Deloitte.

# The time is now
## 2009 Life Sciences & Health Care Security Study

A global perspective on cyber security, privacy and data protection in the life sciences and health care industry

# Contents

# Foreword

The global economic environment and the ever-changing regulatory landscape have impacted most businesses, regardless of sector, size and region. Life sciences organizations grapple with the risk of diminished pipelines; health care providers deal with the ever-increasing cost of health care; and health care payers work to fulfill their mandates in the face of increasing regulation and pressure on costs.

The changing environment has a profound effect on how organizations realize their security and privacy objectives. The lifeblood of any life sciences or health care organization is information, whether patient, intellectual property, or revenue. Organizations are dealing with the challenge of how to protect their information while facing increasingly sophisticated security threats and spiraling regulatory and legislative requirements—all against a backdrop of reduced spending, staff cuts and organizational changes.

For organizations in the United States, the billions being invested by the federal government in the health care industry as part of the recent economic stimulus will have huge ramifications. On the one hand, there is the promise of great improvements in the quality and availability of useful information coupled with efficiency gains. On the other hand, there is increased responsibility to protect this information and a commensurate level of risk for not doing so. Whether it is the broader purview of the Health Insurance Portability and Accountability Act (HIPAA), the widespread adoption and use of electronic health record (EHR) technologies under the HITECH ACT of the American Recovery and Reinvestment Act (ARRA), or the implementation of electronic exchanges for health, there will be significant pressure on organizations to meet these challenges.

The management challenge—particularly tough in hard economic times—is to strike the proper balance between maximum exploitation of the opportunity and prudent, cost-efficient mitigation of the risk. On behalf of Deloitte Touche Tohmatsu's (DTT) Member Firm Security and Privacy Services practices and DTT's Life Sciences and Health Care Industry group, we hope you will find this study insightful. A significant level of effort goes into producing a study such as this, particularly on the part of the participants from the various organizations who offer not only their time but their candid assessments. We would like to thank all the participants from the various organizations who offer not only their time but their candid assessments. We would like to thank all the participants from life sciences, health care provider and health care payer institutions around the world who took part in this study.

The industry is heading into a period of massive opportunity as it seeks to maximize the value of data and the promise of new automation. But it is our view that the industry is not yet prepared to meet the challenges of managing the risk as this opportunity emerges. Whether this is because the industry is behind in implementing important foundational technologies, such as identity and access management solutions, or because there is a reluctance to adequately fund the security functions to meet the ever-increasing volume and sophistication of threats, the reality remains that the industry must now act aggressively to catch up.

Amry Junaideen
Health Sciences & Government Leader – Security & Privacy
Deloitte United States
Deloitte & Touche LLP

Ted DeZabala
National Managing Partner – Security & Privacy
Deloitte United States
Deloitte & Touche LLP

# Objectives of the study

The objectives of the 2009 Life Sciences & Health Care Security Study are 1) to help respondents assess the state of information security within their own organizations; 2) to allow executives to compare their organization's status with that of other life science, health care provider and health care payer institutions around the world, and 3) to provide management with insights and help them to identify trends that will aid informed strategic decisions. Overall, the goal is to bring readers closer to being able to answer questions, such as: How is the state of information security changing within my organization? And, Are these changes aligned with those of the rest of the industry?

In order to ensure that questions were relevant and timely with regard to environmental conditions, Deloitte member firm subject matter specialists were enlisted and their knowledge leveraged to identify questions that incorporate the critical issues being addressed by life sciences and health care at the global level.

# The value of benchmarking

The life sciences and health care industry, now more than ever, recognizes the importance of performance measurements and benchmarks in helping manage complex systems and processes. The 2009 Life Sciences & Health Care Security Study for life sciences and health care organizations is intended to enable benchmarking against comparable organizations. Comparison with a peer group can assist organizations in identifying those practices that, when adopted and implemented, have the potential to produce greater performance or to result in recommendations for performance improvements. However, the value of peer comparison must be tempered by the fact that the standard of due care is both undefined and evolving and by the recognition that individual perspective, particularly on lesser understood issues such as convergence and security strategy, differs greatly when responding to questions.

Since internal breaches are as much a result of inadvertent and careless behavior as they are of malicious intent, third parties have many of the same worries about their people as the organizations they contract with.

### Areas covered by the study

It is possible that an organization may excel in some areas related to information security, e.g., adhering to a common information security framework, and fall short in other areas, e.g., privacy initiatives. In order to be able to pinpoint the specific areas that require attention, DTT's Member Firm Security & Privacy Services practices chose to group the questions by the following six areas of typical life sciences and health care organizations' operations and culture:

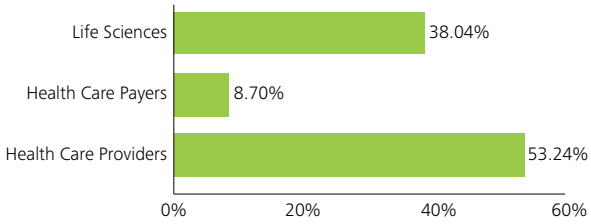
- **Governance**
  Framework, reporting
- **The information security function and the role of the Chief Information Security Officer (CISO)**
  Top functions, information assets, convergence, employees, capability of security personnel, information security strategy, top security initiatives, major barriers to information security, return on security investments, reporting on status/incidents, internal/external audit findings, investment in IT, expenditures, information security budget, causes of project failure, alignment of business and security initiatives
- **Risk**
  Risk tolerance, application security, external/internal threats, cyber attack protection
- **Use of security technologies**
  Technology, testing
- **Quality of operations**
- **Privacy**

# Who responded

Respondents to the 2009 Life Sciences & Health Care Security Study represent life sciences, health care provider and health care payer organizations, and respondent data reflects current trends in security and privacy within these organizations. Among the participating companies, nearly half of all respondents reported revenue between US$1 billion and greater than US$15 billion and more than half reported that they employ between 5,001-50,000 employees.

