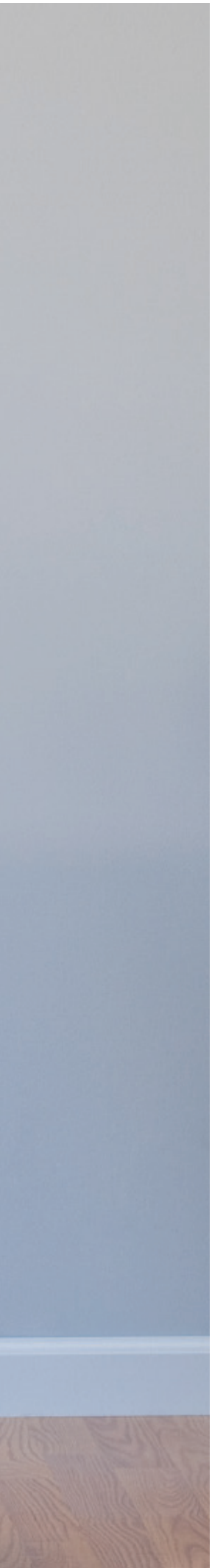


The faceless threat

A Deloitte survey

On the state of information security in the global financial services industry and perspectives from the Middle East.

Deloitte's 7th Annual Financial Services Global Security Survey 'The Faceless Threat' was released earlier this year and represents the input of senior IT executives at nearly 27 percent of the top 100 global financial services firms. But what distinguishes this year's version is the strong participation from Middle East (ME) institutions – so significant in fact, that for the first time the Middle East has been included as a separate discussion in the survey.

Overall figures from the survey denote that the Middle East has more last place finishes than any other region. While other regions across the globe have more robust security and privacy legislations, the Middle East has yet to implement comprehensive security regulations and thus earns the lowest scores with regards to managing privacy – only 11 percent of institutions in the Middle East have one or more executives responsible for privacy and only 17 percent have a program for managing compliance with privacy requirements. Responses from the region also indicate that it is in fifth place, behind the U.S., Asia Pacific, Canada and Europe in feeling that they have both, the commitment and the funding, to address regulatory security requirements. The Middle East also lags behind other regions in terms of having a formally documented and approved information security strategy (47%). Despite this lack of maturity in security and privacy, Middle East institutions share many of the common security issues of more mature global financial institutions, and it is likely that any initiatives from this area will be in line within the global trend.

Overall figures from the survey denote that the Middle East has more last place finishes than any other region.

Security issues for 2010

We live in an environment where technology is becoming more complex daily. The new realities such as mobile media, social networking technologies and extended enterprise are raising emerging security and privacy concerns. We are also seeing increasing regulatory and compliance requirements. Concurrently, we are seeing an increase in the sophistication and proliferation of security breaches and attacks. Organized cyber crime is getting more planned, leading to better targeted and more financially rewarding attacks. The focus of these threats will continue to shift to the next weakest link: people and applications.

From an overall perspective, we note that although there is still a long way to go, organizations are starting to recognize the importance of the information security function to their businesses. This is evident from the fact that 80 percent of the organizations surveyed have an executive responsible for information security. Moreover, despite the worst economic downturn in decades and cost-cutting programs being implemented at many institutions, more than half of the survey's respondents (56 %) indicate that their information security budget has in fact increased. This is one of the areas in which Middle East respondents (56%) are at par with the global average.

Governance & funding

Reporting relationship of the Chief Information Security Officer (CISO): Respondents to this year's survey reported a slight increase over last year in the reporting of the CISO to the CEO and the CFO, indicating that the information security function of organizations is clearly moving in the right direction. However, the most common reporting relationship for the CISO remains to the Chief Information Officer (CIO), although at 24 percent, it marks a decrease from last year (33%). The Middle East comes in close at 20 percent.

Although the CISO still integrates into the Information Technology (IT) function (and therefore continues to be viewed as technical) 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%), with 10 percent of the respondents indicating that CISOs in their organizations report directly to the Board of Directors.

Functions in scope of the Information Security Executive: The CISO's most prevalent mandate remains information security governance (85%). A positive

indication is that CISO's focus continues to be on strategy and planning rather than operations despite a slight drop in the former this year (75% over last year's 80%). Overall, the services delivered by the CISO continue to be geared towards strategy and governance rather than operations.

Security budgets: As in previous years, the lack of a sufficient budget is perceived as the primary barrier to ensuring information security. But this year there is a difference. Whereas 36 percent of respondents state budget constraints as a factor in 2010, that percentage has dropped considerably from last year's 56 percent. 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 an increase in budgets (56% of respondents) and increased interest in expensive projects such as Identity & Access Management (IAM) and Data Leakage Protection (DLP). This may well be due to an increasing realization that, as the information security environment gets more dangerous, so investment in data protection must get more serious. Moreover, regulatory pressures are also pushing organizations to spend more money on security to ensure compliance. However, a relatively large number of respondents (27%) state that they "do not know," a clear indication that there is no separate information security budget within their organization.

