2010 Financial Services Global Security Study

The faceless threat

Contents

Foreword 1

Participant profile 2

Key findings 3

Geography as a factor in security practices 6

Size as a factor in security practices 11

Sector as a factor in security practices 14

Security issues of 2010 17

How DTT's GFSI Group designed, implemented and evaluated the survey 35

Acknowledgments 36

Additional insights 36

Foreword

The new decade marks a turning point for those of us in the information security industry. We now live in an age of cyber warfare. The environment is dangerous and sinister. The children who used to make mischief in their basements are now only bit players and rarely make the news anymore. They have been superseded by organized crime, governments and individuals who make computer fraud their full-time business, either for monetary gain or for competitive or technological advantage. Countries now accuse each other of cyber warfare. Every network of substantial size has been compromised in some way. Governments are appointing senior military brass to focus on cyber warfare. The stakes have never been higher and the battle is being fought in every corner of the world. It's all out there: botnets, zombie networks, Trojans, malware, spam, phishing, much of it now so sophisticated even the most wary of us can be tricked.

We talk a lot about the increasing sophistication of threats. Now we have something else to deal with as well: the decreasing level of competence required to pose a threat. Consider Mariposa, the botnet that originated in Spain and infected millions of computers. The perpetrators had "limited computer skills" and they didn't write their own brilliant computer program – they simply downloaded what they needed from the internet. A new reality is the increasing availability of tools on the internet, allowing those with less know-how to get in on the cyber crime act.

This year's security study responses support the reality that a turning point in the industry has arrived:

- For the first time, organizations are proactive, embracing new technologies as "early majority adopters", no longer content, as "late majority adopters", to simply be reactive.

- For the first time, the lowest percentage of respondents (36%) stated that "lack of sufficient budget", is the major barrier to ensuring information security, compared to 56% last year. During the worst economic downturn in recent memory when so many budgets are being cut, information security budgets are safe for the most part and many have increased.

- For the first time, information security compliance (internal/external audit) remediation is a top-five security initiative as organizations gear up for increased regulation and legislation.

- For the first time, more than half of organizations state that physical information, such as paper, is within the mandate and scope of the executive responsible for information security. The response (59%) is still too low – and indicates a security gap – but, in our opinion, it is moving in the right direction.

This is now the seventh year of our survey. These survey questions involve time and effort on the part of busy people who take time away from very important jobs. My sincere thanks go out to the Chief Information Security Officers, their designates, the security management teams from financial institutions around the world and all the people behind the scenes who make it possible to produce this global security study. Without you it simply could not be done.

We've been discussing change for years. Now it's here. It will take all our smarts, all our knowledge and all our expertise to wage and win the cyber war. It will be challenging and exciting but there will be progress on many fronts. In our view, there is no better time than the present decade to be part of the information security industry.

Adel Melek

Adel Melek
DTT Global Leader, Information & Technology Risk
DTT Global Leader, Enterprise Risk Services
– Global Financial Services Industry

Participant profile

Participant breakdown

The data that allow us to discuss findings and current trends comes directly from those who are on the front lines of the global financial services industry. Deloitte* agreed to preserve the anonymity of the organizations who participated in the survey.

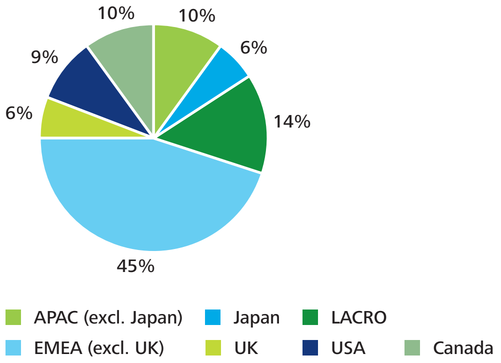
Overall, the participants represent:

- 27% of the top 100 global financial institutions.
- 26% of the top 100 global banks.
- 28% of the top 50 global insurance companies.

More than 350 major financial institutions worldwide have been interviewed by senior Information & Technology Risk practitioners for the 2010 Financial Services Industry (FSI) Global Security Study.

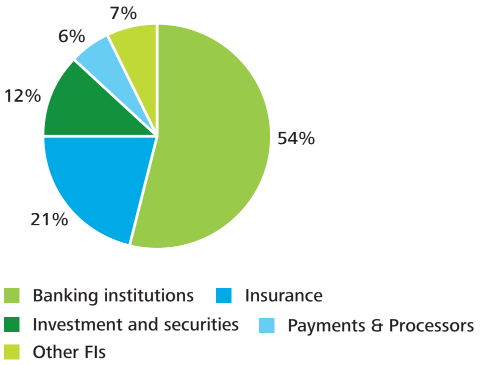
Regional breakdown

Financial services industry respondents to the 2010 FSI Global Security Study are from 45 countries around the world. The regional breakdown is as follows:



Sector breakdown

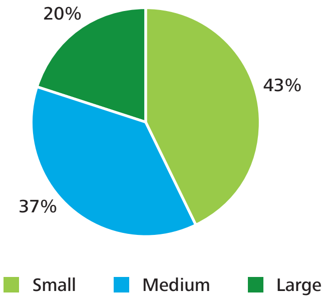
This year, the survey had good representation from the main sectors of the industry. The sector breakdown is as follows:



Size breakdown

For the purpose of this study, organizations considered "small" are those with fewer than 1,000 employees; organizations considered "medium" are those with 1,000 to 10,000 employees, and those considered "large" are those with more than 10,000 employees.

The size breakdown is as follows:



Revenue breakdown

Respondent organizations represent eight revenue categories.

The revenue breakdown is as follows:

<500M	33%
500M to 1B	11%
1B to 1.99B	5%
2B to 4.99B	9%
5B to 9.9B	4%
10B to 14.99B	2%
15B to 20B	3%
>20B	7%

Results may not total 100% as this survey is reporting selected information only; responses from those who decline to answer may not be included in the reported data.

* As used in this document, 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 for a detailed description of the legal structure of Deloitte Touche Tohmatsu and its member firms

Key findings

Cyber warfare has taken a chilling turn

There was a time when the perpetrators of cyber crime were bright children in basements making mischief. Fast forward to 2010. U.S. President Obama has made cyber war defence a top national priority. The U.S. government has appointed a national cyber coordinator. NATO has set up the Cooperative Cyber Defence Centre of Excellence (CCDCOE). When asked what external breaches they had experienced in the last 12 months, the greatest number of financial services industry respondents to the survey indicated repeated occurrences of malicious software originating from outside the organization. The survey reveals CISOs are far less confident that traditional controls will protect their organizations – with good reason. Cyber warfare has gone global and governments and organized crime are piling in.

Perhaps most unsettling of all are the lessons from the Mariposa botnet that infected more than 15 million computers around the world.* Mariposa was not the brainchild of brilliant computer programmers but individuals with "limited computer skills". They downloaded the software they needed from the internet for less than a thousand dollars and were so unsophisticated that one of them, using his home computer, led police to his door.

Today, the security environment is virtually unrecognizable from the early days – a single decade has produced fascinating but chilling developments. The bottom line is that the game has changed and no one is immune.

Identity and Access Management (IAM) is undergoing a metamorphosis

Respondents indicate that IAM is a top security initiative for 2010. Governance, Risk and Compliance (GRC) tend to be the driving forces behind IAM. Key issues, borne out by the top internal/external audit findings, are access certification, knowing who has access to information, whether it is appropriate, and documenting it – and strong governance that establishes automated, continuous processes for managing user access to information resources. IAM is a significantly higher priority for large organizations with more than 10,000 employees (63%) compared to small organizations with less than 1,000 employees (35%). Geography also influences respondents' responses: IAM is less of a priority in the U.K (35%) than in other parts of the world, particularly the U.S. (67%) and Japan (65%).

In the early days of information security (over the last decade), IAM performed the function of a gatekeeper, essentially keeping the bad guys out. But IAM has evolved far beyond that, not only in authentication but in the level of granularity of access as well as in the ability to track back, stroke by stroke, what events took place, when, and by whom. Today, many organizations realize that simply entering a user ID and password is no longer adequate and are experimenting with two-factor authentication.
In addition, IAM has evolved to the point that solutions can be business enablers, allowing the organization to aggregate identities across the enterprise into a single view, simplify user access to multiple applications, reduce IT costs and increase productivity. Organizations are beginning to look at IAM for customers (i.e. using IAM tools for customer identification). On a final note, IAM processes and practices tend to be expensive and thus require buy-in from the lines of business to ensure its success. The security function needs to learn how to sell itself in order to get the required funding for IAM initiatives.

As organizations lose confidence in their ability to protect themselves against internal threats, data loss prevention takes on new urgency

Respondents state that data protection is their second highest priority after IAM. The greatest percentage (42%) is only "somewhat confident" in their ability to thwart attacks that originate internally and only 34% are "very confident". There is a marked difference between internal and external attacks – a respectable 56% state that they are "very confident" in their ability to thwart external attacks. Data loss prevention is a major undertaking that begins with the most time-consuming part: classifying existing information to identify what information needs protection and from whom. But as daunting as the project may be, organizations appear to recognize how crucial it is – respondents indicate that data loss prevention will be one of the most piloted technologies in the next 12 months. Both data protection as a priority and data loss prevention technology piloting show a rise from last year. Key issues around data loss prevention are access certification and data governance.

Regulatory compliance is a key priority for financial institutions

Financial institutions are clearly expecting more regulatory pressure. They also recognize the competitive and reputational requirement to meet – or exceed – industry "leading practice" and standards set by associations such as ISACA, ISO, IIA, etc.

Respondents to the survey include regulatory and legislative compliance as one of their top five initiatives and are hiring more internal auditors to resolve internal and external audit findings.

* Downloaded from http://www.theglobeandmail.com/news/technology/canadian-firm-helps-disable-massive-botnet/article1488838/on March 10, 2010)

For the first time in the history of the survey, information security compliance remediation based on the findings of internal and external auditors is one of the top five security initiatives of organizations. Although "lack of oversight and compliance to security control requirements" is far down the list of internal/external audit findings (only 13%) organizations are shoring up for the anticipated increase in regulation. This is a clear indication that the environment has moved from one of "tell me you're in control" of significant financial and non-financial risks to "prove to me". Therefore, the need to be able to evidence this at any time for regulators, in particular, and as part of good governance practice, is an enterprise-wide issue for financial institutions.

While organizations are increasingly recognizing the need for a formal security strategy, the alignment of security and business objectives is lacking

It is not the existence of a security strategy that is at issue in financial institutions in 2010 (87% of respondents have one or plan to have one within the next 12 months; only 12% do not have one at all). What is more pertinent is that many organizations' security functions do not get input or involvement from the lines of business when the security strategy is being developed, which means that the strategy tends to be security function driven rather than business goals driven. This is clearly not the ideal situation and one that thwarts continued visibility and recognition of the value of the function. In addition, more and more organizations have a centralized security function, which is a positive development from a protection standpoint but may also prevent organizations from collecting feedback from the lines of business. Consequently, security goals are not aligned with those of the business and the security function suffers from lack of impact and business alignment. The absence of clear measurable security metrics that can be understood by lines of business means that the security function cannot clearly demonstrate its value and consequently may have a hard time getting funding for important projects. While 65% of respondents maintain that they actively engage both lines of business and IT decision makers in their security strategy, that still means that at least 30% of organizations do not. Predictably, only 37% of respondents maintain that business and information security initiatives are "appropriately aligned."

Involving business in the creation of the security strategy takes perseverance, consistency and some short-term pain to realize benefits that extend well into the future. The security strategy – developed and utilized in the right way – is the key to changing the profile of the security function.

Security budgets appear to be bucking the current trend of cost-cutting

The survey reveals that, in 2010, despite the global economic downturn of the past two years, there is a significant drop, as compared to last year, in the number of respondents who state that "lack of sufficient budget" is a major barrier that their organization faces (only 36% of respondents this year versus 56% of respondents last year). This may well be a product of a general dawning of the realization that, as the information security environment gets more dangerous, investment in data protection must get more serious. Given this, the security function must now be prepared to demonstrate ROI to further cement this trend. Top spending priorities in 2010 include identity and access management (IAM), data protection, security infrastructure improvement, regulatory and legislative compliance, and information security compliance remediation based on the findings of internal and external auditors.

Security technologies are experiencing a new maturity and a higher profile

There was a time when executives of financial services institutions viewed investment in emerging technologies as unnecessary and risky "budget gobblers". They were content for their organizations to be considered "late adopters" of technology, the theory being that it was more cost-effective to invest in technologies only after they were tried and true. In 2010, that scenario appears to be no longer valid. There are a number of reasons for this shift in attitude. First of all, technologies are much more mature. As an example, early versions of logging/monitoring tools generated endless reports that were of little value. Current technology allows the aggregation of events and automates their analysis.

In addition, Security Information and Event Management (SIEM) is one of the fastest growing segments of the market according to analysts. SIEM solutions analyze security event data in real time to identify threats, and analyze and report on log data for compliance monitoring. With SIEM solutions, gone are the endless reports that caused IT security teams to drown in security event data and lose control of corporate security. Another reason for the higher profile of emerging technologies is that, as revealed by the survey, spending on IT security has remained a priority for organizations. That makes it easier for organizations to improve security infrastructure and invest in products for which they previously had no room in their budgets. The other reason for the changing scenario is that more than 70% of survey respondents indicated they are planning to implement at least one information security-related technology in the next 12 months.

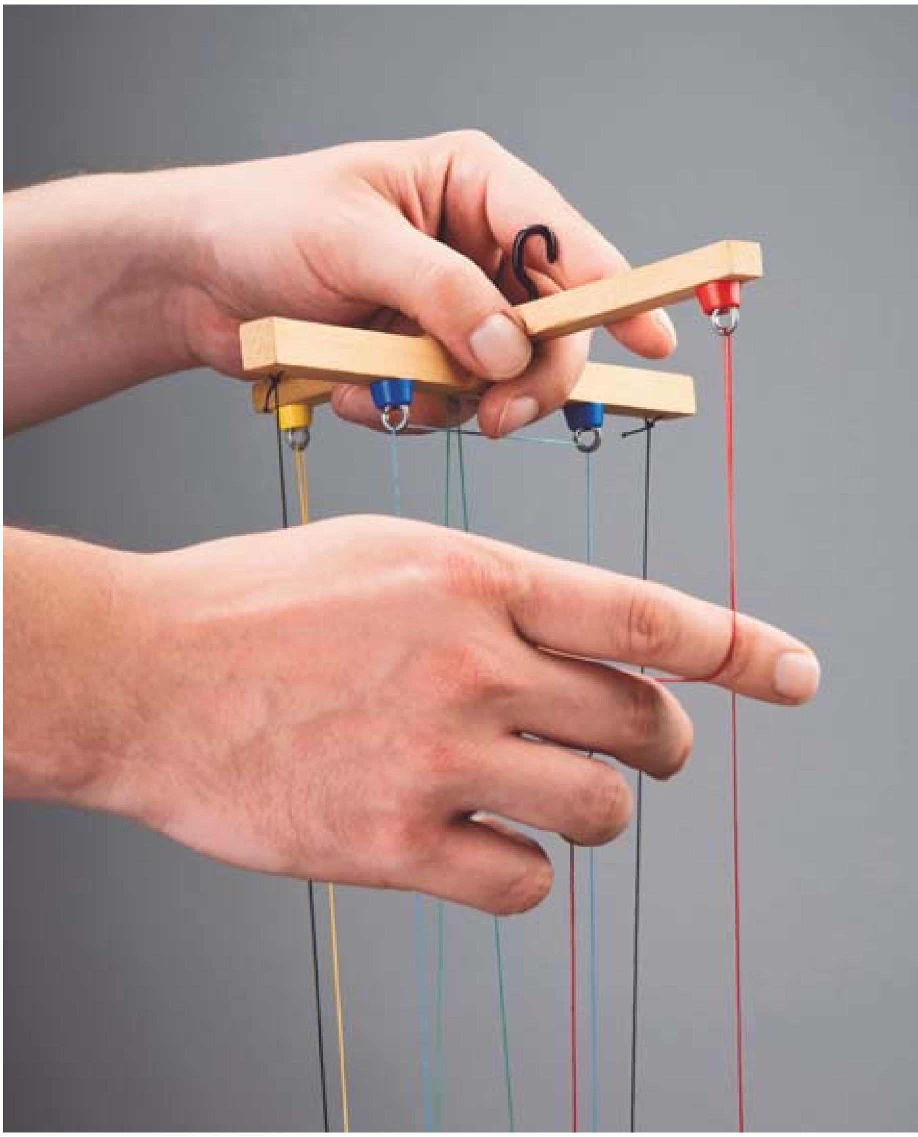
Given the increasing sophistication of threats and the increasing volume of regulation, sitting back and waiting is now viewed as riskier than taking action.