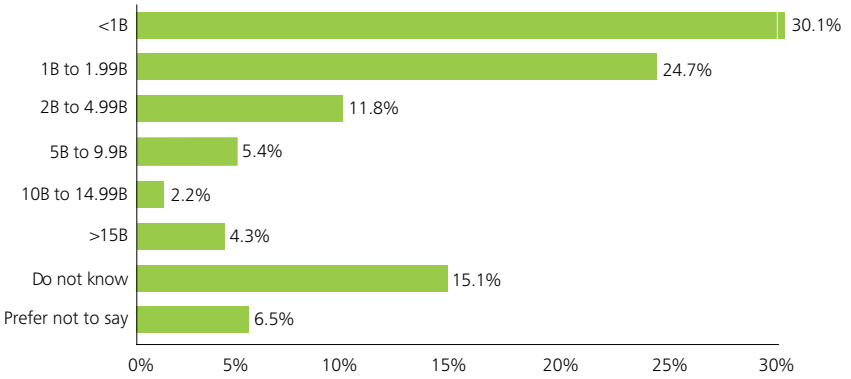
**Industry Sector Segmentation**

Please indicate your organization type



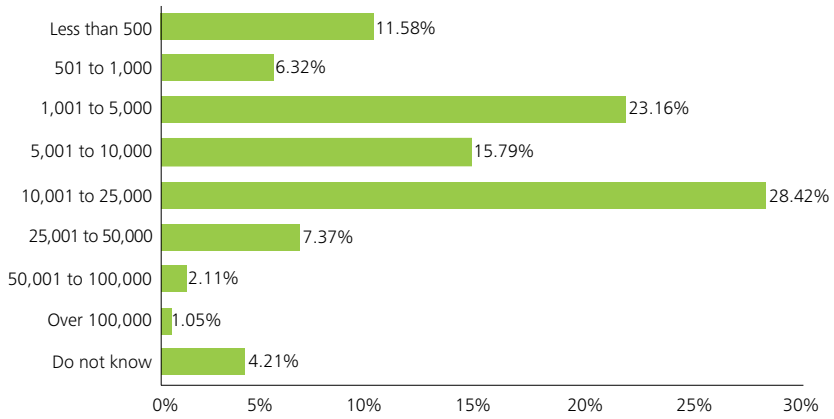

**Annual Revenue Segmentation**

Indicate the approximate annual revenue of your organization in 2007 ($USD): (please select one)



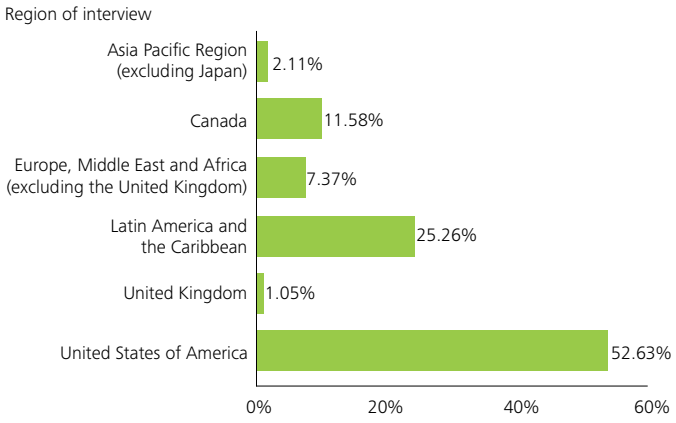
## Number of Employees Segmentation

Number of employees in your organization? (please select one)




## Geographic Segmentation

Region of interview



# Key findings

**Data leakage protection is a primary threat-based initiative.**

Data loss and information leakage are clearly a great concern to respondents. Data leakage is the movement of a data asset from an intended state to an unintended, inappropriate or unauthorized state, representing a risk or a potentially negative impact to the organization. Data leakage protection is keeping information out of the wrong hands. As more and more examples are made public—such as the recent fining of a health care provider whose unprotected web site contained names, addresses, phone numbers and lab results for patients, in violation of U.S. state law and the organization's own privacy policies—there is a scramble to take action. A leakage may or may not cause immediate harm but generally means that security controls have been infiltrated through an attack, simple mistake or lack of awareness. Although only a small percentage of respondents to this study currently have data leakage protection technology fully deployed—compared to the majority for firewalls and anti-virus—it is the technology they are most focused on in the short term. Data leakage protection is the technology indicated by the highest percentage of respondents when asked which technologies they plan to deploy or pilot over the next 12 months.

Most organizations have been relatively slow to embrace the technologies that prevent data leakage because of "traditional thinking": in the past, securing operating systems, networks, storage, communication channels and the hardware they ran on was enough—the idea being that the information residing on them was therefore safe. Today, advances in computing power and storage capacity, coupled with the evolution of a globally connected economy, have eliminated any real scarcity of the IT connectivity, storage, and computing infrastructure. Globalization, service orientation and outsourcing have changed the requirements from those of the last two decades. Because information is what is valuable now, data protection is where the focus must lie.

**With the ever-increasing focus on privacy, identity and access management is a top priority.**

Respondents indicate that identity and access management is a top operational initiative, and there is a strong indication that it will remain a priority for the foreseeable future. This is a core enabler of enterprise applications within the industry, where access to information and data is a growing need. Organizations want to provide employees and third parties with the tools they need to securely access the network and applications whenever they want, wherever they are. This is not for altruistic reasons; employers are well aware of the resultant productivity boon, the role that a flexible working environment plays in attracting and retaining top talent, and the reduced need for real estate assets. But as mobile devices and tablet technology proliferate and as "cyber security" threats, such as the Conficker worm and attacks against users of social networking sites become more commonplace, managing security becomes a complex issue. The constant balancing act for organizations is providing convenient access for employees while maintaining strong access control to information.

