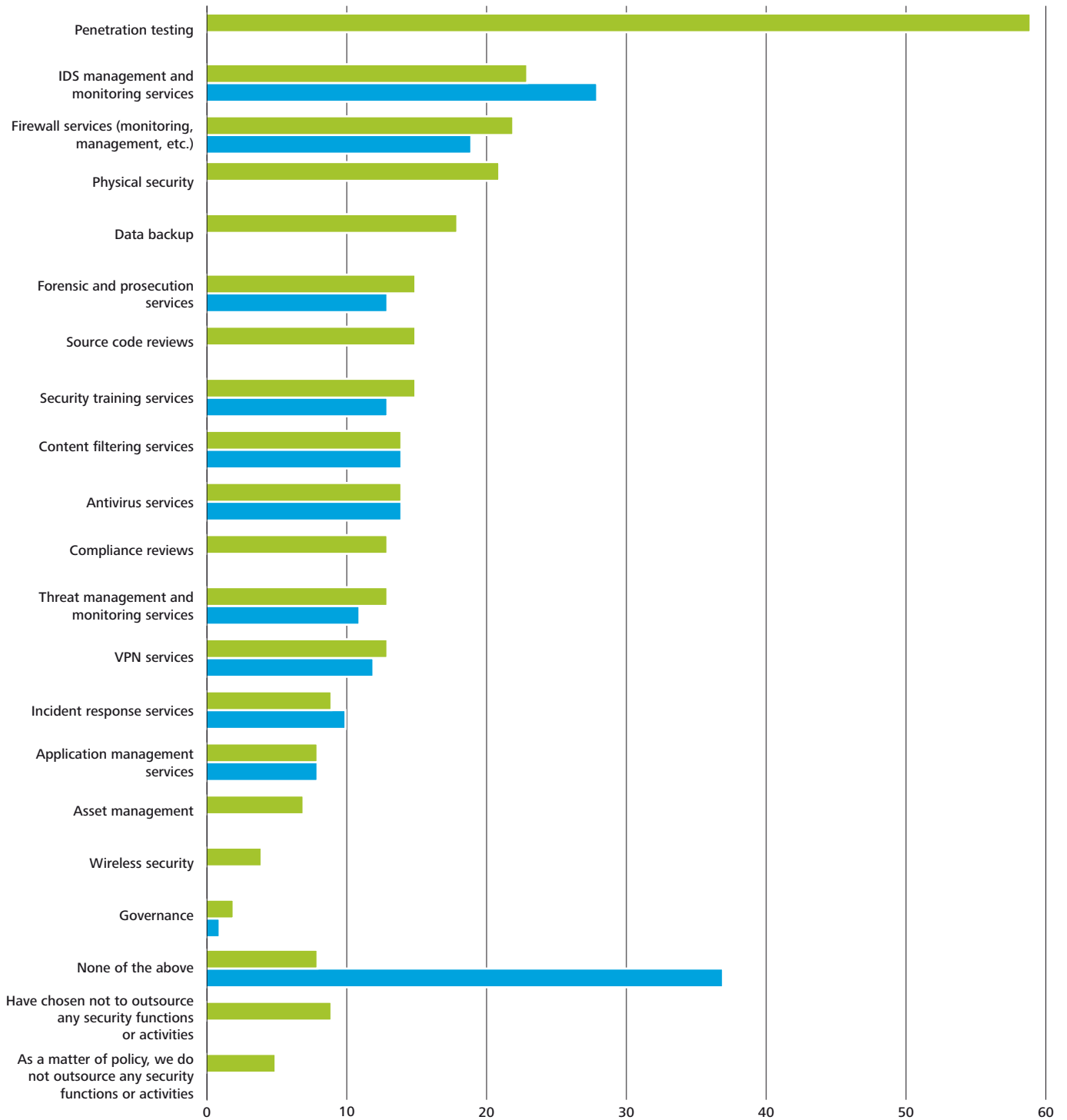
**Outsourcing of information security activities**

This year's survey indicated that penetration testing is the single most outsourced information security activity (59%) from the list provided. This is not surprising, as this type of service is widely available in the market, and required by emerging legal and regulatory requirements and security standards such as the Payment Card Industry Data Security Standards (PCI-DSS). Intrusion detection and monitoring services (23%) as well as firewall services (22%) are high in the list given that many respondents are starting to build business cases for such services and the maturity of these practices make them attractive. Governance, as in previous years, remains low on the list and only 5% of respondents indicate that their policies prohibit any outsourcing of information security activities.