Convergence between information and technology risk functions is moving from concept to reality

Back in 2006, when Deloitte's security survey of the global financial services industry first introduced a question related to convergence, the idea was very much a concept. In 2010, the survey reveals that, in four short years, convergence has come a long way. This result could be attributable to the fact that convergence (formal cooperation between previously disjointed functions and not simply merging the groups on the organizational chart) is now better understood. In the survey, more than 57% of respondents either use enterprise risk councils, have the separate functions report into one common executive or have structurally converged. Only 26% have not undergone a process toward convergence. This is a welcome trend for those in the industry since the advantages of convergence, such as aligning security goals with corporate goals, a single point of contact, and increased information sharing are a clear benefit to the organization.

Paper-based information remains a low priority for the CISO

Paper is still the most prevalent information medium, and paper is still considered the legal copy of record in many disciplines. Yet the responsibility for the protection of paper-based information in organizations appears to have fallen through the cracks. Only 59% of respondents state that assets in physical form, i.e., paper, are within the mandate and scope of the CISO. However, this is an increase from the previous year (45%) and may also support our previous assertion that convergence is becoming more of a reality. Recognition of the risk that paper-based information poses indicates a greater understanding of information security as different from IT security.



Geography as a factor in security practices

	2009 Global	2010 Global	APAC (excl. Japan)	Japan	LACRO	EMEA (excl. UK)	ME	UK	USA	Canada
Respondents who indicated that their information security executive reports to the CIO	33%	24%	22%	🟦 0%	18%	26%	20%	15%	🟩 45%	24%
Respondents who feel they have both commitment and funding to address regulatory security requirements	59%	62%	🟩 74%	🟦 30%	48%	64%	61%	60%	74%	71%
Respondents who indicated that they have a documented and approved information security strategy	61%	60%	🟩 71%	65%	54%	61%	🟦 47%	50%	55%	56%
Respondents who feel that information security and business initiatives are appropriately aligned	32%	37%	🟩 56%	35%	34%	35%	38%	40%	🟦 33%	35%
Respondents who indicated that their information security budget has increased	60%	56%	56%	🟦 16%	64%	53%	56%	70%	56%	🟩 76%
Respondents who indicated that their expenditures on information security were ‘on plan’ or ‘ahead of requirements’	43%	45%	50%	40%	🟩 58%	41%	🟦 27%	50%	30%	53%
Respondents who feel that their internal staff have all the required competencies to handle existing and foreseeable security requirements	34%	45%	49%	🟦 20%	37%	🟩 50%	42%	45%	45%	44%
Respondents who have one or more executive(s) responsible for privacy	57%	53%	37%	🟩 100%	30%	42%	🟦 11%	60%	77%	71%
Respondents who have a program for managing privacy compliance	48%	50%	44%	🟩 95%	24%	44%	🟦 17%	55%	70%	71%
Respondents who train employees to identify and report suspicious activities	71%	64%	🟩 83%	🟦 35%	62%	59%	58%	75%	82%	62%
Respondents who included Identity and Access Management into the list of their priority initiatives for 2010	54%	44%	42%	65%	38%	35%	🟦 15%	35%	🟩 67%	62%
Respondents who are very or extremely confident in their third parties’ security practices		36%	29%	🟩 90%	40%	33%	35%	15%	🟦 6%	41%
Respondents who fully implemented encryption for mobile devices		44%	42%	50%	🟦 12%	42%	13%	🟩 80%	61%	65%
Respondents who indicated that they have and maintain a loss event database		54%	53%	70%	43%	52%	🟦 40%	🟩 79%	68%	44%

🟩 Highest score 🟦 Lowest score

Asia Pacific (excluding Japan)*

Despite the fact that Japan is in the APAC region, for the purposes of this document we discuss Japan separately from the rest of APAC. Overall, APAC ranks higher than the global average on most issues. APAC is consistent with most other regions, with the exception of Japan, in having their CISO report to the Chief Information Officer (CIO), indicating that, as it is with the other regions, information security is viewed primarily as an IT function. Respondents report having 1 to 5 full time information security professionals (54%), slightly higher than the global average of 52%.
They have a documented and approved security strategy (71%), the best showing of any of the regions, and much higher than the global average of 60%.

The most unique feature about APAC survey participants is that they state they have both commitment and adequate funding to fulfill regulatory security requirements (74%). This is far higher than the global average of 62% and on par with the United States. APAC led the pack on the same question in last year’s survey as well. Since they have no funding issues, they appear to have security in check: the security strategy is in place, initiatives are aligned, and they have the time and resources for awareness training, which has helped them get up to speed on competencies. APAC has made a big leap in this area.

* For the purposes of this document, we have separated Japan from the rest of Asia Pacific

This year, 49% of respondents reported that their internal staff had the required competencies to handle existing and foreseeable security requirements, a huge improvement over 34% last year and higher than the global average of 45%. APAC also leads in training employees to identify and report suspicious activities with 83%, far higher than the global average (64%) and slightly higher than the United States.

The only "red flag" issue for APAC may be in the area of privacy. Along with LACRO, they have the highest number of respondents (23%) who state that they have no privacy program in place. When posed the question "Who does your organization's executive(s) responsible for privacy report to?" a high 61% of respondents state that they did not know.

APAC is one of few regions that have no lowest scores this year. It appears that when APAC respondents recognize a problem they do something about it. Privacy may be their issue to improve for the coming year.

Japan

Far more than any other region, Japan reports having their CISO report to the Board of Directors (50% versus a global average of only 10%). This may be due to the fact that board member composition is somewhat different in Japan from many other countries: board members of most public organizations are insiders, i.e., they are corporate executives, and the number of board members tends to be far more numerous than in other parts of the world. Although this situation may be slowly changing, many Japanese organizations still have boards comprised of insiders.

Respondents from Japan state that they have a documented and approved information security strategy, at 65%, slightly higher than the global average (60%), higher even than the United States and Canada (55% and 56%, respectively) and a big leap from last year.

But here is where similarity to other regions ends. Survey participants from Japan appear to have no commitment to the information security strategy and therefore little funding. In fact, responses to questions regarding budgets are mystifying: only 16% indicate that their information security budget has increased, a number that falls woefully short of the global average of 56% and the general trend of budget increases given the environment. They are the lowest of all regions in believing that their staff has required competencies (20%). Only 35% train employees to identify and report suspicious activities (versus the global average of 64% and much lower than APAC at 83%).

Japan's bright spot is privacy. They are far and away the leaders in the area of privacy: 100% have an executive responsible for privacy (versus the global average of 53%) and 95% have a program for managing privacy compliance (versus the global average of 50%). Japan is also the region most confident about third party security practices. Even though they do not adhere to information security practices that some consider to be most effective, Japan apparently had an uneventful year with no major scandals or data losses. This may simply be luck or it could be influenced by culture and language: integrity and honour are revered and celebrated attributes in Japan and the language barrier may also be an issue as most attacks on Japanese organizations have originated from outside Japan.

Latin America & Caribbean (LACRO)

LACRO had an impressive showing last year, leading the pack in many areas. This year, however, they have fallen to the middle of the pack in areas they led last year. In LACRO, as in other regions, the majority of respondents indicate that their executive responsible for information security reports to the CIO. LACRO is close to the global average (60%) in having a documented and approved security strategy (54%) but this is a surprising finding given that they led in this area last year. In addition, LACRO's lack of commitment and funding, at 48%, is second only to Japan's and much lower than the global average of 62%. LACRO ranks among the lowest regions who feel that information security and business initiatives are appropriately aligned, and this finding is consistent with their lack of commitment and funding.

> Japan's bright spot is privacy: 100% of respondents have an executive responsible for privacy and 95% have a program for managing privacy compliance.

As it is in APAC, privacy is an issue for LACRO – which comes as no surprise, given that there is little or no privacy legislation in the countries of the region and a dominant open and welcoming culture; in fact, they fare the worst in having an executive responsible for privacy (30% versus the global average of 53%) and in having a program for managing privacy compliance (24% versus the global average of 50%).

LACRO also scored among the lowest in having encryption for mobile devices (12% versus the global average of 44%) and in having and maintaining a loss event database (43% versus the global average of 54%). Clearly, without a loss event database, it is hard to have an accurate information security perspective.

A bright spot is that LACRO respondents (64%) indicate that their information security budgets have increased. This is higher than the global average of 56% and higher than at least three other regions. So while LACRO respondents are higher only than Japan in feeling that they do not have commitment and funding, it appears that there is an effort to right this issue through increased budgets.

EMEA (excluding U.K.)

As in all other regions, with the exception of Japan, the majority of respondents (26%) indicate that their executive responsible for information security reports to the CIO. The highest of all regions, EMEA respondents (50%) indicate that their security staff has all the required competencies to handle existing and foreseeable security requirements, higher than the global average of 45%. A respectable percentage of respondents (61%) indicate a documented and approved information security strategy, in line with the global average of 60%. EMEA respondents are slightly higher than the global average in having the commitment and funding to address security requirements (64%). While just over half of EMEA respondents (53%) indicate that their information security budget has increased, that number is still second lowest to Japan and below the global average of 56%.

EMEA respondents do not have a great deal of confidence in the security practices of their third parties, although, at 33%, there are still three other regions – U.S., U.K. and APAC – that score lower. EMEA is one of four regions that does not score the lowest of all regions in any one area.

Middle East

This is the first year that the survey includes the Middle East (ME) as a separate region given the tremendous response and interest shown in completing this survey. Overall, we note that ME has more lowest scores than any other region. While other regions across the globe have more robust security and privacy legislation, the ME has yet to implement comprehensive security regulations. For example, the region has yet to have any formal privacy regulation, thus the low score with regard to managing privacy; only 11% have one or more executive(s) responsible for privacy and only 17% have a program for managing compliance with privacy requirements.

In addition, responses from the ME indicated that the region is in fifth place, after the U.S., APAC, Canada, and overall EMEA, in feeling that they have both the commitment and funding to address regulatory security requirements. The ME also lags behind other regions in terms of having a formally documented and approved information security strategy (47%).

Deloitte believes that ME is the region where a lot is likely to happen in a short time – the UAE has recently established a Computer Emergency Response Team (aeCERT) and Saudi Arabia is investing heavily in security technology. Similarly, Central Banks in Qatar and Lebanon have issued circulars and directives on various security-related matters. Jobs for information security professionals in the ME abound on the internet and the region hosts various conferences and events featuring information security.

United Kingdom (U.K.)

For the most part, the U.K. looks a lot like EMEA in many areas. However, only 15% of U.K. respondents (the lowest number of all regions with the exception of Japan) indicate that their executive responsible for information security reports to the CIO. The majority of U.K. respondents state that the most common reporting line (20%) is to the Chief Operations Officer. There is an increasing trend in the U.K. of re-organizing security as part of a combined security/fraud/financial crime/physical security function reporting to a COO.

This would indicate a higher profile for the information security function, which seems to be at odds with the fact that the U.K. scores the lowest of all the regions in having a documented and approved information security strategy (50%) and below the global average of 60%. Surprisingly, however, even with the low numbers concerning the strategy, U.K. organizations indicate that they have had their information security budgets increased (70%), the second highest behind Canada at 76%.

The U.K. has always had enthusiastic and knowledgeable consumers of technology (they lead the world in the number of cellular phones per capita) so it is not surprising that they excel (and lead the pack) in fully implemented encryption for mobile devices (80% versus the global average of only 44%). The U.K. also leads the rest in having and maintaining a loss event database (79% versus a global average of 53%). This is not surprising since banks, under the operational risk requirements for Basel II, are required to systematically collect loss event data. Basel affects all banks and financial institutions whose regulating authorities adopt the standards and methods. Even financial institutions that are not subject to Basel often follow the banks' lead since Basel is seen as the ultimate standard.

U.K. respondents are in line with the global average (both 45%) in believing that they have the required competencies to handle existing and foreseeable security requirements.

But the survey findings reveal an interesting dichotomy about U.K. organizations. While they excel in encryption and risk management (loss event database), they pay little attention to IAM and, in fact, rank lowest of all regions (35%) and far below the U.S. (67%) in making IAM a top security initiative. All other regions indicate that IAM is either the top or in the top three of their security initiatives for 2010. Another interesting finding is that only 15% of U.K. organizations are confident in their third parties security practices, second lowest only to the U.S. at 6%, yet they excel in maintaining a loss event database.

United States (U.S.)

The majority of the U.S. respondents report having an executive responsible for information security, and this is the highest response among all regions at 91%.

The United States is the region where the greatest number of executives responsible for security report to the CIO, 45% compared to the global average of 24%. This finding cements the fact that the security function in U.S. organizations is considered hugely a technical function. U.S. respondents are the middle of the pack (55%) when it comes to having a documented and approved information security strategy. However, they score the lowest of all regions (33%) when it comes to the alignment of security and business initiatives, not surprising since many of their information security functions are considered part of IT. When information security is considered mostly a technical function within a centralized security model, there may be no representatives in the lines of business and therefore not enough interaction between security and the business.

While U.S. respondents indicate that they have the commitment and funding to address regulatory security requirements (74% and on par with APAC, the highest of all regions) the responses would appear to apply more to commitment than funding since, when asked to characterize their expenditures on information security, the highest number of U.S. respondents indicate that they are merely "catching up" as opposed to the highest number of other respondents who state that they are "on plan".

With increased regulatory expectations, "catching up" may indicate a problem for U.S. organizations in responding to regulatory pressures.

Many consider the United States, the home of Wall Street and the most powerful capital markets system in the world, to be the country most beset by financial scandals. Understandably, IAM is high on U.S. respondents list of priorities; at 67%, it is the highest of any region. This may partially explain why respondents say they are "catching up" in information security expenditures since IAM is expensive.

The U.S., the U.K. and Canada customarily rely on outsourcers to perform at least some of their internal functions but the U.S., of all respondents, has the lowest level of confidence (6% compared to a global average of 36%) in their third parties' security practices. That begs the question as to why they outsource to the degree that they do, particularly when they indicate that they have the required competencies to handle existing and foreseeable security requirements.

Understandably, given the terrorist attacks of 9/11 and subsequent thwarted attacks and threats, respondents from the United States were more likely to choose state or industrial espionage as a high threat (21%) compared, for example, to their close neighbor, Canada, where respondents rate this same category as 0%.