Most organizations have been relatively slow to embrace the technologies that prevent data leakage because of "traditional thinking"…

**The trend towards outsourcing raises a host of third-party security concerns.**

There is a general trend towards outsourcing to third parties, either as a cost-saving measure or because a specialized skill set is not available in house. A large percentage of organizations use third parties to store sensitive data on their behalf, e.g., personally identifiable information (PII) or protected health information (PHI). Respondents admit that their people (which includes third parties) are organizations' biggest security worry—83% are equally or more concerned with internal security threats than with external threats. Most respondents indicate that third parties are engaged only after an initial independent review and most are granted restricted access to the organization's information and systems. However, a low percentage perform spot checks on vendor sites or information security audits of vendors after a vendor has been engaged. And, of course, vendors have a strong vested interest in making sure that their relationship with the host organization is above reproach from a security standpoint. However, since internal breaches are as much a result of inadvertent and careless behavior as they are of malicious intent, third parties have many of the same worries about their people as the organizations they contract with. The full-scale adoption of EHR, an objective of the economic stimulus package to the health care industry in the United States, will mean an escalation in the use and reliance on third parties and vendors, with the associated escalation in risk to consumer, patient and business information. In the life sciences sector, there is more and more data sharing with alliances and partnerships. Cloud computing, where data and software are housed in remote data centers rather than in on-site servers, is tempting to organizations that are trying to reduce capital costs and boost efficiency but, at the same time, adds another layer of complexity to safeguarding PHI and meeting the revamped HIPAA security and privacy rules.

**As the business and regulatory environment of the industry evolves, the role of the CISO takes on greater significance.**

For those organizations that have a Chief Information Security Officer (CISO), the stature of that individual is dependent upon the sophistication of the organization's risk management program and the reporting relationship of the CISO. Study findings indicate that the role of the CISO has taken on a greater significance and visibility in that the scope of the position is now more heavily weighted toward a C-suite focus on security (planning, governance, administration, architecture and IT Risk Management). Almost 43% of respondents' CISOs report to the Chief Information Officer (CIO). This is the most common reporting relationship, one in which the influence of the CISO over the way information is managed tends to be moderate and hands-on ownership for technical responsibility still tends to be high. However, as organizations move toward more mature risk management, the influence of the CISO increases while technical ownership decreases. In organizations with the most evolved risk management programs, CISOs tend to report to a Corporate Risk Officer, a relationship in which the CISO typically has a high degree of influence and a low ownership of technical responsibility.

While the majority of study respondents across all regions indicate that they have a CISO, a full 43% do not, despite the ever-increasing security and privacy risks faced by the industry. This is a disturbing statistic, since a strong level of preparedness to meet current and future security and privacy requirements is a direct corollary to the existence of an appropriately positioned and empowered CISO.

**As the security environment becomes more complex and regulation continues to increase, security budgets fail to keep pace.**

The two most frequently mentioned barriers to ensuring information security are budget constraints and the increasing sophistication of threats. While complaints about inadequate budgets and funding are age old, the study clearly identifies this as being a key impediment. Even though more than 50% of respondents across all sectors state that their information security budgets increased, the majority of increases are still in the lowest category, the 1%-15% range.

As in other industries, there is constant pressure on IT departments within life sciences and health care organizations to not only maintain services but improve upon them while controlling expenses. The majority of respondents across all sectors state that they do not have an information security budget separate from the IT budget; the most common percentage of the IT budget dedicated to information security is 1%-3%. The problem with this approach is that security may fall to the bottom of the funding list as priority is given to projects and infrastructure that are perceived as being more important to the business or contributing to revenue generation.

A high percentage of respondents indicate concern over the increase in sophistication of threats and the endless parade of emerging technologies, such as the ploy that invites social networking users to click on a link releasing a variant of the Koobface worm hosted on an IP address in another part of the world. A free social networking and micro-blogging service that collects personally identifiable information about its users and shares it with third parties brings with it a whole host of security concerns.

Despite their concern, respondents also indicate that their security staff is adequate for responding to security threats. A large number of respondents (40%) feel that budget constraints may be a result of the impact of current global economic conditions on security budgets. The problem with falling budgets for security and privacy is that the bad guys never seem to be affected by cost-cutting—the parade of creative breach ideas continues and grows, with each one more sophisticated than the previous. The big questions for organizations are: What effect will shrinking budgets have on the volume and impact of breaches? And, could the reputational, regulatory and legal ramifications of a major breach result in a "penny wise, dollar foolish" scenario?

A high percentage of respondents indicate concern over the increase in sophistication of threats and the endless parade of emerging technologies

# Geographic highlights

### LACRO

LACRO respondents indicate that their greatest expense is physical access controls, higher than all other categories. This focus is characteristic of an early stage information security program and, as one would expect, LACRO respondents report a greater incidence of both external and internal incidents than any other region. Surprisingly, a large percentage of LACRO respondents consider exposure of sensitive data through a web attack as a non-threat although breaches resulting in substantial losses occurred more frequently for organizations in the LACRO region than in any other region. LACRO-based organizations lead other regions in the absence of an information security policy and their current state is likely a reflection of this. The good news for LACRO respondents is that, as late bloomers, they can progress quickly to the level of other regions, building on some very clear strengths and leap-frogging over earlier technologies.

LACRO respondents are determined to make the necessary investment in security, spending significantly more per employee on security. Across all regions, about 35% of organizations spend $100 per employee on security (slightly higher in the United States). LACRO is the only region that spends more than $1000 per employee (about 14%). In addition, LACRO respondents feel that their security projects are adequately funded and they assess themselves as being on plan when it comes to security spending. LACRO respondents are motivated to move quickly in the right direction when it comes to security: LACRO is the region, along with the United States, that reports having the highest number of online customers.