**Ensuring information security with outsourcing vendors (%)**



**Outsourcing of information security activities (%)**



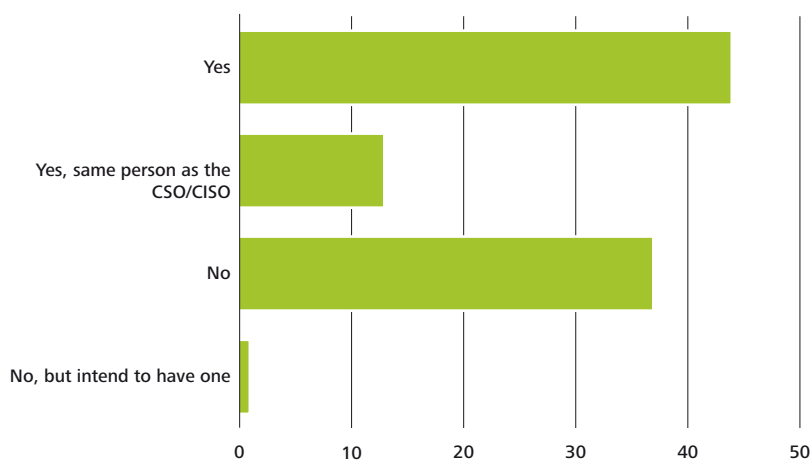
■ 2008 ■ 2007

Due to an expanded question set this year, responses that do not show comparisons to last year indicate that data was not collected for that question last year.

# Privacy



Privacy executive position (%)



## Privacy officer

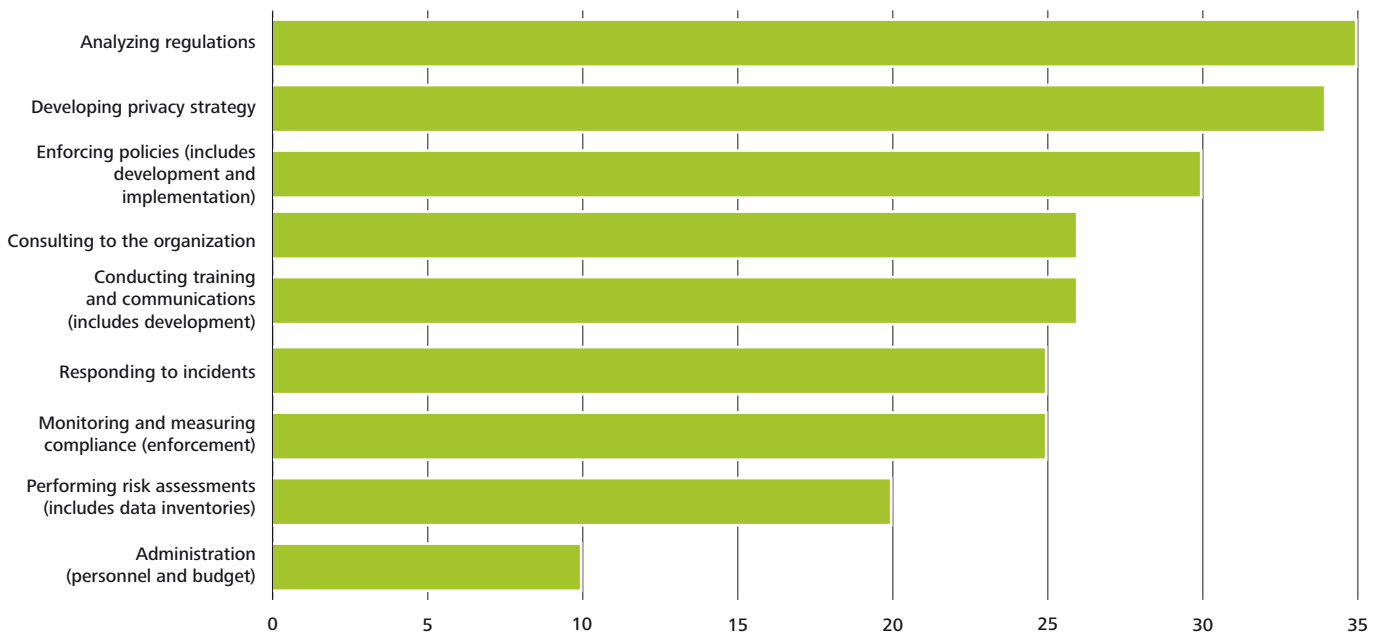
Nearly equal numbers of respondents indicate that they have a dedicated privacy executive officer (44%) as those that have yet to embrace this position (37%).