Canada

The country with a banking system that is often held up as an example of stability to the rest of the world has made significant security improvements over last year, with no lowest scores in any area. Canada is similar to all other regions (with the exception of Japan) in having its CISO report to the CIO. But despite the appearance of information security being a technical function, Canada reported the second highest number of respondents (71%) who believe that they have the commitment and funding to address security regulatory requirements. Canada is middle of the pack (56%) in having a documented and approved information security strategy but has improved in a number of areas over last year: security and business initiatives are more aligned (35% this year versus 28% last year); required competencies are increasing (44% this year versus 33% last year); and Canadian respondents must be celebrating the end of the recession: of respondents who indicate that their information security budgets have increased, Canada leads the pack with 76%.
In addition, there is a huge improvement over last year in expenditures being on plan or ahead of requirements – 53% this year versus only 26% last year.

But despite these improvements, Canadian organizations need to improve in some areas. They are below the global average in training employees to identify and report suspicious practices (62% versus 64%) and below the global average in maintaining a loss event database (44% versus 54%). Without such a risk management process, Canadian financial services organizations will find it difficult to be in compliance with increasing regulatory and industry requirements.

An area that is likely to become an issue for Canadian organizations is industrial espionage. Compared to U.S. respondents, who rated this threat as high, not one Canadian respondent felt it was a concern (0%). However, this may simply be a case of overconfidence or lack of visibility of the real threat. Some in the information security industry generally accept that the next major terrorist attack is likely to begin with a blackout and not with a bang. Despite its relatively benign profile on the world stage, Canada is inextricably linked with the U.S., its closest neighbor and greatest trading partner, and the Canadian government has not done nearly as much as the U.S. and U.K. governments in this area. This may be the "sleeper" threat of the decade and it is, in Deloitte's view, one that probably deserves far more attention.

Size as a factor in security practices

		Global	Employees		
			<1,000	1,000-10,000	>10,000
Governance and funding	Respondents where security executive has information in physical form included into mandate	59%	🟦 50%	63%	🟩 72%
	Respondents including disaster recovery planning into the list of functions of the executive responsible for security	49%	🟩 60%	46%	🟦 29%
	Respondents who have gone through a process of structural convergence between information and technology risk	25%	🟦 21%	25%	🟩 33%
	Respondents who have documented and approved information security strategy	60%	🟦 53%	61%	🟩 72%
	Respondents engaging both lines of business and technology executives in defining information security requirements	65%	🟦 60%	63%	🟩 81%
	Respondents who have established information security metrics aligned to business value and report on a scheduled basis	19%	🟦 16%	17%	🟩 28%
	Respondents indicating lack of sufficient budget as one of their major barriers	36%	36%	🟩 41%	🟦 29%
	Respondents who feel they have both commitment and funding to address regulatory security requirements	62%	🟦 57%	🟩 67%	64%
Threats, risks and mitigation activities	Respondents having excessive access rights in the top list of their audit findings	38%	🟦 32%	34%	🟩 56%
	Respondents who included Identity and Access Management into the list of their priority initiatives for 2010	44%	🟦 35%	44%	🟩 63%
	Respondents indicating increasing sophistication of threats as one of their major barriers	31%	31%	🟦 27%	🟩 41%
	Respondents who have fully implemented the following:				
	• File encryption for mobile devices	44%	🟦 36%	48%	🟩 57%
	• Vulnerability management	58%	🟦 53%	58%	🟩 72%
	• Federated identity management	16%	🟦 10%	20%	🟩 24%
	Respondents who are piloting data loss prevention technology	17%	🟦 13%	14%	🟩 29%
	Respondents who are planning to pilot or implement data loss prevention technology	26%	🟦 22%	🟩 34%	24%
	Respondents who train employees to identify and report suspicious activities	64%	🟦 53%	67%	🟩 79%
	Respondents who indicate that they have and maintain a loss event database	54%	🟦 48%	50%	🟩 78%

🟩 Highest score 🟦 Lowest score

Not surprisingly, large organizations are much more advanced in their security practices than medium or small organizations and the size of the security function is directly dependent on the size of the organization. However, there are some surprises in the size discussion and observations do not always follow a predictable pattern. For the purposes of this discussion, organizations with fewer than 1,000 employees are considered small; organizations with 1,000-10,000 employees are considered medium; and organizations with more than 10,000 employees are considered large.

The information security executive is more likely to report to the CIO in large organizations than small, probably because small organizations are less likely to have a CIO or the person who performs an information security role is likely to do the job of the CIO as well. There is evidence of strong information security practices in larger organizations.

Information in physical form, i.e., paper, is included in the information security executive's mandate of both large (72%) and medium (63%) organizations. This may well be attributable to the fact that, given recent breaches and incidents, large organizations realized they needed to adopt stronger security practices and went through revisions of their information security mandate, part of which involved assigning responsibility for data in various forms. Additionally, in small organizations, Disaster Recovery Planning functions – and we observe the same pattern for business continuity – are often included as part of the mandate of the information security executive (60%) versus for medium (46%) or large (29%), where this is handled by separate individuals. In small organizations, by necessity, the security function is more likely to take on additional responsibilities.

Organizations of all sizes are beginning to realize the need for a security strategy. The increasing sophistication and frequency of threats, the current environment of huge failures and restructurings, increasing regulation that is going to require the existence of a strategy are all factors that have induced large (72%), medium (61%) and small (53%) organizations to have a documented and approved security strategy. In addition, as organizations are adopting more technology, affecting functions outside security, e.g., IAM, they recognize that a security strategy ties everything together. As expected, large organizations (81%) feel the need to engage both lines of business and technology executives in defining information security requirements. This makes sense since they are engaging in large projects across functions. But small (60%) and medium (63%) organizations, where one would think the environment would make communicating and sharing information more conducive, tend to remain siloed when it comes to engaging business and technology.

Regardless of size, less than a third of organizations have established information security metrics aligned to business value and report on a scheduled basis, an area that last year's survey highlighted as needing attention as well. Large organizations (28%) are understandably ahead of medium (17%) and small (16%) organizations but the numbers for all are much lower than they should be. Clearly, measuring security is still an issue for all organizations. All of the organizations report excessive access rights as top audit findings (large: 56%; medium 34%; small: 32%), and it is especially true for large organizations with more people. As a result, large organizations (63%) are looking at IAM as a priority in 2010 but medium (44%) and small (35%) organizations are understandably restricted due to the cost of IAM.

Increasing regulation puts pressure on all organizations, particularly medium and small, because they need the resources to be able to respond to regulatory requirements. Large organizations obviously have more executive commitment but funding is likely to be tight because of the scale and type of projects that have to be implemented is greater than for small and medium. However, respondents in medium-sized organizations are most likely to indicate that lack of sufficient budget is one of their major barriers (41%) versus small organizations (36%) and large (29%).

When it comes to feeling they have both commitment and funding to address regulatory security requirements, medium-sized organizations, at 67%, are more confident than both small organizations (57%) who likely lack resources, and large organizations (64%) who are subject to more regulation. Medium sized organizations may be in the best situation: they have capabilities and resources but are not as heavily regulated as large ones and can escape the focus of attention.

The bad guys are very adaptable. In the earlier years, their targets were large banks and other financial institutions, the theory being that when they scored, they would score big. Now the fraudsters have changed their strategy since they are being thwarted more and more by large financial institutions with their new technology and savvier employees. Fraudsters appear now to forgo the big victory for a series of smaller ones and what better targets than small and medium organizations. They are even targeting functions and people, particularly within financial institutions, because they know they are less protected than those in the larger organizations. As a result, there is not a huge spread when respondents were asked to rate increasing sophistication of threats as one of their major barriers: large (41%); medium (27%); and small (31%).

When it comes to implementing technology, responses follow a predictable pattern: small organizations, who lack the required resources, score lowest and large organizations, with greater resources, score highest. But there are some interesting findings within the data. At 57%, large organizations score higher on implementing file encryption for mobile devices (versus 36% for small and 48% for medium). Understandably, large organizations have greater risk of information leakage through mobile devices because they have more of them. The response is also fueled by regulation; breach notification laws typically state that if the device lost is encrypted, there is no need to report the loss.

Questions regarding data loss prevention reveal some interesting findings. Predictably, organizations that are most likely to be piloting DLP are the ones with the larger workforce, greater volume of data, and typically more valuable data (29%) versus small (13%) and medium (14%) organizations. However, when it comes to planning to pilot or implement DLP, respondents who indicate the highest response are from medium-sized organizations (34%). This may well be because medium-sized organizations, without the budget flexibility, are waiting to see if the technology is mature and effective enough for their needs.

With a close to 80% response rate, large organizations are better than small (53%) and medium-sized (67%) organizations at training their workforce to identify and report suspicious activities. Obviously, the larger the workforce the greater the vigilance required. Larger workforces typically depend upon information security stewards to be able to prevent breaches, and detect and report them when they are happening.

When it comes to the issue of having and maintaining a loss event database, the responses are predictable: 78% for large organizations; 50% for medium organizations and 48% for small organizations. However, as we observed earlier, small to medium-sized organizations are increasingly the target of fraudsters. Recording and retaining internal risk data through a data base helps an organization to identify trends and continuously improve processes. Large organizations also need to be concerned with external risk data to understand and control their exposure and comply with regulation. For financial institutions, a formal program for managing risk data can drive growth through superior service delivery and improved decision making that is dependent on having the right data at the right place at the right time.

This is the first time Deloitte has included size-based comparisons in the study. The points made are ones Deloitte believes to be most interesting to readers. Additional data is available. Please contact a Deloitte member firm professional in your region for further insights.

Sector as a factor in security practices

	Global	Banking institutions	Insurance	Investments and securities	Payments and processors
Respondents where security executive reports to:					
• Chief Information Officer (CIO)	24%	🟦 21%	🟩 35%	24%	25%
• Board of Directors	10%	🟩 14%	8%	🟦 2%	5%
• Chief Executive Officer (CEO)	11%	11%	11%	🟦 10%	🟩 15%
Respondents who indicated that they have a documented and approved information security governance structure	76%	82%	76%	🟦 54%	🟩 86%
Respondents who have a centralized information security model	76%	79%	🟦 65%	76%	🟩 81%
Respondents who indicated that they have a documented and approved information security strategy	60%	🟩 70%	54%	🟦 46%	48%
Respondents who indicated that they experienced partial or full convergence between information and technology risk functions	76%	82%	76%	🟦 54%	🟩 86%
Respondents who included in their top security initiatives for 2010:					
• Information security governance	29%	28%	🟦 19%	🟩 41%	33%
• Identity and access management	44%	44%	🟩 51%	🟦 37%	38%
Respondents who indicated the following major barriers their organization face:					
• Lack of support from lines of business	19%	🟦 15%	🟩 32%	17%	24%
• Lack of sufficient budget	36%	32%	🟩 46%	39%	🟦 29%
Respondents who indicated that they have established metrics for information security function that have been aligned to business value and report on a scheduled basis	19%	🟩 24%	14%	🟦 13%	14%
Respondents who fully implemented file encryption for mobile devices	44%	42%	🟩 54%	46%	🟦 38%
Respondents who plan to implement data loss prevention technology	26%	25%	🟩 32%	29%	🟦 19%
Respondents who indicated that their organization trains employees to identify and report suspicious activities	64%	65%	🟩 74%	🟦 51%	57%
Respondents who identified risks related to third parties as part of information risk assessments	39%	37%	🟩 53%	🟦 27%	33%
Respondents who included third parties in the mandate and scope of security executive responsibilities	53%	53%	🟩 65%	46%	🟦 43%

🟩 Highest score 🟦 Lowest score

In Deloitte's "Banking and Securities Outlook 2010"* DTT member firms subject matter specialists named five major trends that they believe will dominate the financial services industry in 2010. Three out of five of these trends relate to topics discussed in this report. They are as follows:

- The extent to which new regulations may impact financial firm's business models.
- The call for continued efforts to improve governance and risk oversight, especially at the board level.
- Meeting the challenge of core IT systems and data aggregation.

The specialists note that banks are cooperating with regulators and are trying to anticipate the direction in which the new rules might go. This is supported by the survey findings: while the CIO remains the primary reporting relationship for banks (21%), the secondary one is the Board of Directors (14%). This is in sharp contrast to the other sectors – Insurance, Investments and Securities, and Payment & Processors – where Boards play a less significant role in security governance.

Banks dominate the other sectors in having a documented and approved information security strategy as well as an information security governance structure (70% and 82%, respectively).

While 86% of the Payments & Processors sector respondents have an approved and documented information security governance structure, that high number is not due to their anticipation of increased regulation but rather to their compliance with Payment Card Industry (PCI) Data Security Standards (DSS) requirements. Banks' increased focus on governance is also reflected in their response to the question on information security function effectiveness measurement: 24% of banks have established metrics that have been aligned to business value and report on a scheduled basis, while Insurance, Investment and Payments & Processors are well below Banks with 14%, 13%, and 14% respectively.

Top security initiatives for 2010 provide an interesting perspective on the differences in security governance between sectors. Organizations in the Investment sector state that they are planning to work on establishing information security governance (41%) – a finding that is supported by the low number of Investment organizations (54%) who have a documented and approved governance structure. Insurance organizations report a low 19% for this particular initiative. However, this is likely not because insurance organizations are so advanced on the security front but rather because they are the lowest of all sectors to have a centralized security model adoption (65%). Strong security governance reporting vertical becomes less important when security is governed in a decentralized fashion. The fact that insurance organizations seem to see nothing wrong with this would indicated that they are experiencing less pressure from regulators or standards bodies.

Banks and insurance organizations are relatively close in their approach to risk function convergence: 82% and 76% respectively have experienced at least partial convergence between information and technology risk functions. Investment organizations are well behind at 54%. Increased convergence was predicted in Deloitte's "Banking and Securities Outlook 2010"; however, this means increased oversight: "It is expected that more boards may introduce explicit charters setting up risk committees (or adding risk to the Audit Committee's responsibilities) and reporting structures to strengthen board oversight and make sure this is communicated to shareholders."*

Increased support for risk-related initiatives in banks is evident in the responses to the question on barriers to information security. Banking respondents who choose "Lack of support from lines of business" and "Lack of sufficient budget" are significantly lower than those of the other sectors, particularly insurance organizations. Payments and Processors are somewhere in the middle; most likely because data security is key to their core business and most of them are already operating under strict PCI DSS requirements.

The insurance industry's focus on third parties is reflected in their answers to third party-related questions: 65% of insurance organizations, the highest across all sectors of financial services, include third parties within the mandate and scope of the information security executive's responsibilities. Additionally, 53% of insurance organizations identify risks related to third parties as part of information risk assessments (banks are second with only 37% who do so). The focus of insurance organizations on third parties extends to suspicious behavior identification: 74% of insurance organizations train their employees to identify and report suspicious behaviors; banks follow with 65% whereas investment organizations and Payments & Processors trail significantly. One would think that banks would lead on most fronts, given that they, of all the sectors, are perceived to have the most liquid assets on hand. However, it is becoming clear that insurance organizations have the strongest practices around third parties of all financial institutions. One of the reasons is that they are compelled to address risks resulting from their diverse and mobile army of insurance representatives: 54% of insurance organizations have fully implemented file encryption for mobile devices versus only 42% of banks who do so. Another reason is that insurance companies hold, and their representatives transmit, confidential personal information about their clients. It seems to be less catastrophic to an organization's reputation to lose millions of dollars than it is to expose personal information.

Deloitte's "Banking and Securities Outlook 2010"* also predicted that "banks are likely to begin a phase of heavy new investment in their technology infrastructure". This fresh appetite for new technology and infrastructure is reflected in banking respondents' answers to technology- and budget-related questions. But yet again, the appetite of insurance organizations is even higher (but this may be because they have much further to come: insurance organizations are ahead of banks with plans to implement data loss prevention technologies (32% versus 25% of banks and 29% of investment organizations). The same trend is apparent when it comes to top initiatives: identity and access management is stated as a priority by 51% of insurance organizations, 44% of banks, 37% of investment organizations and 38% of payments & processors.