State of expenditures on information security: When asked how they would characterize their organization's expenditures on information security, the greatest percentage of respondents state that they are on plan or ahead of requirements (45%), a slight increase over last year. However, when we look at the Middle East we note that the region scored the lowest amongst all the regions in this category (only 27% of respondents indicate that they are on plan or ahead of requirements). In the Middle East, the majority of organizations are either behind or catching up on the expenditures on information security. This means that although the budgets have increased, Middle East organizations are unable to translate the budget into spending because of a lack of sufficient resources to drive various security initiatives.

When asked whether information security professionals have all the required competencies to handle existing and foreseeable security requirements, 45 percent of global respondents indicate that they do, whilst in the Middle East we note that this figure is at 42 percent. This could explain why even though budgets have increased for the Middle East, the majority of respondents (58%) feel that they don't have the required competencies, which is impacting their spending on information security. We also see that organizations are trying to address this spending gap by utilizing consultants/ contractors. When asked about their major expenditures covered under the information security budget, respondents indicate that software, consultants/ contractors and hardware as their greatest expenditures (66%, 62% and 61% respectively).

Threats, risks and mitigation activities

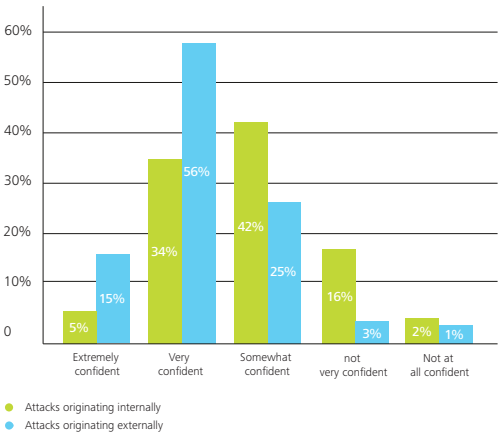
Financial institutions are fighting on two fronts: external and internal. The external landscape is getting more dangerous and threats are getting more ingenious and harder to detect. The survey shows that the second most reported barrier in ensuring information security is the increasing sophistication of threats (at 31% versus last year's 38%) followed by emerging technologies at 24 percent. Similarly, organizations are getting more concerned about their employees' inadvertent behavior, such as social engineering, phishing, etc. Moreover, as individuals communicate and transact with each other more over the Internet through e-mail, instant messaging, Internet purchases and social networking, there is greater potential for information to fall into the wrong hands.

As in previous years, people remain the organization's greatest worry. When asked to rate their level of confidence that their organization's assets are protected from an attack, only 5% of respondents said that they were "extremely confident" that they are protected from

As in previous years, people remain the organization's greatest worry. When asked to rate their level of confidence that their organization's assets are protected from an attack, only 5% of respondents said that they were "extremely confident."

We note that in many cases, organizations themselves are the enablers of mistakes on the part of their employees. Employees routinely have access to more information and applications than they need to do their job.

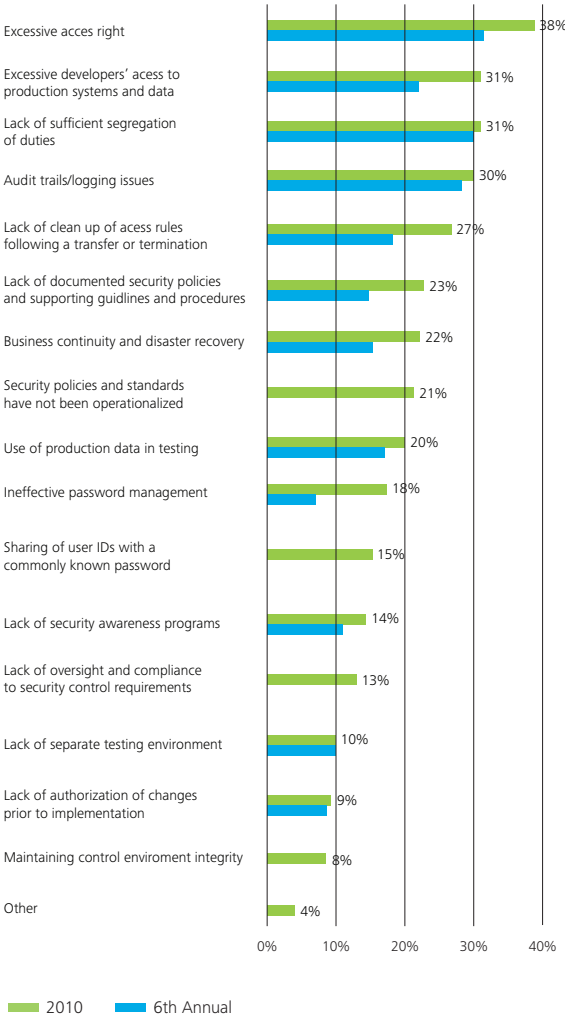
Chart 1 – Confidence that your organization's information assets are protected from internal and external attacks