### United States

The security issue of greatest concern for organizations in the United States is data loss and information leakage, particularly as it relates to vendors and third parties. The vast majority of organizations (90%) in the United States are far more likely to allow third parties to store sensitive data on their behalf than any other region. Only 57% of U.S. organizations are likely to conduct objective independent reviews of vendors to evaluate their security posture before engaging them. In the United States, where the largest use of EHRs is for insurance purposes, data protection is particularly relevant, more so for this purpose than in other regions with national health care programs. Interestingly, and perhaps due to their use of EHRs for insurance purposes, respondents from the United States are the only ones who indicate that they use fraud detection/prevention technologies. As expected, respondents cite data leakage protection as their primary threat-based security initiative.

All U.S. organizations surveyed provide authorization consistent with the principle of least privilege. While organizations in other regions provide access, most tend to provide it above what is needed.

There were more breaches resulting in substantial loss in the United States than any other region, understandable given the size of the industry. A large percentage of organizations (48%) had financial loss of US$1M and a quarter of the organizations did not experience any financial loss. The United States and LACRO region organizations were the only ones to experience losses between US$1M to US$5M.

The industry continues to improve its privacy initiatives, with respondents in the United States ahead of other regions in terms of the maturity of their programs. This highlights the finding that regulation is the key driver for privacy initiatives. U.S. respondents were far ahead of the other regions in tracking loss of customer data and reporting publicly in jurisdictions where required by law and regulations.

### Canada

Canadian organizations are remarkably advanced in some areas of security and startlingly behind in others. In Canada, more so than in any other region, the CISO is more likely to report to a C-suite executive unrelated to technology (a CEO or CFO), which one could assume means that the function has a higher profile outside the technology function. Yet, more so than any other region, respondents maintain that they lack management support and functional executives have no involvement (0%) in the information security strategy.

Canadian organizations excel in having a document retention policy and lead all areas in its enforcement. They maintain, more so than respondents in any other region, that they are "late majority" adopters of security technology yet Canadian organizations report more external financial fraud involving information systems than any other region. They rate the loss of customer data as a higher threat than any other region, even the United States, where EHR storage is far more prevalent.

Segregation of duties is a major internal/external audit finding for Canadian respondents and may go hand-in-hand with their assertion that employee misconduct is a major security issue for them. More so than any other region, they are focusing on security training and awareness as a way of dealing with this.

### Other regions

Other Regions (Europe, the Middle East and Africa, Asia Pacific) indicate that their primary threat-based initiative is data leakage protection. More so than all other regions, they have a formally documented information security strategy. However, they have the lowest percentage of overall respondents that adhere to a common security framework.

Disaster recovery planning/business continuity planning (DRP/BCP) ranks high as an internal/external audit finding for Other Regions, as does lack of security awareness programs. Interestingly, they are the only geographic group that is more confident about preventing an internal attack than an external one but yet they recognize, along with LACRO, the United States and Canada, that human error is one of the top three root causes of failure.

# Sector highlights

### Life sciences

Approximately 44% of respondent's organizations in the life sciences sector do not have a CISO. This is a major detriment to the profile of the security function, given that part of the CISO's role is to make senior management aware of increasing risks to the organization and the importance of an adequate security budget to combat them. Like other sectors, life sciences organizations have done little to converge the physical and logical security functions but have taken small steps toward exchanging information.

Security regulatory compliance is the top organizational initiative for the life sciences sector, security infrastructure improvements and identity and access management are the top operational initiatives, and data leakage protection is the top threat-based initiative. Top expenditures for the life sciences sector are infrastructure protection, desktop and gateway anti-virus, and security consultants.

When it comes to barriers to information security, life sciences was the only sector where respondents felt that the increasing sophistication of threats was as great a factor as budget constraints and lack of resources and this is understandable. Biotech and pharmaceutical companies face greater security risks than the other two sectors, given the tremendous value of their intellectual property and the amount of clinical trial information that they generate, as well as the risks associated with data sharing necessitated by partnerships and alliances.

### Health care providers

This is the sector with the most mature security functions—a full 71% have a CISO. The most common reporting relationship for the CISO is to the CIO. Only 10% of provider organizations have converged security functions, with 8% intending to converge in the next 12 to 24 months. Again, this is a sector where total convergence may simply not make sense.

Regulatory compliance initiatives are the primary organizational initiative for providers, followed by reporting and measurement. Providers face the challenge of complying with varying requests, which means that they must assess each component of a measure's requirements to ensure that appropriate data are collected and reported accurately. As with other sectors, identity and access management is the primary operational initiative. Data leakage protection is cited overwhelmingly (71%) as the primary threat-based initiative.

Budget constraints and lack of resources are cited as the greatest barrier to security. However, while the security budget often does not support the organization's top initiatives, in this sector it does: the majority of respondents state that their health care regulatory compliance spending will increase, indicating that, while budgets may shrink and the global economic situation may continue to decline, spending on regulatory compliance is still a high priority.

### Health care payers

Health care payers are the sector least likely to have a CISO; 57% do not. Of those organizations that do have a CISO, the majority, as in other sectors, report to a CIO. It may be that convergence of physical and logical security rarely, if at all, becomes necessary in the payer sector but, as in other sectors, the two areas have taken steps to collaborate to facilitate knowledge sharing.

Governance for security and security regulatory compliance are the top organizational initiatives; identity and access management is the top operational initiative; and data leakage protection is the top threat-based initiative (by more than 30% over its next closest contender, malicious attacks). While these initiatives are generally reflective of the top internal/external audit findings, the majority of respondents' IT budgets do not support them. The greatest portions of IT budget, after personnel and organizational costs, go to infrastructure protection devices and products, as well as incident response, indicating a reactive rather than a proactive response. And, as in other sectors, budget constraints and lack of resources were seen as the greatest barrier to security.