* http://www.deloitte.com/view/en_US/us/Industries/ Banking-Securities-Financial-Services/article/05ff8971f7a75210VgnVCM200000bb42f00aRCRD.htm

While this may indicate that insurance organizations are eager to catch up with banks in the level of protection of their information assets, these numbers may provide some insights for technology and solution vendors: second- and third-tier vendors are likely to have greater success and return on their effort in the insurance sector.

Overall, while banks appear to have a stronger security posture than other financial services institutions, insurance organizations are catching up fast and have an edge in dealing with third-party risks. Payments & Processors are strong in technology and areas that fall under PCI DSS but sometimes lack in other areas. Investments and securities organizations appear to be trailing across multiple domains.

This is the first time Deloitte has included sector-based comparisons in the study. The points made are ones Deloitte believes to be most interesting to readers. Additional data is available. Please contact a Deloitte member firm professional in your region for further insights.

Strong security governance reporting vertical becomes less important when security is governed in a decentralized fashion.

Security issues of 2010

Security management

The economic downturn and the resulting increased risk environment have turned out to be a boon for the profile of the information security function. Its importance to the organization is reflected in a number of areas such as reporting relationships, mandates, budgets, convergence of information and technology risk functions and is driven by factors we will discuss later on in the study. The survey results show that, while there is still a long way to go, organizations are starting to sit up and take notice and recognize the importance of the information security function to the business.

Overall, 80% of organizations in the survey have an executive responsible for information security, the same percentage as last year. What's different this year is the reporting relationship.

While the most common reporting relationship for executives responsible for information security remains to the CIO, at 24%, the response to the same question last year was 33%. So although the role still reports into the IT function (and therefore continues to be viewed as technical), it is clear that there is a marked decrease in this reporting relationship over last year. The next most common reporting relationship for the CISO is to the CEO (11%), and 10% of the respondents indicate that CISOs in their organizations report to the Board of Directors. Overall, with a decrease in reporting to the CIO and a slight increase over last year in reporting both to the CEO and the CFO, the information security function appear to be moving in the right direction in the organization.

The most prevalent mandate of the CISO is information security governance at 85%. A very good sign is that that CISOs' focus continues to be on strategy and planning (75%) versus operations although there is a slight drop in strategy and planning this year over last year (80%). Overall, the services delivered by the CISO continue to be geared towards strategy and governance rather than operations.

Chart 1. Reporting relationship of executive responsible for information security

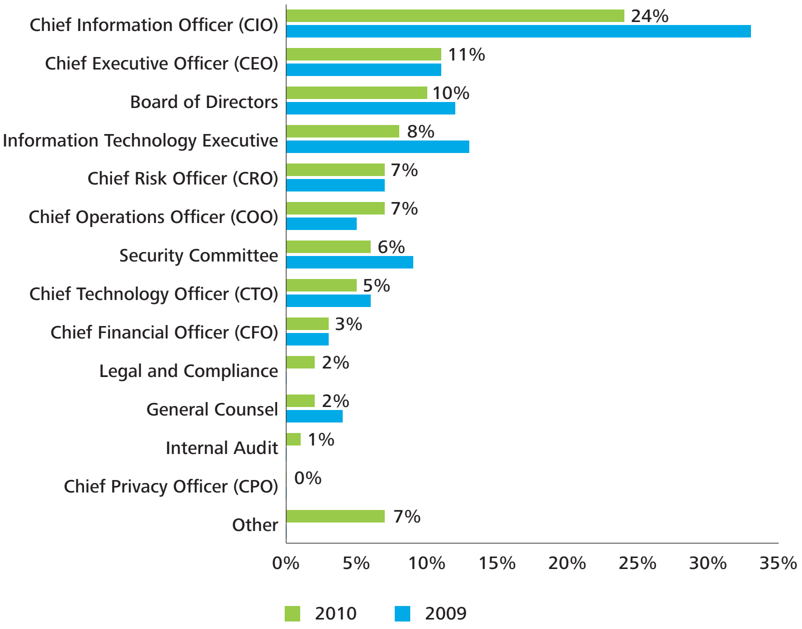


Chart 2. Functions within the scope of the executive responsible for information security

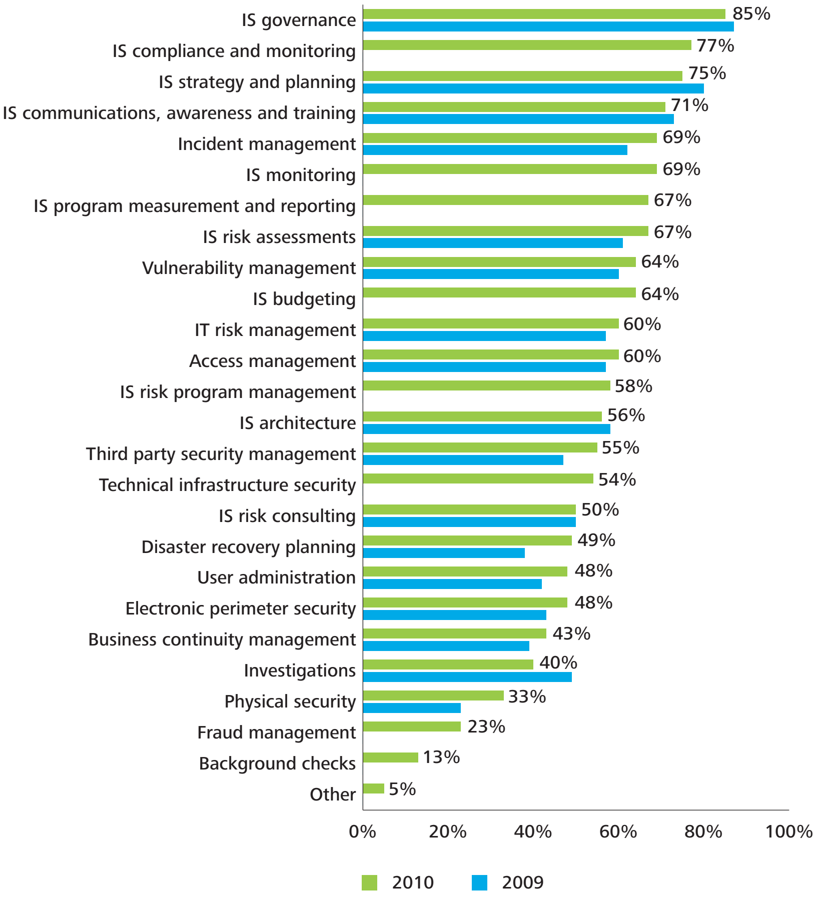


Chart 3. Assets included within the scope and mandate of the executive responsible for information security

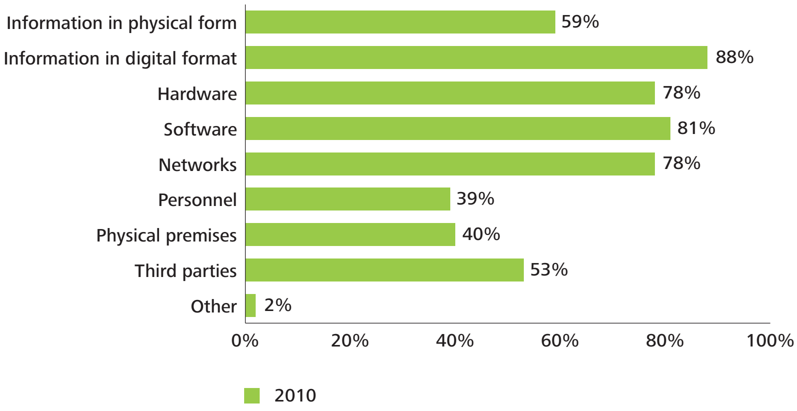
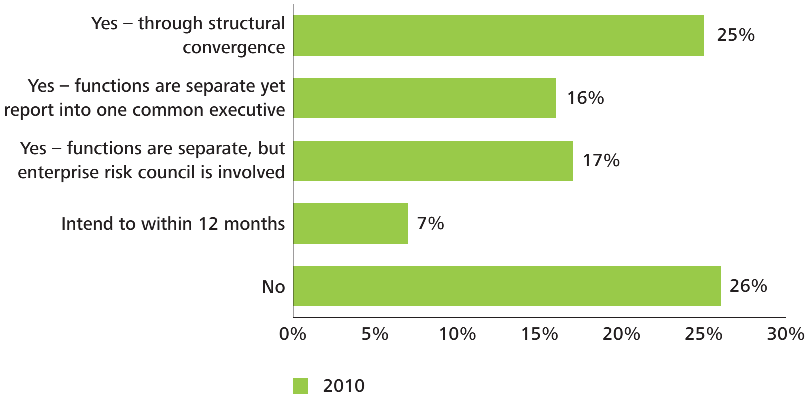


Chart 4. Organizations that have undergone a process of convergence of information and technology risk functions



A breakthrough was revealed in this year's survey. When respondents were asked to rank assets within the scope of the executive responsible for information security, it was no surprise that information in digital format was the primary responsibility, at 88%. And while physical assets, such as paper are still only at 59%, the breakthrough is that this is now indicated by more than half of respondents, a marked increase from 45% last year (the U.S. leads the pack this year with 70%). This is evidence not only of the expanding role of the CISO but also the move towards convergence between risk functions in the organization. However, there is clearly still a security gap around paper assets.

The new decade marks the first time that observers of the industry can truly say that convergence is happening. More than 58% of organizations have undergone some process towards convergence, whether through enterprise risk councils, structural convergence or with separate functions reporting to one common executive. Convergence of information and technology risk is highest in UK (75%) and in the U.S. (67%). Large organizations are more likely to experience convergence and small and medium-sized organizations have higher responses to no convergence: 31% and 25%, respectively.

Only 26% have not undergone any process towards convergence. Since having a total understanding of an organization's exposure to risk is so crucial these days and it is simply too expensive to have groups related to security working in silos, it appears that many organizations see convergence as a way to get a total security picture and save money in the process. Given the current threat environment and legislative requirements, convergence of risk functions may simply turn out to be the natural and logical state over time, like the globalization of the world.

As security functions mature and their mandates grow, there is evidence of convergence in a number of areas: the CISO's responsibility for physical security surging from 23% last year to 33% this year and physical assets such as paper increasingly part of the mandate of the CISO. However, one role that seems to maintain distance is that of the CRO. This link may become stronger in the coming years.

As in previous years, lack of sufficient budget is perceived as the primary barrier to ensuring information security.

But this year there is a difference. While 36% of respondents state this as a factor in 2010, that percentage has dropped considerably from last year (56%). It would appear that budgets are becoming less of a barrier as organizations recognize that they have to spend money to protect their information, evidenced by the increased interest in expensive projects such as IAM. The second most reported barrier is increasing sophistication of threats at 31% (last year 38%). For the first time, organizations appear eager to embrace emerging technologies to combat threats, previously avoided because of lack of maturity and expense. It may be an overstatement to say that information security budgets are recession-proof but they appear to be headed in that direction.

A documented and approved governance structure for information security is clearly not a barrier to ensuring information security. Only 7% of respondents do not have a documented and approved governance structure. The remainder either have one documented or approved (76%), intend to have one documented and approved in the next 12 months (11%) or have one documented but not approved (5%).

Chart 5. Major barriers faced in ensuring information security

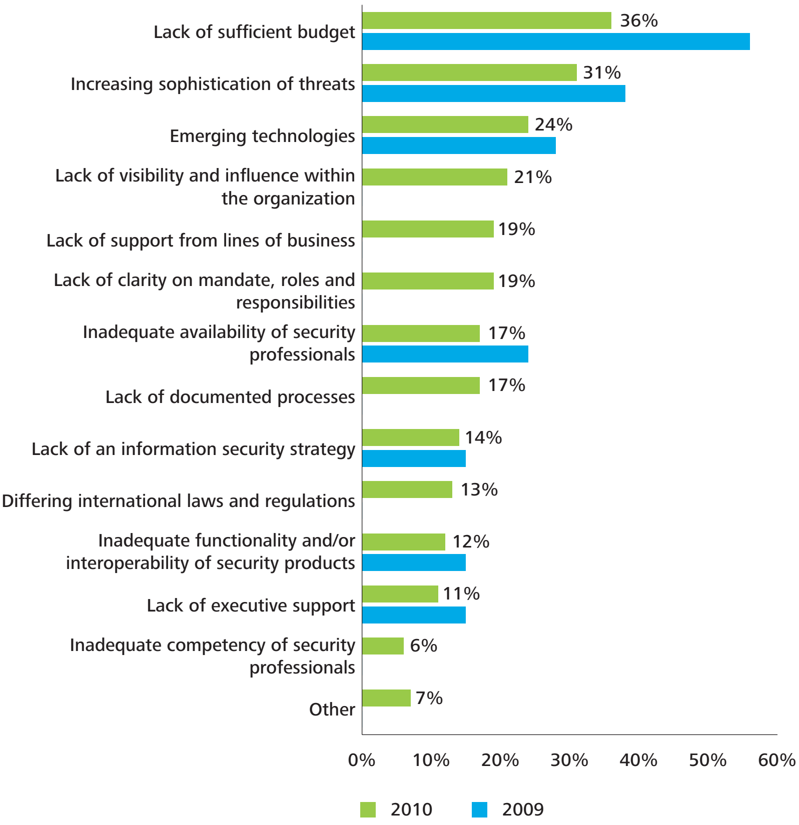


Chart 6. Existence of a documented and approved governance structure for information security

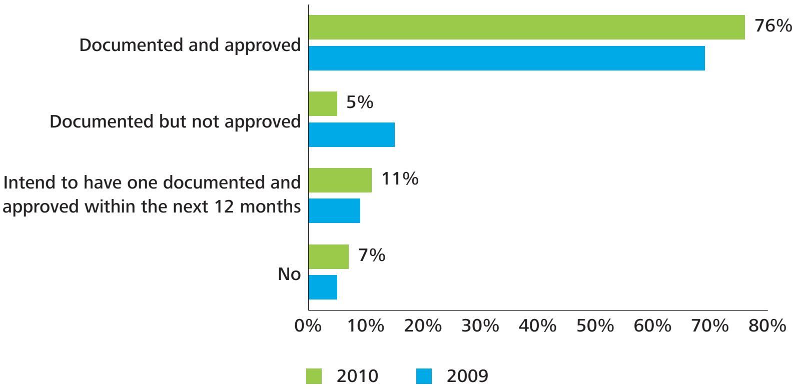
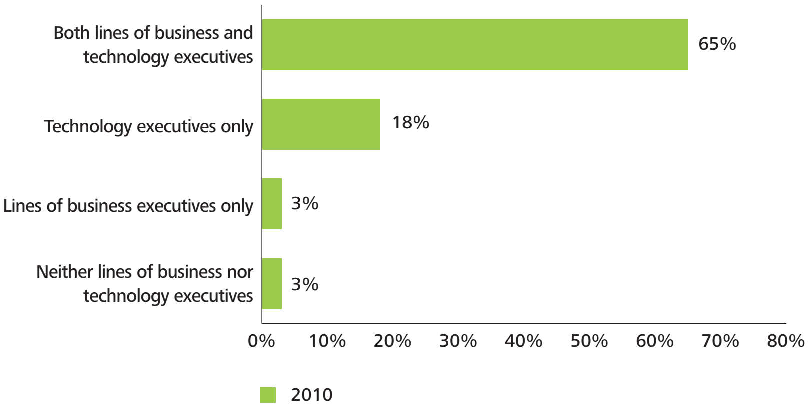


Chart 7. Frequency of reporting on the information security status of the organization to various groups

	Monthly	Quarterly	Semi-annually	Annually	Ad hoc	Never
Board of Directors	11%	18%	8%	18%	25%	9%
CEO	22%	18%	7%	11%	28%	5%
Senior and executive management	38%	23%	4%	5%	19%	2%

Chart 8. Who is engaged in identifying requirements for the information security strategy



A security strategy that starts out with input and buy-in from the lines of business means that, ideally, information security projects will map back to the organization's strategic business objectives.