The reporting structure for the privacy officer is relatively unchanged, compared to 2007. The Board of Directors is still the most frequently mentioned line of reporting. Top reporting links, listed in declining order, are:

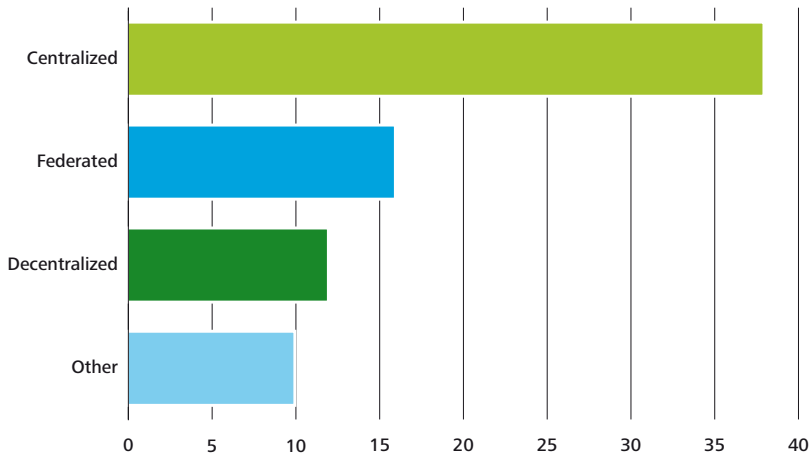
- Board of Directors
- CEO
- Legal
- General Counsel
- CRO
- CIO

Respondents indicate that the most common responsibility of the privacy officer, other than keeping management informed, is analyzing regulation (35%). This is in keeping with the top security initiatives (compliance with regulation as the second most common); and this is something CISOs should also keep an eye on as well – changing legislation and regulations contribute to the evolution of Chief Privacy Officer role, and CISOs need to get involved in the process as well, because it directly impacts their function.

**Responsibilities of a privacy executive (%)**



**Privacy structure (%)**



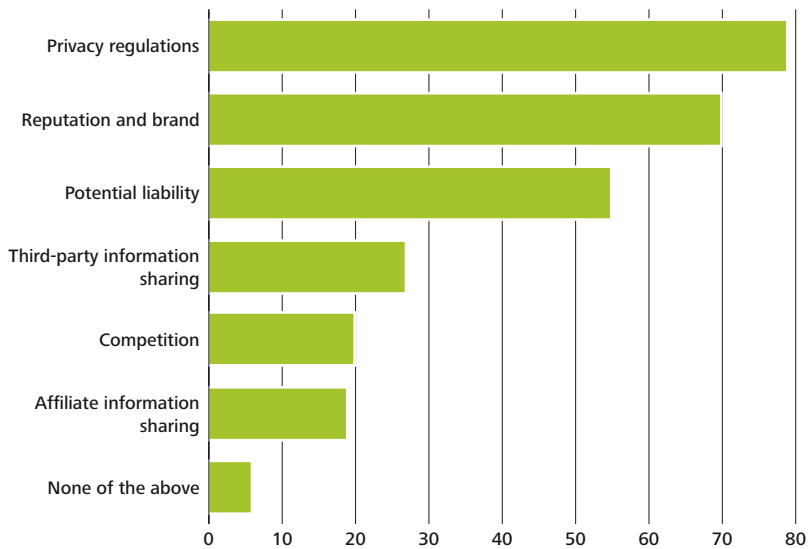
- Centralized (managed from a centralized managed group)
- Federated (centralized groups that set common standards and perform central functions while each business unit has a security representative for specific activities to the business unit)
- Decentralized (responsibility placed within business units)
- Other

Privacy is administered using a centralized model (38%). The federated model (at 16%) has a long way to go to catch up.