More than half of health care payer respondents in the United States cite managing third-party information-sharing as one of the top three privacy concerns in the organization. The major challenge organizations face with regard to outsourcers and third parties is the process of ensuring that outsourcers are compliant with the organization's information security policies. Most do not conduct a regular assessment to ensure compliance nor do they go through the process of assessing, reviewing, and testing third-party capabilities on a regular basis.

# Study findings and discussion – Life Sciences

## Governance & Reporting

### Defined security governance framework

Over 44% of respondents do not have a security governance framework defined. This may indicate a lack of execution on organizational security policies as well as a lack of oversight and discipline for non-compliance with organizations' security strategy and policies.

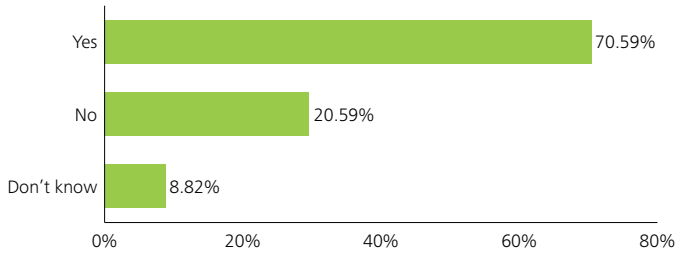
### Commonly accepted security framework

The majority of respondents (70%) utilize a commonly accepted security framework. However, the security frameworks are built heavily around industry standards, such as COBIT, ISO27001/27002, CCOW, HITSP/TN900, etc. (16%) rather than around compliance regulations (12%) or internal policies and standards (10%). The industry standards focus would suggest that respondents see the necessity for the framework from a competitive point of view, rather than from recognition of the link between a security framework and effective information security. Less than half (40%) of respondents use their security framework to measure and monitor their risks. Even fewer (28%) utilize the security framework to prioritize security efforts. These findings beg an obvious question: are organizations getting the most effective use out of their security frameworks?

Almost 70% of respondents believe a common framework will be helpful to the industry, a response that may reflect some frustration with the vagueness of existing security requirements.

The changes expected to arise out of the stimulus bill in the United States may help to move the security framework along. ARRA requires the Certification Commission for Health Care Information Technology (CCHIT) to develop security criteria for EHR implementations.

**Figure 1 (LS) – Adherence to a commonly accepted security framework**

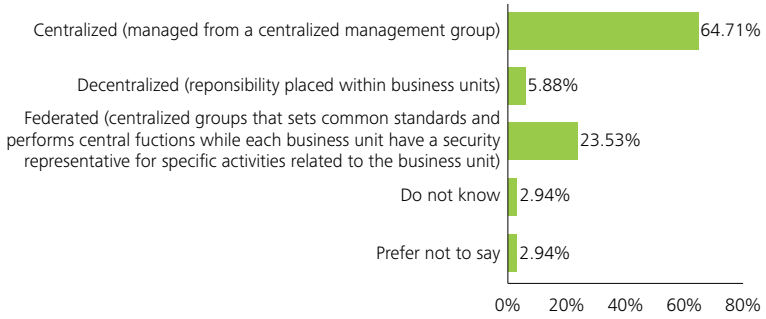



Large life sciences and biotechnology organizations with operations in EU countries have to be particularly cognizant of protecting information when it comes to their obligations under the EU Directive on data privacy.

## Information security model structure

The greatest number of respondents (65%) state that their information security model structure is a centralized one, the traditional information security structure. The federated model (where a centralized group sets common standards and performs central functions while the business units maintain some control over "local" execution) accounts for 24% of respondents. This percentage is understandable given that the federated model is more applicable to large, global organizations and does not make sense for up-and-coming biotechnology companies or small hospital systems, for example. In an age of increasing regulation and oversight as well as the impact of moving to more shared services centers, it is understandable that the decentralized model (6%) is losing ground.

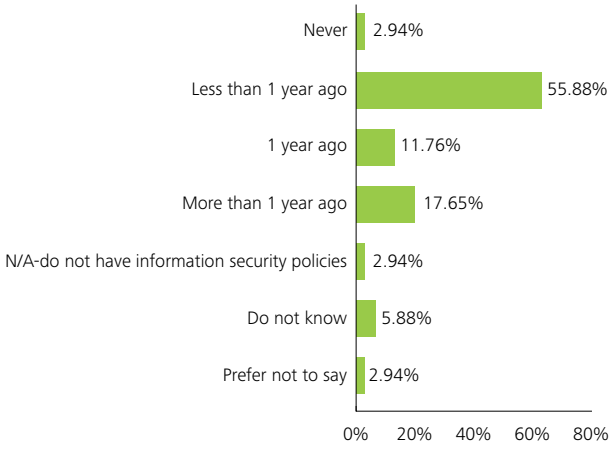
**Figure 2 (LS) – Information Security Model Structure**




## Electronic storage of medical records

Less than half (44%) of respondents indicate that they store medical records electronically. This percentage could well remain in this range for a number of years. Those who store electronic records use them primarily for serving patients. The U.S. stimulus package is focused on providers and independent physician groups with respect to EHR under the HITECH Act. The large pharmaceutical and biotech organizations do not generally have a reason to store medical records although they may electronically store medical records related to research studies.

**Figure 3 (LS) – Compliance with relevant laws and regulations**




## Policy compliance

It appears that organizations surveyed are being proactive with regard to policy review for compliance with relevant laws and regulations. Of the organizations surveyed, nearly 70% have reviewed their policies to ensure compliance within the past year or at least one year ago. This finding is consistent with a heavy focus on compliance by life sciences organizations. Only 18% state that they have reviewed their policies more than a year ago.