The purpose of reporting by the information security function should be primarily to capture the attention of the business. But this does not appear to be happening.

For the Board of Directors, the most common frequency of reporting is ad hoc at 25% and quarterly at 18%. For the CEO, the most common frequency is ad hoc at 28%, and monthly at 22%. For senior and executive management, the most common frequency is monthly at 38%, with ad hoc at 19%. For both the Board of Directors and the CEO, reporting is more ad hoc than scheduled. Even for senior and executive management, 19% of respondents say that their reporting is ad hoc.

Ideally, for reporting to provide the most visibility for the function it should be scheduled, frequent and demonstrate the relationship between information risk and business success, particularly to the Board and C-suite.

The slow but steady progress that is reflected in responses to questions related to security management demonstrate that the information security function is moving towards recognition as a strategic necessity.

Business alignment

Business alignment starts with the basics: a documented and approved information security strategy. A security strategy that starts out with input and buy-in from the lines of business means that, ideally, information security projects will map back to the organization's strategic business objectives. But sticking to this takes determination, consistency and focus on the part of the CISO, who must make tough decisions about the kinds of investments that he or she is willing to support.

More than a half of respondents (60%) have a documented and approved security strategy. But when asked if they engage both lines of business and technology executives in identifying requirements for the strategy, only 65% of respondents state that they do.

If respondents consult only one group with regard to the security strategy, it is far more likely to be technology executives (18%) than lines of business executives (3%). Without the right level of involvement from the lines of business, security goals cannot be aligned with those of the business.

When asked how their organization's information security model is structured, respondents indicate that the most prevalent is centralized (76%).

A centralized security function is an effective means of enforcing security and protecting the organization at all levels, so the growth of centralized security model adoption may be a welcome change. However, being the sole source of security guidelines may also encourage security executives to limit the amount of feedback they collect from the lines of business. As a result, security function effectiveness may suffer due to lack of visibility and lack of alignment with business units' priorities and goals; this will also negatively affect the security function's ability to secure funding for critical projects. Even with a centralized security model, the leading practice is to have security resources embedded into or attached to the lines of business and geographic units to translate their requirements back to information security leadership.

Although it was mentioned previously that fewer respondents state that budgets are a barrier this year (36%) versus last year (56%), projects that adhere to the strategy approved by the lines of business (i.e., those that support the strategic business objectives) are far more likely to receive funding than those that do not appear to further business objectives.

It was stated earlier that more than half of respondents have a security strategy. But establishing strategic objectives, while an important step, is only part of the exercise. Performance against those objectives must be measured and the results used to demonstrate how well the function is doing in pursuing the strategy.

But only 19% of respondents state that they have established metrics aligned to business value and report on them on a scheduled basis; 33% are working on establishing metrics and aligning them to business value. However, nearly 20% either have no measurement or very little and another 21% have established metrics that are technical but not well understood by functions outside information security and IT (which may as well be no measurement in terms of visibility in the organization). In the absence of clear metrics that can be understood by the lines of business, the security function cannot demonstrate its value and consequently, its visibility suffers.

Chart 9. Information security model structure

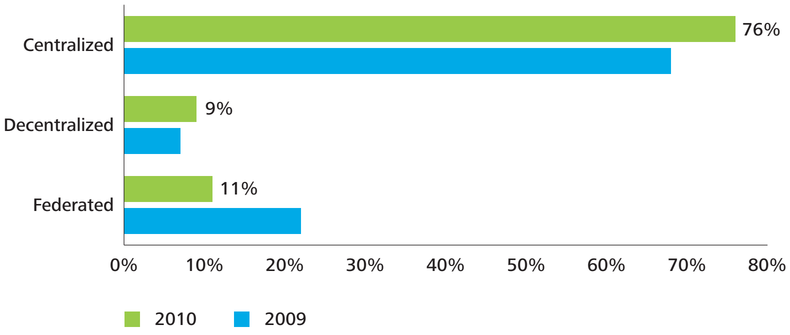


Chart 10. Measuring and demonstrating the value and effectiveness of the information security function's activities

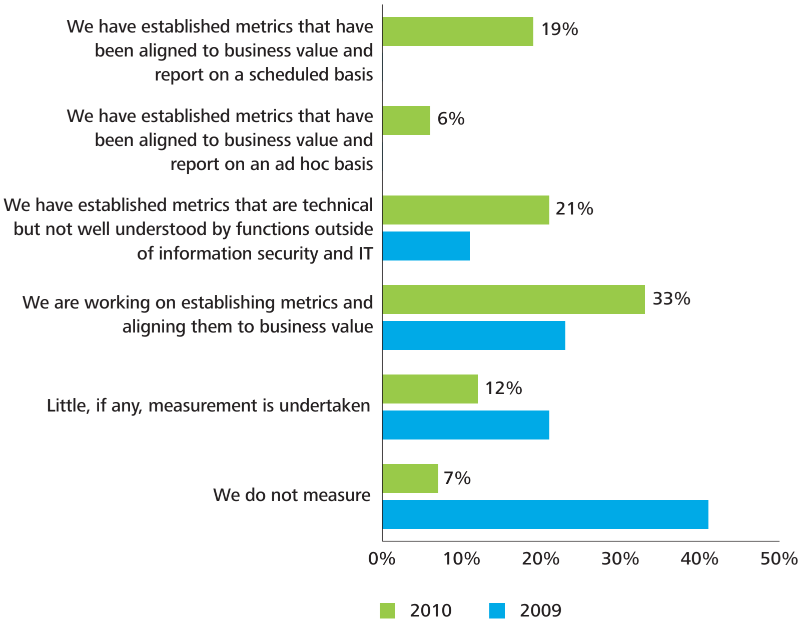


Chart 11. Effectiveness of information security function at meeting the needs and expectations of the organization

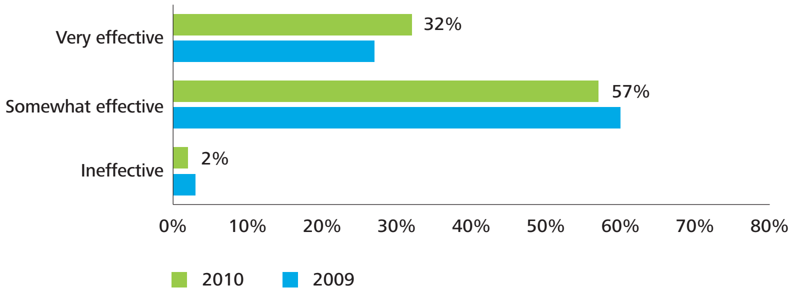


Chart 12. Extent to which business and information security initiatives are aligned with each other

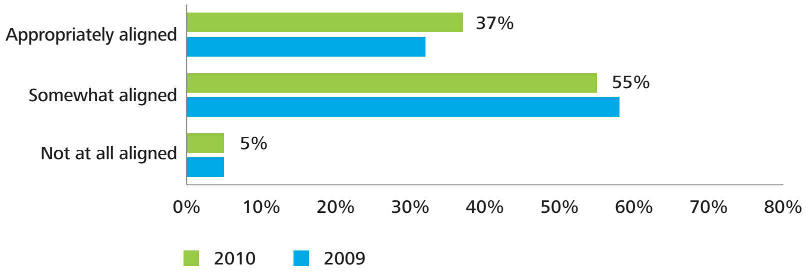


Chart 13. Year-over-year trending in the information security budget

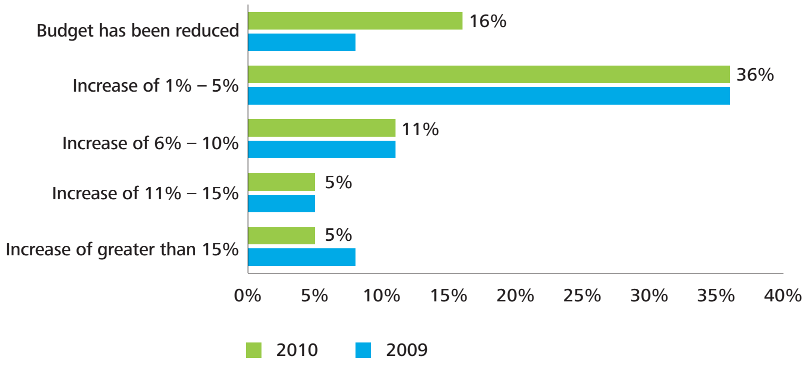
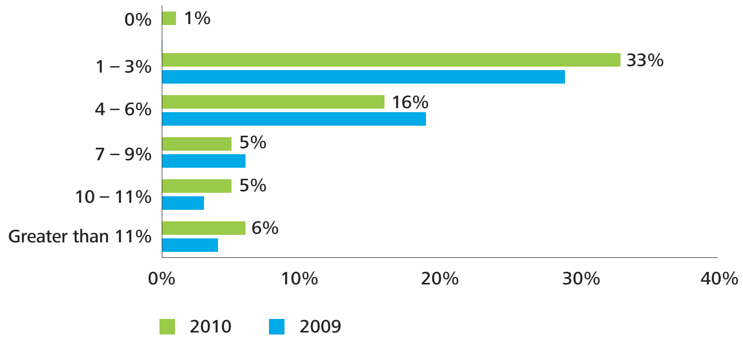


Chart 14. Percentage of organization's overall IT budget dedicated to information security



When respondents were asked to rate feedback from the lines of business and other internal sources as to how effective the information security function is at meeting the needs and expectations of the organization, the majority responded "somewhat effective", 57%, approximately the same percentage as last year. Only 32% could state "very effective".

When asked how their organization's business and information security initiatives align with each other, the majority of respondents (55%) indicate "somewhat aligned". Only 37% state that they are "appropriately aligned".

This gets back to one of the greatest challenges facing the information security function: demonstrating value to the business. The business is on the front lines, acting with competitive urgency. The information security function needs to demonstrate that it is aligned with the needs of the business, not sheltered from the marketplace doing its own thing.

Security budgets/economy

A quote from Charles Dickens might best describe security budgets and the economy: "It was the best of times, it was the worst of times, it was the age of wisdom, it was the age of foolishness…"* Despite the worst economy in decades and a lot of budgets being reduced in all areas, the information security function appears to be flying under the cost cutters' radar, a fact that may speak to a new regard for the value of the function.

Only 16% of respondents state that their information security budgets have been reduced while 36% indicate an increase of between 1% to 5%. While this is not a large increase, it is still an increase in a time when most budgets are being cut.

When asked what percentage of their organization's overall IT budget is dedicated to information security, 33% indicated 1%-3%.

* A Tale of Two Cities,
Charles Dickens, English
Novelist (1812-1870)

When asked how they would characterize their organization's expenditures on information security, the greatest percentage of respondents state that they are on plan (41%), a slight increase over last year. "Catching up" was indicated by 32% of respondents.

When asked whether information security professionals have the required competencies to handle existing and foreseeable security requirements, 45% of respondents indicate that they do; 24% of respondents indicate that their staff is missing some competencies but adequately closing the gap through training and development.

That means that nearly 70% of respondents feel that their security requirements can be handled in-house. However, when asked about their major expenditures covered under the information security budget, respondents indicate that software, hardware and consultants/contractors are their greatest expenditures (66%, 62% and 61%, respectively).

One might wonder, since most respondents say their people are skilled enough, why contractors would be a major expense, not to mention the level of risk that they might add. But it is possible to have a full complement of required competencies, especially for day-to-day security operations and still use consultants for specific projects.

The information security function needs to demonstrate that it is aligned with the needs of the business, not sheltered from the marketplace, doing its own thing.

Chart 15. State of expenditures on information security

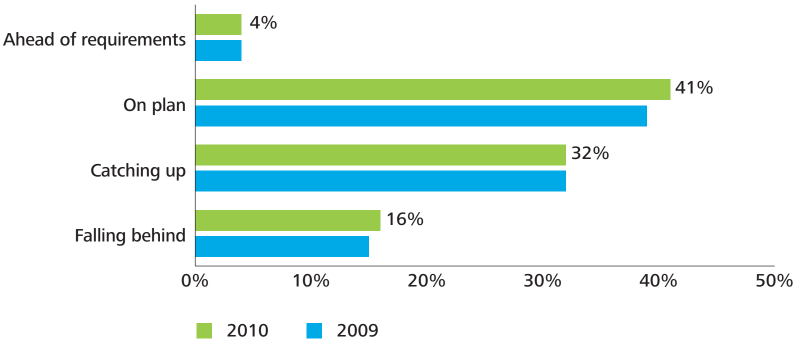


Chart 16. Required competencies to handle existing and foreseeable security requirements

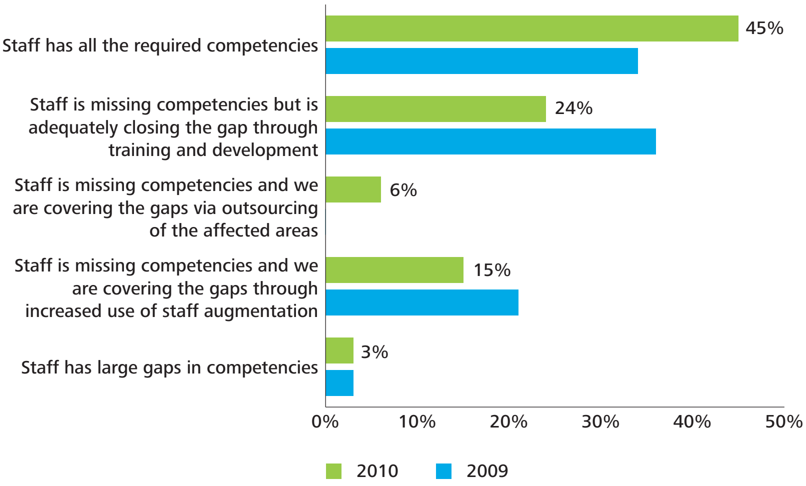
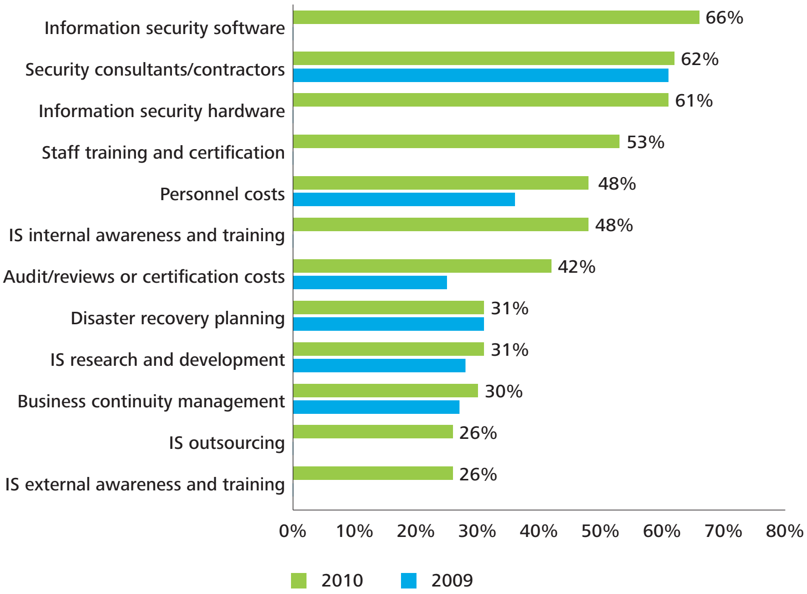


Chart 17. What is covered under the information security budget



Threat landscape/cybersecurity

In 2010, the threat landscape is more dangerous and more threatening than it has ever been before. For the most part, the children are gone and the big guns (government, organized crime) are in. The battle for your information is now high-stakes cyber warfare played out in every corner of the world. The threat lexicon continues to build at a dizzying rate: botnets, zombies, malicious PDFs, targeted attacks, hacking groups, spear phishing … the list continues. In his speech on May 29, 2009, U.S. President Barack Obama estimated annual world-wide loss from intellectual property theft by cyber criminals alone at $1 trillion.*

As in previous years, people are the organization's greatest worry – the ultimate "can't live with them, can't live without them" scenario.