**Privacy drivers**

Privacy drivers are overwhelmingly privacy regulations (79%) and protection of reputation and brand (70%).

**Influential drivers for privacy (%)**

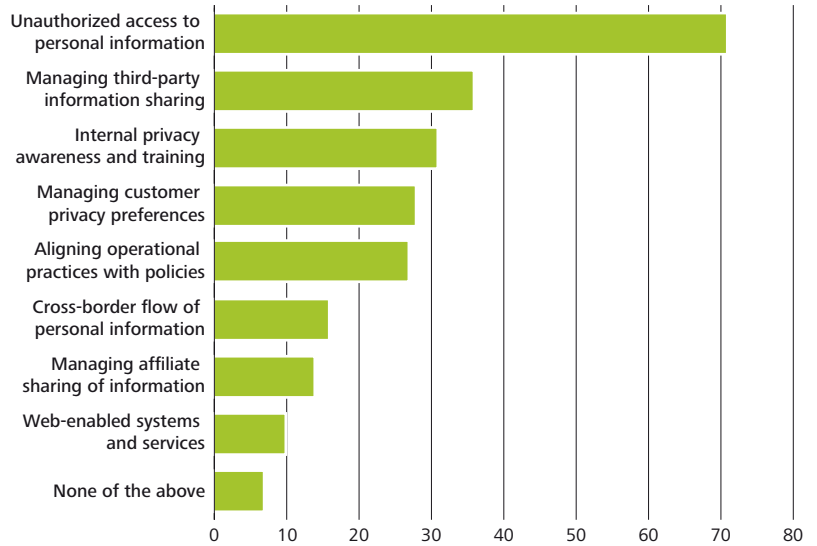


In keeping with the theme of the findings and mirroring those of the top security initiatives, unauthorized access to information (71%) is overwhelmingly ahead of managing third-party information sharing (36%) as the top privacy concern of the organization. Internal privacy awareness and training was stated as the number three concern.

**Privacy programs and policies**

While most organizations have policies in place regarding privacy, there is not a huge difference between the number of organizations who have a program in place for managing privacy compliance (48%) and those who do not (37%). It is interesting to note that a low percentage of the respondents' privacy officers were responsible for analyzing privacy regulation (35%) and monitoring and measuring compliance (25%).

**Areas of concern from privacy perspective (%)**



**Presence of privacy programs and policies**

<b>Program for managing privacy compliance</b>	
Yes	48%
No	37%
Do not know	12%
Prefer not to say	2%
<b>Written privacy, fair information practices or data collection policy</b>	
Yes	63%
No	27%
Do not know	8%
Prefer not to say	2%
<b>Personal information destruction formal policy</b>	
Yes	61%
No	28%
Do not know	9%
Prefer not to say	2%
<b>Formal complaints procedure for personal information management practices or policies</b>	
Yes	60%
No	23%
Do not know	14%
Prefer not to say	3%

# Contacts

## Global leaders

### **Jack Ribeiro**

Managing Partner – Global Financial Services Industry (GFSI) Practice  
Deloitte Touche Tohmatsu  
+1 212 436 2573  
jribeiro@deloitte.com

### **Leon Bloom**

Deputy Managing Partner – Global Financial Services Industry (GFSI) Practice  
Deloitte Touche Tohmatsu  
+1 416 601 6244  
lebloom@deloitte.ca

### **Adel Melek**

Global Leader, Security & Privacy Services  
Global Financial Services Industry (GFSI) Practice  
Deloitte Touche Tohmatsu  
+1 416 601 6524  
amelek@deloitte.ca

### **Mark Layton**

Global Enterprise Risk Leader  
Deloitte Touche Tohmatsu  
+1 214 840 7979  
mlayton@deloitte.com

## Security & Privacy Services regional leaders

### **Adel Melek**

Canada – Toronto  
Deloitte & Touche LLP  
+1 416 601 6524  
amelek@deloitte.ca

### **Ted DeZabala**

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

### **Carlo Schupp**

EMEA – Brussels, Belgium  
Deloitte Touche Tohmatsu  
+ 32 2 800 20 77  
cschupp@deloitte.com