Almost 66 % of respondents have assessed the practicality of their security policy in the last year, which indicates a heightened focus on not only documenting the policy but making sure that it can be operationalized.

When asked if they had reviewed their policies against industry security standards, 54% of respondents indicate that they have done so in the last year. This is slightly less than the number of organizations that state that they have reviewed their policies against legal and regulatory compliance requirements.

### Records management policy

The majority (63%) of respondents indicate they have a records management policy based on current global regulatory requirements. But it is not clear what percentage of those that have one have actually operationalized it. For those who have not, this practice presents a major security issue because keeping data longer than necessary for legal, regulatory or legitimate business purposes dramatically increases an organization's risk, e.g., breach of PII.

### E-discovery

E-discovery relates to the compulsory disclosure, at a party's request, of electronic information that relates to litigation. IT plays an important role in how content that becomes evidence is created, preserved, collected and turned over to the appropriate authorities. Of respondents surveyed, 82% say that they have someone in the organization that can produce a computer file that can be used as legal evidence. However, almost half of respondents either do not have access to an attorney who can accurately present the organization's IT architecture, do not know, or prefer not to say. This may be indicative of a problem area in that attorneys may write policies (privacy, security, data retention, etc.) that do not accurately represent the organization's operating environment and cannot, therefore, be operationalized.

### Document retention

There appears to be a document retention policy in 70% of the respondent's organizations. While less than half (47%) say the policy is strictly enforced, another 47% say it is either not enforced or they do not know.

### Executive support for projects

With regard to senior executive support of security projects to address regulatory and legal requirements, roughly 60% of the organizations say that they are receiving adequate funding and support for projects. However, 21% indicate that they receive support but no funding while 6% say there is neither commitment nor funding.

**Figure 4 (LS) – Presence of individual within organization who can provide electronic legal evidence**

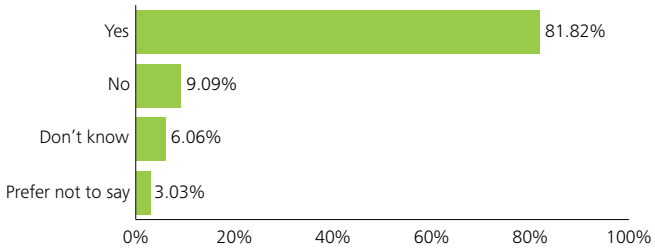
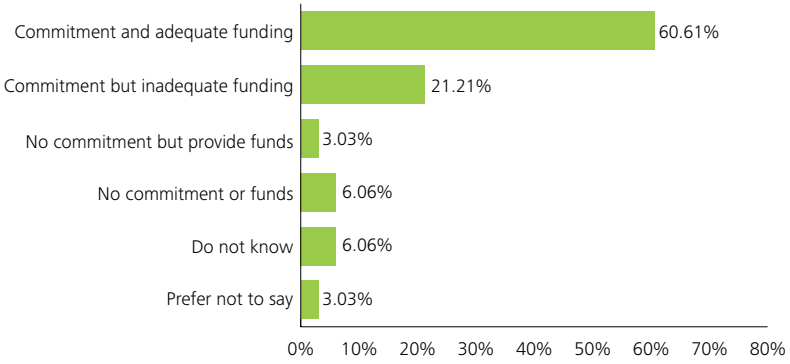



**Figure 5 (LS) – Senior executive support for projects that address regulatory or legal requirements**



# The information security function and the role of the CISO

### Existence of a CISO

While 50% of respondents do have a CISO, a full 44% do not, despite the significant security and privacy risks faced by the life sciences industry. This is a major security issue since part of the role of the CISO is articulating the benefits of the security program and making senior management aware of increasing risks to the organization.

### Reporting relationship of the CISO

Respondents indicate that the most common reporting relationship for the CISO is the CIO. While this reporting relationship is logical, it is not necessarily the most optimal for the profile of the CISO, because it is one in which the influence of the CISO over the way information is managed tends to be moderate, while hands-on ownership for technical responsibility still tends to be high.

**Figure 6 (LS) – Existence of a CISO within the organization**

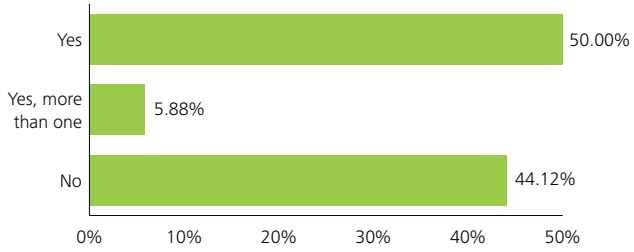
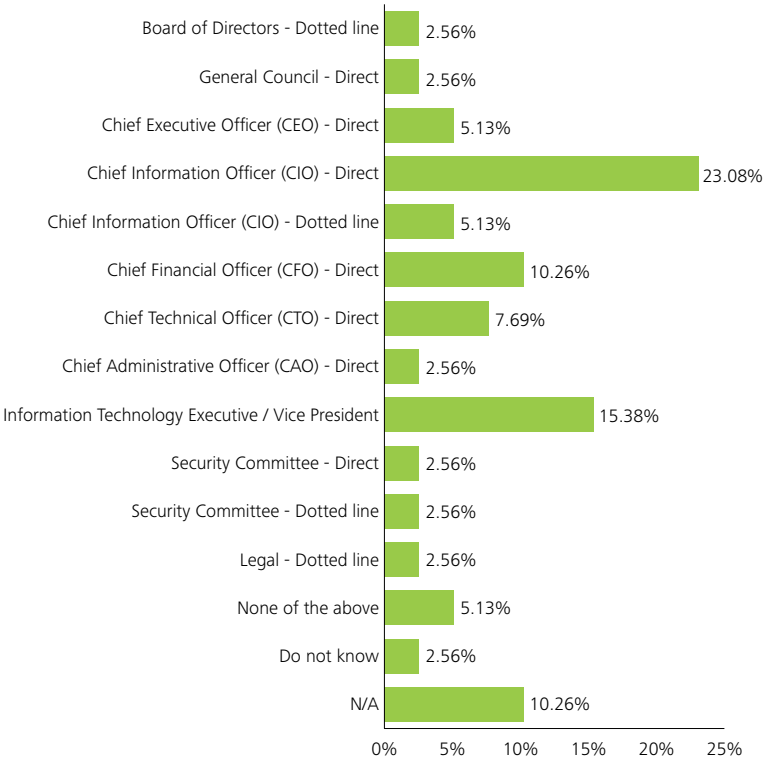