Chart 18. Confidence that your organization's information assets are protected from internal and external attacks

	Extremely confident	Very confident	Somewhat confident	Not very confident	Not confident at all
Attacks originating internally	5%	34%	42%	16%	2%
Attacks originating externally	15%	56%	25%	3%	1%

When asked to rate their level of confidence that their organization's assets are protected from an attack, the greatest number of respondents (42%) indicate that they are only "somewhat confident" they are protected against internal attacks versus 25% who are "somewhat confident" they are protected against external attacks. Only 34% said they were "very confident" about being protected against internal attacks versus 56% who said they were "very confident" about being protected against external attacks. And this loss of confidence in internal people is a trend; almost 50% in last year's survey indicated that they were only "somewhat confident". Some new scams have appeared on the horizon described by a pair of similar words that have entered the security lexicon: cyber mules and cyber moles. Cyber mules (or money mules) unwittingly carry out illegal acts for hackers.

As an example, a recent story describes how consumers are lured into fake working-at-home scams that require them to receive money transfers and then forward the funds to Eastern Europe, either directly or through other cyber mules.* Cyber moles are internal individuals who steal corporate data. In other words, the illegal actions of cyber mules are inadvertent; the illegal actions of cyber moles are deliberate.

Despite the external environment, and as concerned as organizations are about it, human failings – carelessness, laziness, forgetfulness, fatigue, etc. – are more of a concern. It seems that organizations recognize that, despite the occasional disgruntled or malicious employee or third party, generally, their people are not "out to get them", they are just human. When asked to rate threats, respondents indicate that their highest threats are "non-intentional loss of sensitive information" and "increasing sophistication and proliferation of threats", both at 42%.

Financial institutions are now fighting on both fronts: externally and internally. As the external landscape gets more dangerous and threats get more ingenious and harder to detect, organizations worry more about their employee's inadvertent behaviour. And as individuals communicate and transact with each other more over the internet through emails, instant messaging, internet purchases, etc. there is a greater and greater potential for information to fall into the wrong hands. Deloitte member firms are receiving multiple requests for information on leading practices in content filtering, use of social media, data leakage protection – organizations world-wide are definitely concerned, and are taking steps towards protecting their valuable assets.

But in many cases organizations themselves are the enablers of mistakes on the part of their own people. Excessive access rights was the top internal/external audit finding at 38%. Employees routinely have access to more information and applications than they need to do their job. If an employee is dismissed on Friday, he or she may have access to the organization's information until Monday, when the IT group gets the directive from Human Resources to remove that person's access privileges. A contractor may fulfill a contract within the organization but that person's access rights may linger long after the contract is completed. Organizations tend to be overly generous with access rights so as not to impact employee productivity. But any productivity gains may pale in comparison to the negative consequences of a security breach. The issue of excessive access rights represents a huge gap in the information security for most organizations.

* downloaded from http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/on March 27, 2010

** downloaded from http://voices.washingtonpost.com/securityfix/2009/11/fdic_uptick_in_money_mule_scam.htm downloaded on March 27, 2010

In 2009, it was estimated that there were 30,000 new malware programs detected per day.* Malware is becoming much harder to detect and malware automation is likely to make attacks more frequent. Botnets are considered to be the major security threat on the internet. A botnet is a group of infected machines (also called zombies) that are controlled by the owner or the software source, called the "botmaster". Once the malicious software has been installed in a computer it becomes a zombie, and is totally controlled by the commands of the botmaster. Botnets can bring down servers, infect millions of computers with spyware and other malicious code, be used as agents for identity theft, steal company secrets, send out of spam, and engage in click fraud, blackmail, and extortion. In a recent Fortune 500 attack, criminals placed custom coded malware, that had specific IP address targets, hardcoded and hid the code using "near normal" appearing system file names, dates, and sizes. And botnets aside, attacks against social networking sites were a growing trend last year, as were attacks via peer-to-peer networks. Understandably, IAM and data protection are top security initiatives for 2010 and data loss prevention is the technology that most organizations plan to deploy in the next 12 months.

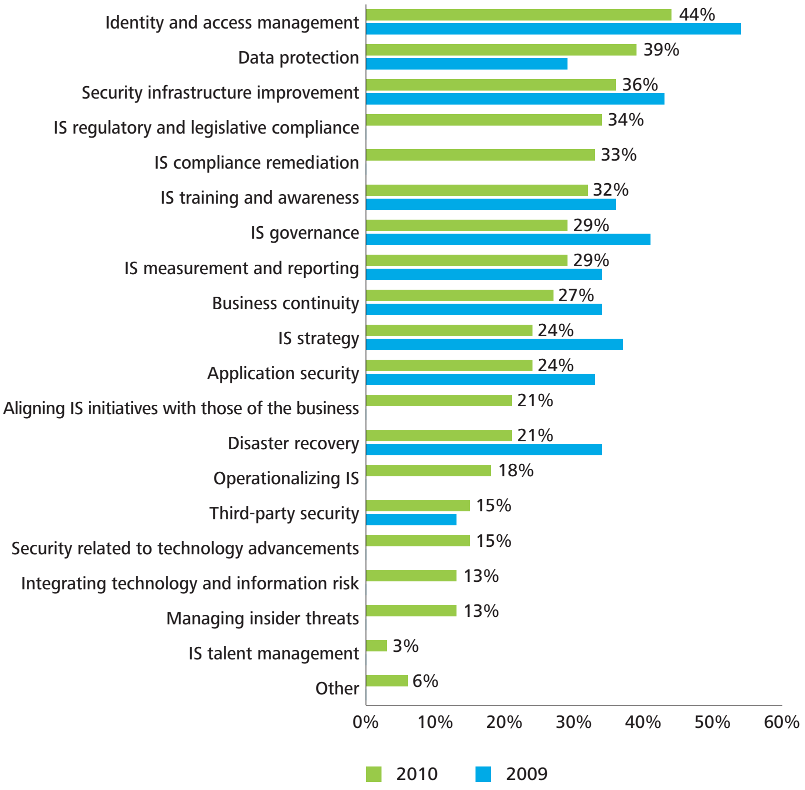
Training is obviously not effective if intent is malicious but it does change behaviour when loss is non-intentional, which is what organizations are most concerned about. Our survey shows that training and awareness are on the rise, especially when combined with enforcement and consequences. Training and awareness in such a context are very effective at changing behaviour and attitudes – one only has to look at the progress of recycling programs in North America, so successful so quickly that some cities experienced sharp budget shortfalls due to a decline in refuse revenues.

Data protection is a top security initiative with information security awareness and training rounding out the top six.

Chart 19. Threat perception

	Low	Medium	High
Increasing sophistication and proliferation of threats	9%	46%	42%
Non-intentional loss of sensitive information	14%	40%	42%
Phishing, pharming and other related variants	14%	49%	35%
Employee abuse of IT systems and information	16%	48%	33%
External financial fraud involving information systems	27%	38%	33%
Exploits of vulnerabilities in emerging technologies	20%	44%	32%
Attacks exploiting vulnerabilities of end point devices	18%	47%	32%
Attacks exploiting vulnerabilities due to unsecured code	19%	47%	31%
Social engineering	18%	49%	30%
Employee errors and omissions	11%	56%	30%
Security breaches involving third party organizations	21%	49%	27%
Zombie networks	22%	49%	25%
Attacks exploiting vulnerabilities due to unsecured code	27%	48%	22%
Differing cultural interpretations of security positive behavior	26%	49%	22%
Insider and rogue trading	28%	52%	15%
State or industrial espionage	55%	33%	10%

Chart 20. Top security initiatives



* Downloaded from http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1420681,00.html on March 14, 2010

Chart 21. Training for employees to identify and report suspicious activities

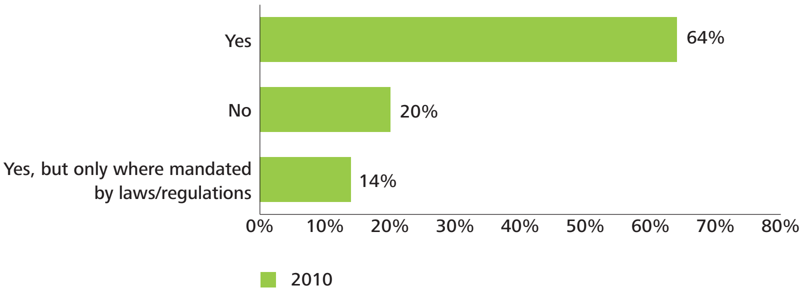


Chart 22. Customized IS training by job role and function

Customized training provided	Yes	No
Executives	32%	58%
People handling sensitive information	48%	45%
IT application developers and programmers	54%	38%
Systems administrators	56%	36%
Third party contractors	21%	60%

Chart 23. External breaches experienced in the last 12 months

	One occurrence	Repeated occurrences
Malicious software originating from outside the organization	14%	20%
Loss of information originating from a physical attack outside the organization	10%	10%
External financial fraud involving information systems	5%	9%
Breach of information originating from outside organization	7%	4%
Breach of information originating from a third party vendor	6%	4%
Theft of information resulting from state or industrial espionage	2%	1%
Website defacement	4%	1%
Mobile network breach originating from outside the organization	1%	1%
Other form of external breach	5%	4%

When asked if their organizations provide training to employees to identify and report suspicious activities, 64% responded that they did. Respondents are also focused on targeted training.

IT application developers and programmers are most likely to receive targeted training (54%) followed by people handling sensitive information (48%). Least likely to receive targeted training are executives at 32%.

When asked about external breaches experienced in the past 12 months, respondents cite repeated occurrences of "malicious software originating outside the organization" most often (20%).

Training and awareness are very effective at changing behaviour and attitudes – one only has to look at the progress of recycling programs in North America, so successful so quickly that some cities experienced sharp budget shortfalls due to a decline in refuse revenues.

Despite the ominous and dangerous external landscape, organizations that have sustained a breach report that losses are minimal.

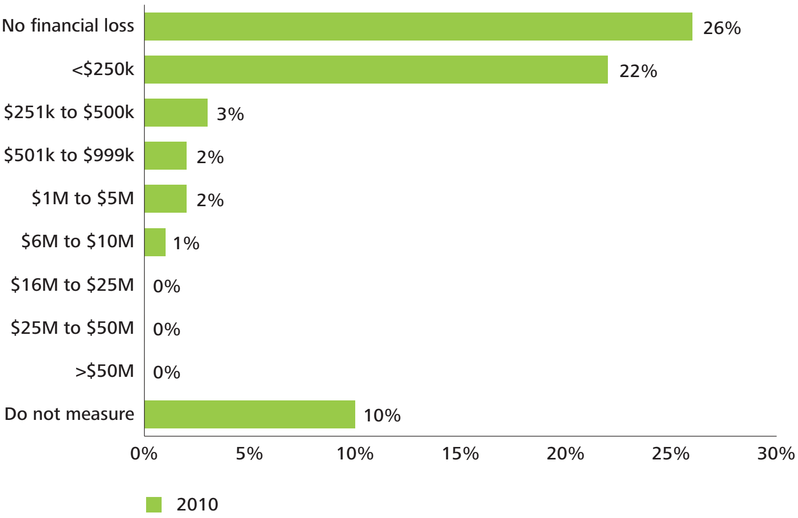
However, while 26% of respondents report no financial loss and 22% report a loss of $250,000 or less, the largest number of respondents (34%) chose the category "Not applicable/do not know". Organizations may simply not know what they don't know: only 54% maintain a loss event database and, of those respondents who answered the question about a loss event database, 41% comprise the two categories "do not have" or "not applicable/do not know."

The U.S. Identity Theft Research Center's 2007 Data Breach Statistics indicated that well over 127,000,000 records were exposed in 446 data breach incidents in 2007, and the Open Security Foundation reported that well over 83 million more were compromised in 2008.* When asked which attributes were included to determine the monetary damages suffered as a result of breaches in the last 12 months, 15% of respondents chose "internal investigation and forensic costs".

Chart 24. Internal breaches experienced in the last 12 months

	One occurrence	Repeated occurrences
Accidental breach of information originating from inside the organization	8%	11%
Malicious software originating from inside the organization	9%	10%
Breach of information originating from inside the organization conducted by an employee	11%	8%
Internal financial fraud involving information systems	7%	4%
Breach of information originating from inside the organization conducted by a non-employee	3%	2%
Breach of information originating from a third party vendor	3%	2%
Mobile network breach originating from inside the organization	1%	1%
Insider and rogue trading	2%	0%
Other form of internal breach	3%	3%

Chart 25. Estimated total monetary damages resulting from breaches over the last 12 months



* Downloaded from https://litigation-essentials.lexisnexis.com/webcd/app?action=DocumentDisplay&crawlid=1&srctype=smi&srcid=3B15&doctype=cite&docid=4+ISJLP+661&key=e6edb7eff741987c9ffcd1c5499c79d4 on March 14, 2010

Chart 26. Attributes included in the calculation to determine monetary damages as a result of breaches in the last 12 months

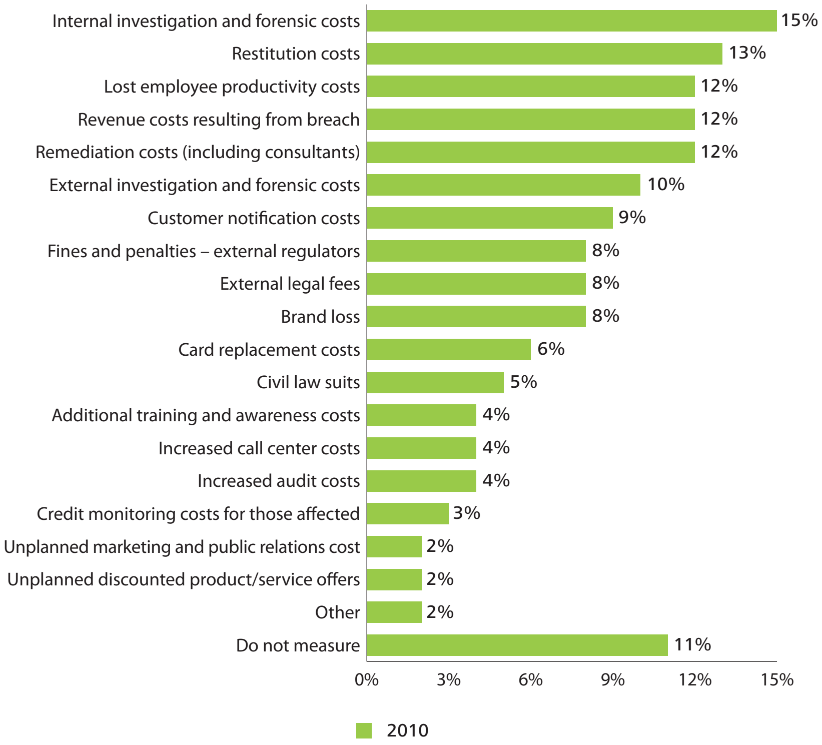


Chart 27. Frequency with which organization conducts specific testing or review

	Quarterly	Semi-annually	Annually	Adhoc	Never
Vulnerability scanning	40%	12%	14%	23%	6%
Internal penetration testing	15%	11%	21%	28%	19%
External penetration testing	16%	13%	31%	21%	14%
Penetration testing conducted by third party	13%	12%	38%	22%	10%
Application security code review	6%	3%	9%	46%	23%

Chart 28. Top security initiatives by sector

Global	Banking institutions, insurance companies	Investment	Payments & processors
Identity and access management	Identity and access management	Informantion security governance	Informantion security compliance remediation
Data protection	Data protection	Identity and access management	Data protection
Security infrastructure improvement	Security infrastructure improvement	Data protection	Business continuity

When asked how often their organizations conduct testing or review, the top response was vulnerability scanning conducted on a quarterly basis (40%). Penetration testing conducted by a third party annually was the next most popular response (38%).