### **Uantchern Loh**

APAC – Kuala Lumpur, Malaysia  
Deloitte KassimChan  
+65 6216 3282  
uloh@deloitte.com

### **Martin Carmuega**

LACRO – Buenos Aires, Argentina  
Deloitte & Co. S.R.L.  
+54 11 43204003  
mcarmuega@deloitte.com

### **Mitsuhiko Maruyama**

Japan – Tokyo  
Deloitte Touche Tohmatsu (Japan Group)  
+81-3-4218-7304  
mitsuhiko.maruyama@tohmatu.co.jp

## Regional contacts

### APAC

#### **Bruce Daly**

Tokyo, Japan  
Deloitte Touche Tohmatsu (Japan Group)  
+81 3 4218 7284  
brdaly@deloitte.com

#### **Joshua Chua**

Singapore  
Deloitte & Touche LLP  
+65 6216 3188  
joshuachua@deloitte.com

#### **Abhay Gupte**

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

#### **Danny Lau**

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

#### **Tommy Viljoen**

Sydney, Australia  
Deloitte Australia  
+61 02 9322 7713  
tfviljoen@deloitte.com.au

**Canada****Marcel Labelle**

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

**Donald Mccoll**

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

**CIS****Wayne Brandt**

Moscow, Russia  
ZAO Deloitte & Touche CIS  
+7 495 787 0600  
wbrandt@deloitte.ru

**EMEA****Francois Renault**

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

**Kris Budnik**

Johannesburg, South Africa  
Deloitte & Touche  
+27 0 11 806 5224  
kbudnick@deloitte.co.za

**Mike Maddison**

London, U.K.  
Deloitte & Touche LLP U.K.  
+44 20 7303 0017  
mmaddison@deloitte.co.uk

**Alfonso Mur**

Madrid, Spain  
Deloitte SL  
+34 915145000 x2103  
amur@deloitte.es

**Sven Probst**

Zurich, Switzerland  
Deloitte AG  
+41 44 421 6401  
sprobst@deloitte.ch

**Hans Bootsma**

Amstelveen, Netherlands  
Deloitte Holding B.V.  
+31 61 098 0182  
hbootsma@deloitte.nl

**LACRO****Robson Calil Chaar**

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

**Jeremy Smith**

Cayman Islands  
Deloitte Touche Tohmatsu  
+1 345 814 3315  
jersmith@deloitte.com

**Mauricio Torres Romero**

Mexico City, Mexico  
Galaz, Yamazaki, Ruiz Urquiza, S.C.  
Deloitte  
+52 55 50806943  
mtorresromero@deloittemx.com

**USA****Rich Baich**

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

**John Clark**

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

**Kenneth DeJarnette**

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

**Mark Steinhoff**

Boston, USA  
Deloitte & Touche LLP  
+ 1 617 437 2614  
msteinhoff@deloitte.com

Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, and its network of member firms, each of which is a legally separate and independent entity. Please see [www.deloitte.com/about](http://www.deloitte.com/about) for a detailed description of the legal structure of Deloitte Touche Tohmatsu and its member firms.

#### **Deloitte Global Profile**

Deloitte provides audit, tax, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in 140 countries, Deloitte brings world-class capabilities and deep local expertise to help clients succeed wherever they operate. Deloitte's 165,000 professionals are committed to becoming the standard of excellence.

Deloitte's professionals are unified by a collaborative culture that fosters integrity, outstanding value to markets and clients, commitment to each other, and strength from cultural diversity. They enjoy an environment of continuous learning, challenging experiences, and enriching career opportunities. Deloitte's professionals are dedicated to strengthening corporate responsibility, building public trust, and making a positive impact in their communities.

#### **Disclaimer**

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. None of Deloitte Touche Tohmatsu, its member firms, or its and their affiliates are, by means of these survey results, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. These survey results are not a substitute for such professional advice or services, nor should they be used as a basis for any decision or action that may affect your finances or your business. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

None of Deloitte Touche Tohmatsu, its member firms, or its and their respective affiliates shall be responsible for any loss whatsoever sustained by any person who relies on this publication.

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.

© 2009 Deloitte Touche Tohmatsu.

Designed and produced by The Creative Studio at Deloitte, London. 28433

Item #8286