**Figure 7 (LS) – Reporting relationship of the CISO**



## Responsibilities of the CISO

Study results indicate that the focus of the CISO is increasingly on core information security-related activities, such as risk management (68%), vulnerability and threat management (65%), security architecture (65%), security governance (62%), and internal security awareness. Areas such as business continuity, privacy, physical security, and law enforcement interaction receive less of the CISO's attention. This may indicate an increasing trend to divide these responsibilities among several resources within the organization. This is an interesting finding because security is such a big part of privacy as well as of situations dealing with law enforcement.

## Information assets protected under the responsibility of the CISO

Respondents indicate that the CISO's focus appears to be heavily weighted to digital assets, despite the evidence that loss of paper and other information in a non-digital format can have significant ramifications to the organization.

## Convergence

Physical and logical security continue to be largely segregated despite the fact that physical security plays an important role in the protection of both digital and paper assets. Respondents indicate that only 6% of organizations have fully converged physical and logical security and 65% have done nothing to converge.

This finding can benefit from some perspective. The idea behind convergence in a security context is the ability to combine physical and logical security systems to enable security efficiencies, including, for example, better access control and, therefore, tighter overall security. Most people typically view convergence as an all or nothing proposition—and a massively expensive and complex undertaking—rather than as a series of small steps, such as the establishment of risk councils, etc. For example, 14% of organizations have physical and logical operations segregated but facilitate knowledge enablement and information exchange between the groups, which are

**Figure 8 (LS) – Functions within the scope of the CISO**

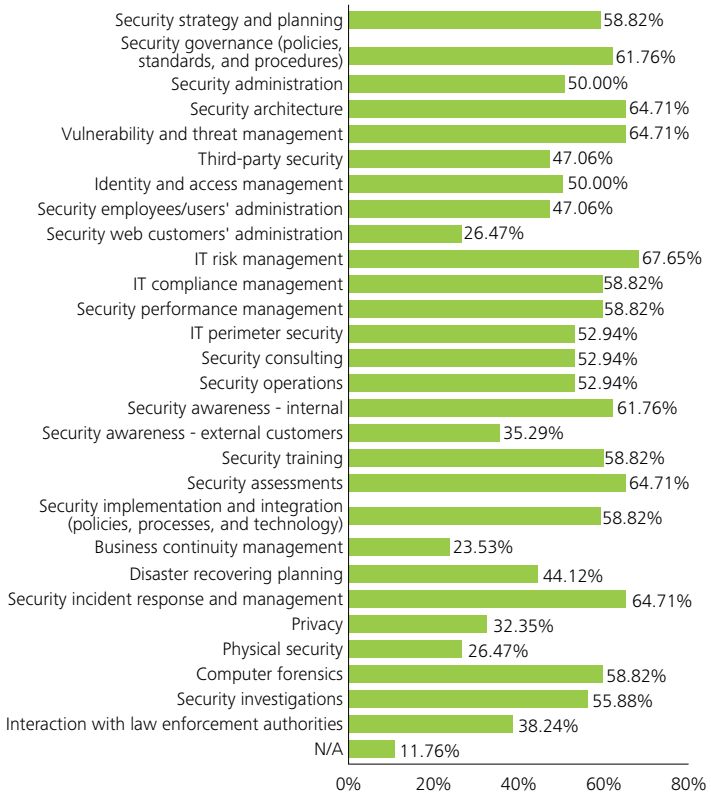
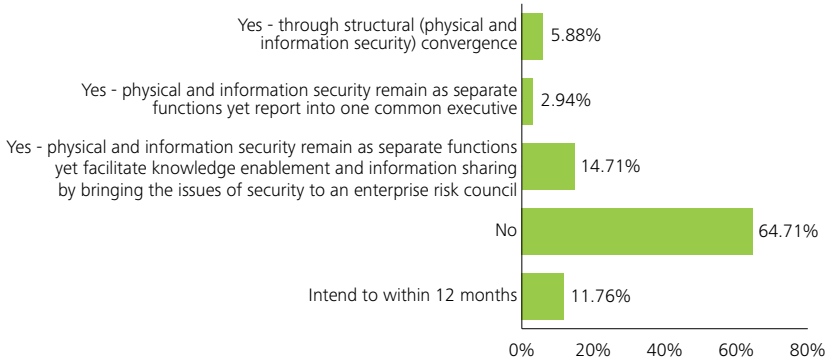



**Figure 9 (LS) – Convergence of information security and physical security**



small steps toward convergence. Also, 14% state that they intend to converge physical and logical security in the next 12 months. The physical and logical security functions report to the same leader in only 3% of the organizations surveyed.

### Information security strategy

Respondents indicate that 38% of organizations have a fully documented information security strategy. Respondents that do not have a strategy comprise 21%. The same number (21%) have a security strategy in draft form, 18% have a plan to complete the document within 12 months and 3% plan to complete the document within 24 months.