However, responses to this question revealed a gaping security hole: 46% of respondents state that their application security code review is conducted only on an ad hoc basis. If the frequency is ad hoc the processes are likely to be informal or inconsistent. Since applications are not ignored by the hackers they should not be ignored by the organization.

Identity and Access Management (IAM)

Respondents indicate that identity and access management and data protection are their top two security initiatives for 2010.

The two go hand in hand: with strong IAM, data protection is more assured because the organization's people, without excessive access to information they do not need to do their jobs, are less likely to cause the "non-intentional loss of sensitive information" which organizations state is one of their greatest threats. Excessive access rights was the top internal/external audit finding this year and last year as well. Data loss prevention technologies were cited as the top technologies that organizations plan to fully deploy or pilot within the next 12 months.

The truth is that completely eliminating excessive access rights is almost impossible. However, that is no excuse not to have reasonable targets. Allowing an employee who leaves the organization to have access to the network two weeks later is not reasonable. Nor is allowing a junior Human Resources assistant to have access to payroll information about employees, including executives. But setting reasonable targets and sticking to them is difficult because the workforce is not static. Employees are hired, promoted (sometimes doing both jobs for a period of time) and fired; job requirements change; contractors come and go; off-site consultants (often in an unsecure environment) need access to documents and applications; mergers and acquisitions mean restructuring. The financial services industry is particularly hard hit: banks have failed and merged resulting in thousands of employees being laid off and those left behind taking on more work and heightened levels of stress. It's a lot to keep up with.

But IAM solutions are costly, particularly so for small and medium-sized organizations. "Lack of sufficient budget" is chosen by respondents as the top barrier to ensuring information security. But as long as the information security function does not learn how to sell itself, it will be difficult for it to get the budgets it needs. IAM is primarily a line of business project. But when asked how many actively involve both lines of business and IT decision makers in identifying requirements for the security strategy, only 65% do so.

When asked how effective the information security function is at meeting the needs and expectations of the organization based on feedback from the lines of business, only 32% of respondents state "very effective" with the greatest percentage, 57%, stating "somewhat effective". The word "somewhat" can cover a multitude of ills and that category likely includes some for whom the next choice, "ineffective", is simply too difficult to admit.

In addition, when respondents are asked to what extent business and information security are aligned with each other, only 37% state that they are "appropriately aligned". In order for projects such as IAM to get approved and underway, the lines of business need to have a vested interest in them.

Many financial institutions, particularly banks, continue to use user name and password for customers' authentication or password and "secret question", both of which are now considered weak.

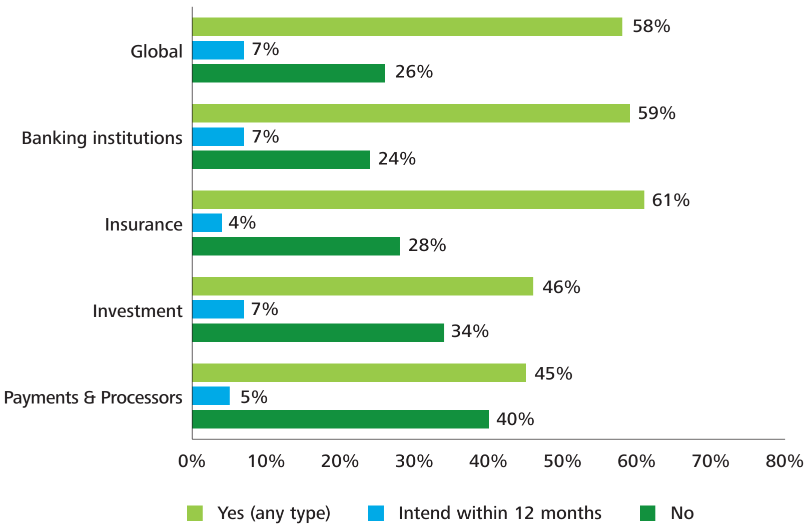
Chart 29. Top audit findings by sector

Global	Banking institutions	Insurance	Investment	Payments & processors
Excessive access rights	Excessive access rights	Excessive access rights	Excessive access rights	Lack of sufficient segregation of duties
Excessive developers' access to production systems and data	Lack of sufficient segregation of duties	Excessive developers' access to production systems and data	Lack of sufficient segregation of duties	Audit trails/logging issues
Lack of sufficient segregation of duties	Audit trails/ logging issues	Lack of clean up of access rules following a transfer or termination	Excessive developers' access to production systems and data	Lack of clean up of access rules following a transfer or termination

More and more financial institutions are looking into 2-factor authentication, which requires not only the user name and password but also another method of authentication such as a smart card in the user's possession or something unique to the user, such as a fingerprint. For those organizations who have customer-facing applications, the fine line they need to tread is how to convert to stronger authentication without inconveniencing and turning customers off. Since IAM is complex and expensive, there are those who suggest that the future of IAM might be in SaaS (Software as a Service) delivery, essentially outsourcing to save money (like computing power through mainframes in the 70s and 80s). However, while outsourcing might relieve the organization of responsibility for IAM, it does not relieve the organization of the duty to protect its data and stay compliant. Trying to comply with audits conducted off-site could add a whole new dimension of difficulty.

What is interesting is that respondents state that emerging technologies are the third most identified barrier to information security, after lack of sufficient budget and increasing sophistication of threats. However, when asked to identify their organization's top five security initiatives, respondents rank "security related to technology advancement" a low 14%.

Chart 30. Sector convergence



The world has changed and the stakes are higher in 2010. Organizations now need a holistic security solution capable of 360 degrees of protection.

Convergence

The question about convergence in this year's survey differs from those of previous years. In 2009, respondents were asked about the convergence of physical and logical security. This year, respondents were asked about convergence between functions mandated with technology risk and information risk responsibilities.

The question of convergence was introduced into the survey in 2006. Back then, the idea of convergence did not resonate with a lot of people. That may have been primarily because convergence was misunderstood. Many people saw it simply as putting together physical and logical technologies but could not understand how that was going to help productivity or business gains. In addition, convergence was considered an all or nothing undertaking: you either converged completely or you didn't at all. There was nothing in between.

But that was back when threats were perpetrated by teenagers and organizations were confident that they could handle what was out there. The world has changed and the stakes are higher in 2010. Organizations now need a holistic security solution capable of 360 degrees of protection. Security threats need to be addressed in tandem. People understand convergence better now. They understand that when it comes to security, the silo approach cannot be a good thing because that means that one group doesn't know what the other is doing or how things are going.

When asked if they had undergone a process of convergence ("Has your organization undergone a process of convergence between functions mandated with Technology Risk and Information Risk responsibilities?"), 58% of respondents indicated that they have, either through enterprise risk councils, through having separate functions report into one common executive or through structural convergence. Only 26% have not undergone a process towards convergence. Clearly, the responses to this question are very much dependent upon the size of the organization; this is an issue that is not likely to be relevant to an organization of 1000 people or less and the same would apply to many of the medium sized organizations as well.

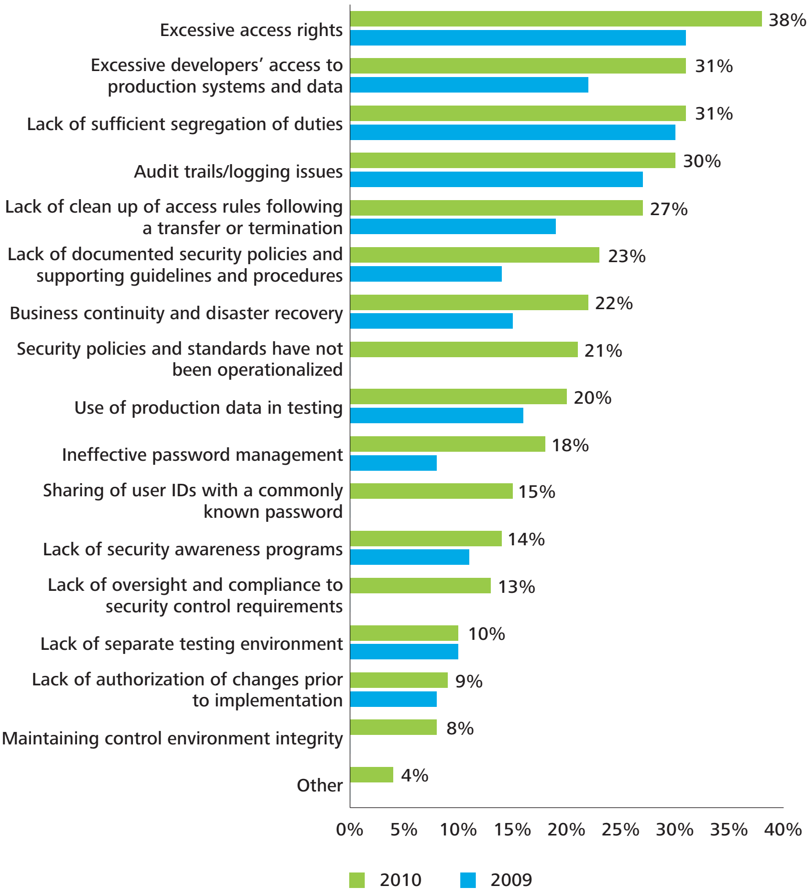
Data protection

Data makes the world go round. The most valuable asset of any organization, after its people, is its data. Data loss prevention is the hottest topic in 2010. Data loss prevention technology is the number one security technology that organizations plan to fully deploy or pilot within the next 12 months. All of respondents' top internal/external audit findings have to do with protecting data: excessive access rights, lack of sufficient segregation of duties, excessive developers' access to production, and audit trails/logging issues. And these findings are similar to last year's.

Respondents indicate that their organizations' security initiatives for 2010 are aligned with these issues (a finding that was not always the case in previous years' surveys): IAM (44%); data protection (39%); security infrastructure improvement (36%); information security regulatory and legislative compliance (34%) and information security compliance (internal/external audit) remediation (33%). Just outside the top five is information security training and awareness (32%) (see chart 20). The number five initiative, internal and external audit remediation, which has never been cited as a top five priority in previous surveys, demonstrates that financial organizations are gearing up for increased regulation and legislative compliance.

Organizations are recognizing that awareness and training programs can be very effective. There is evidence in many aspects of daily life that awareness and training change attitudes: smoking, littering, recycling, etc. Where organizations might have considered training and awareness too "fluffy" in the past, they are now recognizing that, since their workforce is subject to human failings, a combination of effective controls and training and awareness programs can go a long way toward protecting data. Most organizations (64%) train their employees to identify and report suspicious activities. There is also an interest in targeted training, particularly for IT application developers, system administrators and people handling sensitive information.

Chart 31. Top internal/external audit findings



Organizations are recognizing that awareness and training programs can be very effective.

Chart 32. Confidence in the information security practices of third parties

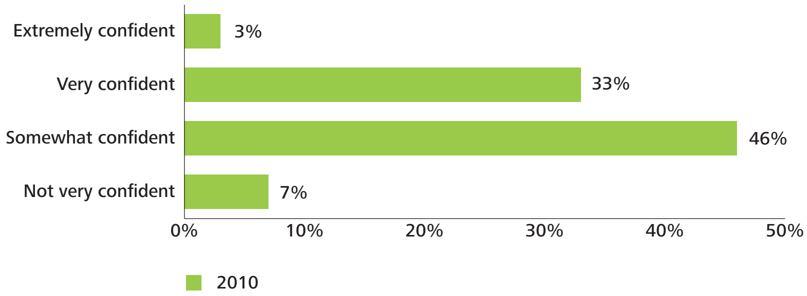
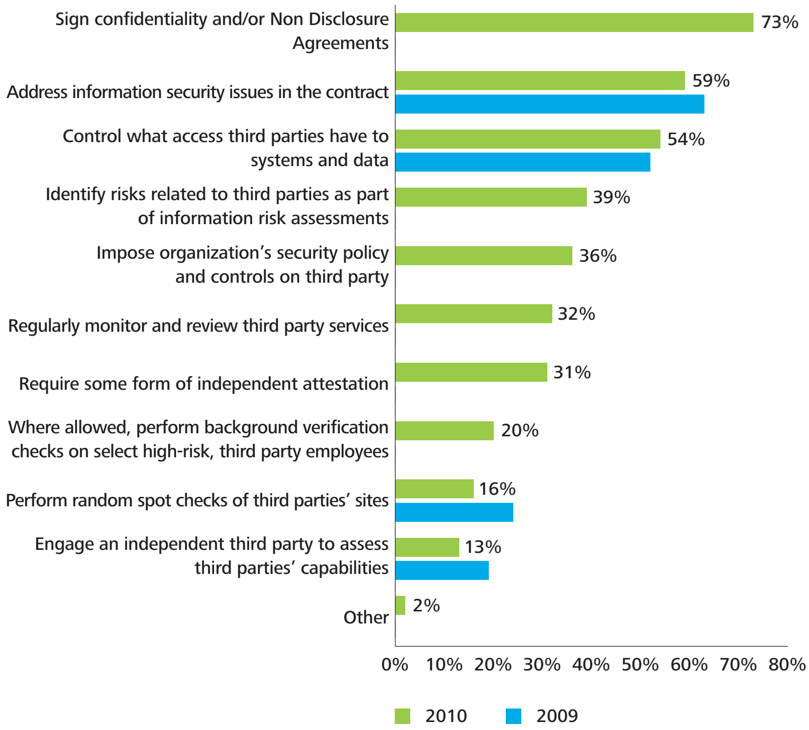


Chart 33. Ensuring the security practices of third parties



Given the risk landscape and the increasing sophistication of threats, organizations are no longer content to adopt only when the mainstream does.

Third parties are still an issue when it comes to data protection, as they have been in previous years.

Third parties are least likely to receive information security training (21% compared to 56% for system administrators), perhaps because they are typically removed from the organization and therefore out of sight and out of mind. But there is still insufficient attention paid to the security practices of third parties.

Despite their best intentions and their vested interest in being as accommodating as possible to their host organization, third parties are just as vulnerable to the same "non-intentional data loss". When asked how confident they are in the in the information security practices of their third parties, the majority of respondents (46%) indicate that they are "somewhat confident" while 33% indicate that they are "very confident". Altogether, 82% of respondents have some level of confidence in the security of their third parties. Perhaps organizations perceive that if third parties want to continue to be in business they will ensure that their security practices are above reproach. The most effective means to ensure that the level of security of third parties is aligned to your own organization is through a combination of explicit terms, conditions and expectations, as well as continuous audits, examinations and assessments. Only 7% of respondents are not "very confident" about their third parties which begs the question as to why these people are allowed to continue as third parties.

When asked how organizations ensure the security practices of their third parties, respondents state that they address information security requirements in a contract with third parties (59%) and control what access third parties have to their systems (54%).