internal attacks versus 15 percent who are "extremely confident" that they are protected against external attacks. Similarly, only 34 percent said they were "very confident" about being protected against internal attacks versus 56 percent who said they were "very confident" about being protected against external attacks (see chart 1). This loss of confidence in internal people is a trend; almost half in last year's survey indicated that they were "somewhat confident."

We note that in many cases, organizations themselves are the enablers of mistakes on the part of their employees. Excessive access rights, at 38%, was the top internal/external audit finding, with four of the top five findings related to access rights (see chart 2). Employees routinely have access to more information and applications than they need to do their job as organizations tend to be overly generous with access rights so as not to impact employee productivity. But

Chart 2 – Top internal/external audit findings

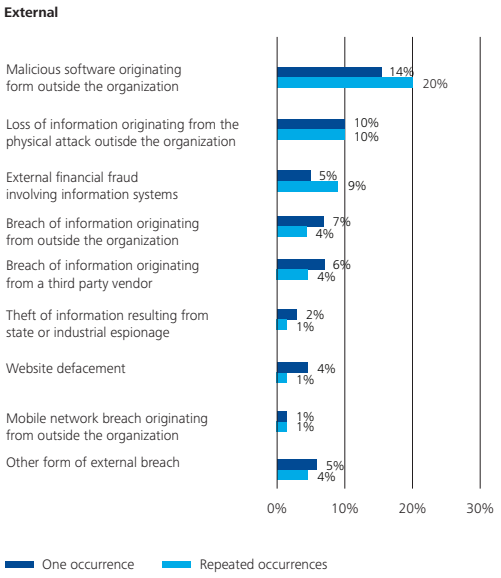


The issue of excessive access rights represents a huge gap in the information security of most organizations.

any productivity gains pale in comparison to the negative consequences of a potential security breach.

External & internal breaches: When asked about external breaches experienced in the past 12 months, respondents most often cite repeated occurrences of "Malicious software originating outside the organization" (20%). When asked about internal breaches, respondents cite repeated occurrences of both "Accidental breach of information originating from inside the organization" (11%) and "Malicious software originating from inside the organization" (10%).

Chart 3 – Breaches experienced in the last 12 months



Despite the ominous and dangerous external landscape, organizations that have sustained a breach report that losses are minimal. However, while 26 percent of respondents report no financial loss and 22 percent report a loss of only $250,000, a significant number of respondents (10%) chose the category "Not applicable/ do not know."

When asked how often their organizations conduct testing or reviews, 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%).

Chart 4 – Frequency with which organizations conduct specific testing or review

	Quarterly	Semi-Annually	Annually	Ad hoc	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%

However, responses to this question revealed a gaping security hole: 46 percent of respondents state that their application security code review is conducted only on an ad hoc basis and 23 percent, never. On an ad hoc basis, the processes are likely to be informal or inconsistent. Since hackers do not ignore applications, neither should organizations.

46 percent of respondents state that their application security code review is conducted only on an ad hoc basis and 23 percent, never. On an ad hoc basis, the processes are likely to be informal or inconsistent. Since hackers do not ignore applications, neither should organizations.

Key finding from sector-based breakdown

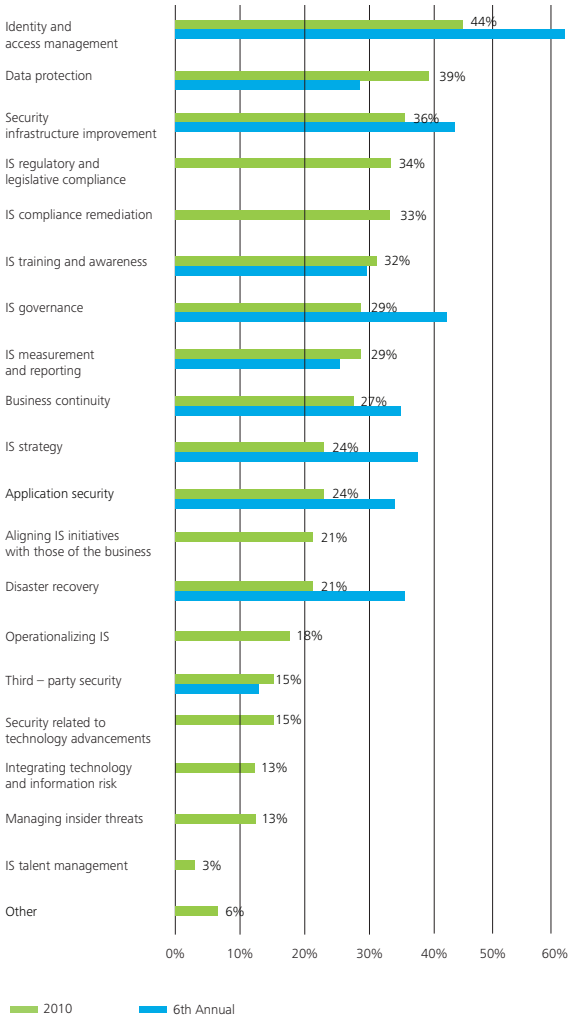
For the first time, Deloitte's survey breaks out sector-based comparisons. While banks appear to have a stronger security posture than other financial services institutions, insurers are quickly catching up. Of key 2010 priorities, insurers have a bigger appetite for identity and access management (a priority for 51% of insurance organizations and only 44% of banks) and data loss prevention technologies (32% percent versus 25% respectively.)