A single control is not enough; rather, a series of controls must be in place. To ensure the security practices of their third parties, organizations must apply due diligence during and after selection process:

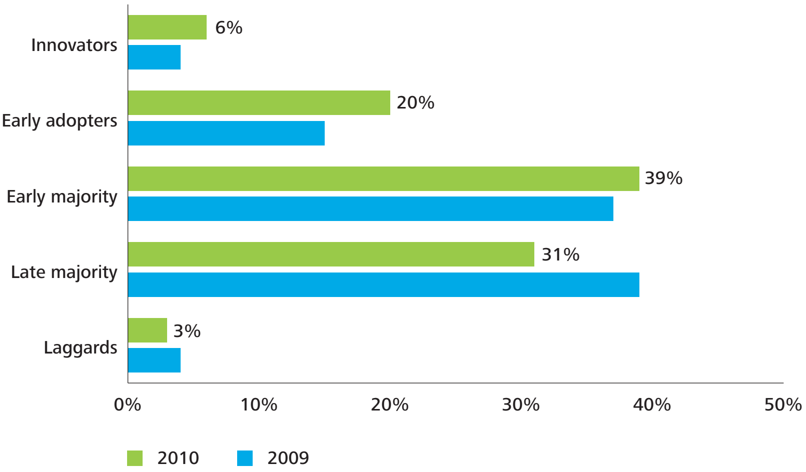
- review third parties' security policies and controls;
- regularly monitor and review their third parties' services;
- require some form of independent assessment;
- where allowed, perform background verification checks on select high-risk, third party employees; and
- perform random spot checks of third parties' sites.

Emerging technologies

One of the most exciting trends uncovered by the survey is in the area of emerging technologies. Emerging technologies bring new opportunities but greater risks as well. But organizations now seem willing to take more risks to be able to capitalize on opportunities.

For the first time in the history of the survey, "early majority" was chosen by the greatest number of respondents (nearly 40%). Early majority adopters are not willing to take the same risks as innovators or early adopters, but, while thoughtful in deployment, they adopt faster than the mainstream (late majority). This indicates a major breakthrough in the thinking of financial institutions as they move from reactive towards proactive. Given the risk landscape and the increasing sophistication of threats, organizations are no longer content to adopt only when the mainstream does. While this may not be true in other industries, financial institutions have to take this stance for survival – because they have the money, they are more likely to be targets. Even the "early adopters" category (thought leaders who try out new technologies carefully, having learned from the innovators) shows an increase this year (20%) over last year (15%).

Chart 34. Organization's adoption of security technology



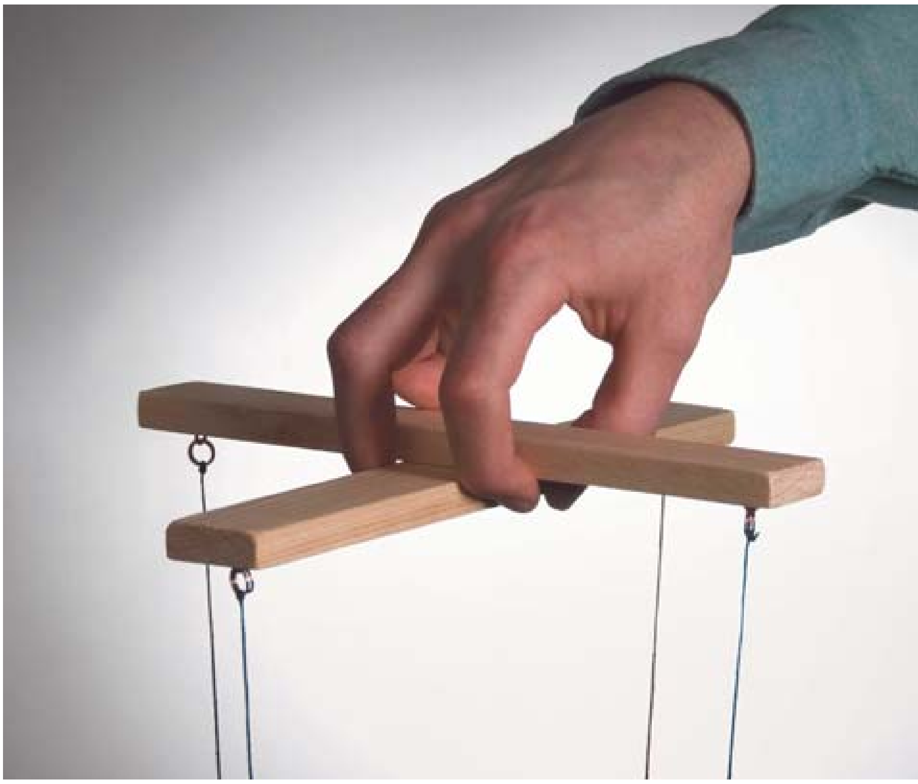


Chart 35. Types of technologies deployed, piloted or planned

	Full	Pilot	Plan
Data loss prevention technology	32%	17%	26%
Federated identity management	16%	11%	21%
Encrypted storage devices	33%	17%	20%
Enterprise Single Sign On	21%	14%	19%
File encryption for mobile devices	44%	13%	18%
Network access control	43%	13%	18%
Security compliance tools	30%	13%	18%
Email encryption	38%	17%	18%
Biometric technologies for user authentication	13%	7%	18%
Security log and event management systems	50%	19%	17%
Data at rest security/encryption	32%	14%	15%
Incident management workflow tools	38%	13%	13%
Email authentication	39%	13%	12%
Network behavior analysis	38%	15%	12%
Web access management systems	44%	10%	12%
Wireless security solutions	34%	11%	11%
Web services security	39%	12%	11%
Vulnerability management	58%	12%	10%
Intrusion Detection and/or Prevention Systems (IDS/IPS)	78%	7%	7%
Anti phishing solutions	63%	8%	5%
Content filtering/monitoring	82%	5%	4%
Anti spyware software	84%	4%	3%
Spam filtering solutions	93%	0%	1%
Antivirus	97%	1%	0%
Firewalls	97%	1%	0%

More than 70% of organizations indicate that they are planning to implement at least one new information security-related technology in the next 12 months; this is an exciting time for vendors, who have huge opportunities to demonstrate the effectiveness of their products in a receptive atmosphere. The greatest number of respondents indicates that data loss prevention is the technology that their organizations are planning to adopt.

Despite recent high-profile security breaches that have succeeded due, in part to, the absence of encryption, when it comes to the "fully deployed" category, only 38% of organizations have email encryption, only 33% have encrypted storage devices, only 44% have file encryption for mobile devices, and only 32% have data at rest security/encryption. There are major regional differences. U.K. respondents indicate 80% for file encryption of mobile devices, well above the global average. And the U.S. (67%) differs hugely from APAC (22%) when it comes to email encryption. In some areas, encryption is a relatively easy and very effective security measure and yet surprisingly under-utilized. For example, only 12% of respondents from LACRO indicate that they have "fully deployed" file encryption for mobile devices but only 26% indicate that it is "planned" or being "piloted" (34%).

Data at rest encryption appears to be a largely ignored area. Although many successful breaches have occurred by intercepting data in transit, the majority of information (e.g., medical records, insurance information, personal financial information, etc.) is data at rest. Only 32% of respondents have data at rest security/encryption fully deployed and the numbers are low for "piloting" (14%) or "planned" (15%).

Along with encryption technologies and security log and event management systems, data loss prevention technologies are those most likely to be piloted or planned. Federated identity management technologies are close behind as well as enterprise single sign on of technologies that are planned.

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

The 2010 Financial Services Industry Global Security Study reports on the outcome of focused discussions between Deloitte member firm Information & Technology Risk Services professionals and Information Technology executives of top global FSIs – a sub-set of participants from 7 industries, which were part of 2010 Global Security Study (financial services; consumer business; technology, media, and telecommunications; energy, resources & utilities; life sciences and healthcare; public sector; manufacturing).

Discussions with representatives of these organizations were designed to identify, record, and present the state of the practice of information security in the financial services industry with a particular emphasis on identifying levels of perceived risks, the types of risks with which FSIs are concerned, and the resources being used to mitigate these risks. The survey also identifies technologies that are being implemented to improve security and the value FSIs are gaining from their security and privacy investments.

To fulfill this objective, senior Deloitte member firm professionals designed a questionnaire that probed key aspects of strategic and operational areas of security and privacy across all industries and in financial services industry in particular. Responses of participants were subsequently analyzed and consolidated and are presented herein in both qualitative and quantitative formats.

Size and structure

The overall number of questions was reduced compared to previous year to reduce the burden on participants. However, new questions were also added to reflect topics being asked about by Deloitte member firm clients and raised by the media.

The 2010 Global Security Study questionnaire had 3 distinct parts: core part – which applied to all industries, industry part – targeted industry-specific questions, and business continuity management part – in-depth questions on business continuity and disaster recovery processes (previously, a separate survey – its results are not included in this publication).

Questions were selected based on their global suitability, added value, and for the financial industry part – also based on their potential to reflect the most important operating dimensions of a financial institution's processes or systems in relation to security and privacy.

The collection process

Once the questionnaire was finalized and agreed upon by the survey team, questionnaires were distributed to the participating regions electronically. Data collection involved gathering both quantitative and qualitative data related to the identified areas. Each participating region assigned responsibility to senior member firm professionals within their firms' Information & Technology Risk practices and those people obtained answers from various financial institutions with which they had a relationship.

Most of the data collection process took place through face-to-face interviews with the CISO/Chief Security Officer or designate, and in some instances, with the security management team. Deloitte member firm professionals also offered preselected financial institutions the ability to submit answers online using an online questionnaire managed by DeloitteDEX Advisory Services.

Data analysis and validation

Results of the survey have been analyzed according to industry leading practices and reviewed by senior members of Deloitte's Information & Technology Risk Services. Some basic measures of dispersion were calculated from the data sets. Some answers to specific questions were not used in calculations to keep the analysis simple and straightforward. Results in some charts may not total 100% as the study team was reporting selected information only; responses from those who decline to answer may not be included in the reported data.

Additional insights

As the amount of data collected during 2010 Global Security Study far exceeds the boundaries of this publication, it reports only on the most important data points at an aggregate level. The study team encourages you to contact your local Deloitte member firm Information & Technology Risk, or Security, Privacy and Resiliency practitioners for further insights about security practices within your industry, sub-sector, region, country, or a peer group of companies.

Acknowledgments

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

Survey development team

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

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

Andrei Kananovich
Deloitte Canada
+1 416 874 4125
akananovich@deloitte.ca

Data collection
DeliotteDEX:

Olivier Curet
Deloitte United States
(Deloitte & Touche LLP)
+1 216 589 5448
ocuret@deloitte.com

Sheila Celata
Deloitte United States
(Deloitte & Touche LLP)
+1 617 437 2128
scelata@deloitte.com

Marketing support
Chris Patterson
Deloitte United States
(Deloitte Touche Tohmatsu)
+1 212 436 2779
chrpatterson@deloitte.com

Michelle Chodosh
Deloitte United States
(Deloitte Touche Tohmatsu)
+1 212 436 6242
mchodosh@deloitte.com

Contributors

Tariq Ajmal
Deloitte Middle East

Leon Bloom
Deloitte Canada

Mark Carter
Deloitte United Kingdom

Bruce Daly
Deloitte Japan

Mike Maddison
Deloitte United Kingdom

Simon X Owen
Deloitte United Kingdom

Contacts

Global leaders

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

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

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

Adel Melek
Global Leader Information
& Technology Risk
Deloitte Touche Tohmatsu
+1 416 601 6524
amelek@deloitte.ca

Security, Privacy, and Resiliency Services regional leaders

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

Bruce Daly
Deloitte Japan
+81 3 4218 7284
brdaly@deloitte.com

Ted DeZabala
Deloitte United States
(Deloitte & Touche LLP)
+1 212 436 2957
tdezabala@deloitte.com

Uantchern Loh
Deloitte Malaysia
+65 6216 3282
uloh@deloitte.com

Martin Carmuega
Deloitte Argentina
+54 11 43204003
mcarmuega@deloitte.com

Simon X Owen
Deloitte United Kingdom
+44 20 7303 7219
sxowen@deloitte.co.uk

Regional contacts

APAC

Joshua Chua
Deloitte Singapore
+65 6216 3188
joshuachua@deloitte.com

Vishal Chawla
Deloitte India
+1 703 251 1793
vchawla@deloitte.com

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

Mitsuhiko Maruyama
Deloitte Japan
+81-3-4218-7304
mitsuhiko.maruyama
@tohmatsu.co.jp

Tommy Viljoen
Deloitte Australia
+61 02 9322 7713
tfviljoen@deloitte.com.au

EMEA

Kris Budnik
Deloitte South Africa
+27 0 11 806 5224
kbudnick@deloitte.co.za

Mike Maddison
Deloitte United Kingdom
+44 20 7303 0017
mmaddison@deloitte.co.uk

Mark Carter
Deloitte United Kingdom
+44 20 7007 0048
markcarter@deloitte.co.uk

Colm McDonnell
Deloitte Ireland
+353 1 4172348
cmcdonnell@deloitte.ie

Alfonso Mur
Deloitte Spain
+34 915145000 x2103
amur@deloitte.es

Chris Norman
Deloitte France
+33 1 55 61 47 72
cnorman@deloitte.fr

Sven Probst
Deloitte Switzerland
+41 44 421 6401
sprobst@deloitte.ch

Carsten Schinschel
Deloitte Germany
+49 211 8772 3163
cschinschel@deloitte.de

Rob Stout
Deloitte Netherlands
+31 88 288 2398
RStout@deloitte.nl

Chris Verdonck
Deloitte Belgium
+ 32 2 800 24 20
cverdonck@deloitte.com

Middle East

Tariq M. Ajmal
Deloitte Middle East
+971 2 676 0025
tajmal@deloitte.com

CIS

Paul O'Brien
Deloitte Russia
+7 495 787 0600
paulobrien@deloitte.ru

Wayne Brandt
Deloitte Russia
+7 495 787 0600
wbrandt@deloitte.ru

LACRO

Martin Carmuega
Deloitte Argentina
+54 11 4320 4003
mcarmuega@deloitte.com

André Gargaro
Deloitte Brazil
+55 11 5186 1268
agargaro@deloitte.com

Jeremy Smith
Deloitte Cayman Islands
+1 345 814 3315
jersmith@deloitte.com

Mauricio Torres Romero
Deloitte Mexico
+52 55 50806943
mtorresromero@deloittemx.com

USA

Rich Baich
Deloitte United States
(Deloitte & Touche LLP)
+1 704 887 1563
jbaich@deloitte.com

John Clark
Deloitte United States
(Deloitte & Touche LLP)
+1 312 486 3985
johclark@deloitte.com

Kenneth DeJarnette
Deloitte United States
(Deloitte & Touche LLP)
+1 415 783 4316
kdejarnette@deloitte.com

Ted DeZabala
Deloitte United States
(Deloitte & Touche LLP)
+1 212 436 2957
tdezabala@deloitte.com

Ed Powers
Deloitte United States
(Deloitte & Touche LLP)
+ 1 212 436-5599
epowers@deloitte.com

Mark Steinhoff
Deloitte United States
(Deloitte & Touche LLP)
+ 1 617 437 2614
msteinhoff@deloitte.com

Canada

Donald Mccoll
Deloitte Canada
+1 416 601 6373
dmccoll@deloitte.ca

Marcel Labelle
Deloitte Canada
+1 514 393 5472
marlabelle@deloitte.ca

Disclaimer
This publication contains general information only, and none of Deloitte Touche Tohmatsu, its member firms, or its and their affiliates are, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it 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.

Item# 100046

Designed and produced by The Creative Studio at Deloitte, London. 3434A