Identity and Access Management (IAM) remains a top security initiative followed by data protection and Information Security Infrastructure improvement.

Key security priorities for 2010

Identity and Access Management (IAM) remains a top security initiative followed by data protection and Information Security Infrastructure improvement. We also note this year that both Information Security (IS) regulatory and legislative compliance and IS compliance remediation complete the top five initiatives.

Chart 5 – Top security initiatives



Identity & Access Management (IAM)

Identity and Access Management (IAM) was identified as the industry's top security initiative for 2010. Among 19 different types of initiatives, 44 percent listed IAM as their top initiative. This is not surprising given that excessive access rights was the top internal/external audit finding at 38% (see chart 2). IAM solutions not only provide authentication, but allow organizations to aggregate identities across the enterprise into a single view, simplify user access to multiple applications as well as provide the ability to track back, stroke by stroke, what events took place, when and by whom.

However, we note that as the size of the organization decreases, so the number of respondents who identify this area as a priority decreases. Although IAM is a priority for larger organizations with more than 10,000 employees (63% of respondents have included IAM into the list of their priority initiatives for 2010), only 35% consider this a priority for less than 1,000 employees. It is therefore not surprising that when compared globally (44%), only 15% of Financial Institutions in the Middle East (lowest of all the regions), where organizations are smaller size, put IAM in their priority initiatives for 2010. As institutions in the Middle East become more mature, it is expected that the percentage of respondents who prioritize this initiative will increase.

Data Loss Prevention (DLP)

Data loss is caused by an intended or unintended action on the part of an organization's people. It is a major undertaking that begins with the most time consuming part: classifying existing information to identify what information needs protection and from whom.*

Respondents state that data protection is their second highest priority after IAM (39%). With 42% of respondents only "somewhat confident" in their ability to thwart internal attacks, it is no surprise that Data Loss Prevention technology is the number one security technology that organizations plan to fully deploy or pilot within the next 12 months.

Regulatory compliance

A third of respondents to the survey (34%) include regulatory and legislative compliance as one of their top five initiatives. Financial institutions are clearly expecting more regulatory pressure from various bodies such as the Payment Card Industry Data Security Standard (PCI DSS). We see this first hand in the Middle East where Central Banks in Qatar and Lebanon have issued circulars and directives on various security related matters and other Central Banks are working on them. Similarly, bodies like Tadawul (Saudi Stock Exchange) and the Emirates Securities & Commodities Authority (ESCA) have issued security requirements for brokers to comply with. They also recognize the competitive and reputational requirements to meet – or exceed – industry "leading practice" and standards such as CobIT, ISO27001, ISO20000, ITIL, etc. Moreover, for the first time in the history of our survey, information security compliance remediation based on the findings of internal and external auditors is one of the top five security initiatives of organizations. Evidence of this is the fact that organizations are hiring more internal auditors to resolve internal and external audit findings in preparation for dealing with more regulation.

With 42% of respondents only "somewhat confident" in their ability to thwart internal attacks, it is no surprise that Data Loss Prevention technology is the number one security technology that organizations plan to fully deploy or pilot within the next 12 months.

Conclusion

The Middle East is perhaps 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 and others are in process. Jobs for information security professionals in the Middle East abound on the Internet and the region hosts various conferences and events featuring information security. Deloitte is focusing on the Middle East through its regional Information & Technology Risk practice, investing in security lab and by getting involved in a number of emerging initiatives through publications, seminars and engagements.

by **Tariq Ajmal**, partner-in-charge of Information and Technology Risk Services, Deloitte in the Middle East.

* For more information on data protection, please consult the article entitled "Protecting What Matters" in the August 2010 issue of ME Point of View magazine.

Tariq Ajmal is one of the contributors to the 7th Annual GFSI Survey.