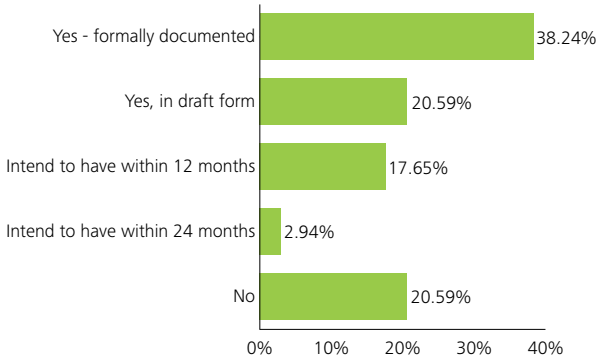
Since the information security strategy is a plan as to how the organization can mitigate risks while complying with legal, statutory, contractual, and internally developed requirements, those organizations that do not have one are likely to be at a distinct disadvantage going forward. A security strategy is a foundational step towards protecting PII as well as PHI and intellectual assets.

### Areas covered by information security strategy

Another issue beyond the mere existence of a strategy is how it is being used and what it contains. Of those organizations that have a documented security strategy or are in the process of implementing one, 62% indicate that the focus of the strategy is to assign security roles and responsibilities. While this is a necessary part of the strategy, the bigger issue is whether the strategy captures the organization's information security strategy requirements, whether it includes a people strategy, whether it includes metrics and performance management (which is necessary to help ensure that what is being

Study findings indicate that the role of the CISO has taken on a greater significance and visibility in that the scope of the position is now more heavily weighted toward a C-suite focus on security.

**Figure 10 (LS) – Presence of a defined information security strategy**



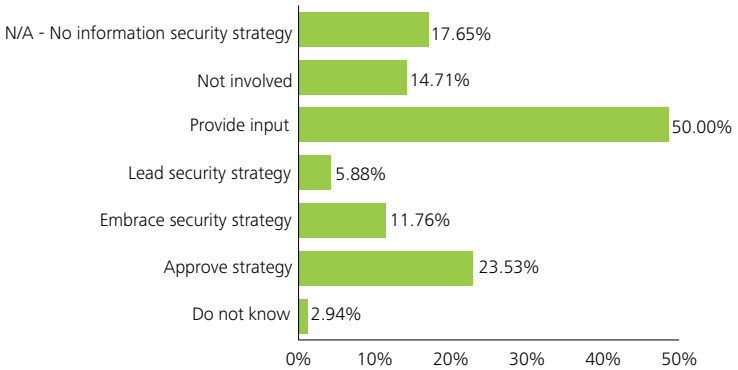
done is meeting the expectations of business), and finally, whether or not the defined information security strategy requirements are aligned with the strategic objectives of the organization. In this sector, a majority of respondents (53%) state that their information security strategy covers alignment with the organization's strategic priorities. This is a relatively high and encouraging finding.

### Level of involvement in information security strategy

There appears to be involvement from executives in the information security strategy. Half of respondents indicate that their executives provide input and 24% indicate they are involved in approving the strategy.

**Figure 11 (LS) – Topic areas covered by information security strategy**


**Figure 12 (LS) – Level of involvement of executives in information security strategy**



## Top security initiatives

The top security initiative, from the combined pool of organizational, operational and threat-based initiatives, is security regulatory compliance, understandable given the current regulatory climate. Data leakage protection is the initiative mentioned by the next greatest percentage of respondents, followed by, in a three-way tie, governance for security, security infrastructure improvement, and identity and access management. Identity and access management is a major focus for organizations as they struggle to strike a balance between access to information and protection of data.

## Barriers to implementing IT security

When it comes to barriers to implementing IT security, over 40% of respondents believe that budget constraints and/or lack of resources are the greatest barriers, understandable given the economic climate. Following closely on the heels of the number one barrier, are the increasing sophistication of threats and emerging technologies, tied for the number two spot at 38%. As the bombardment and sophistication of threats increase, organizations may typically be perceived as treading water in responding to them, no matter how proactive they are generally.

## Reporting on status/incidents

The most frequent reporting to the Board of Directors is annually (29%) which is slightly lower than annual reporting to the audit committee, (32%). When it comes to the CEO, 50% of respondents indicate that the person is briefed only on an ad hoc basis, when an incident occurs, or not at all. Lines of business executives fare better, with the most frequent reporting quarterly (23%). But almost 59% of respondents are providing updates on information security on an ad hoc basis or not at all.

This finding is indicative of a lack of organizational awareness of security risks, which can impact security program funding and can also result in major financial and reputational damage. ARRA includes wide-reaching data breach notification provisions for entities covered by HIPAA and organizations servicing those entities. The Act is likely to increase joint enforcement activities by the Federal Trade Commission and the Department of Health and Human Services Office for Civil Rights. An example is the recent settlement by a U.S. pharmacy chain charged with violating HIPAA and with failing to take appropriate

**Figure 13 (LS) – Top security initiatives: organizational, operational, threat-based**

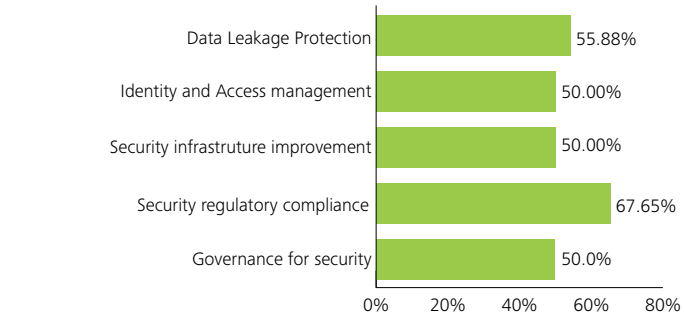
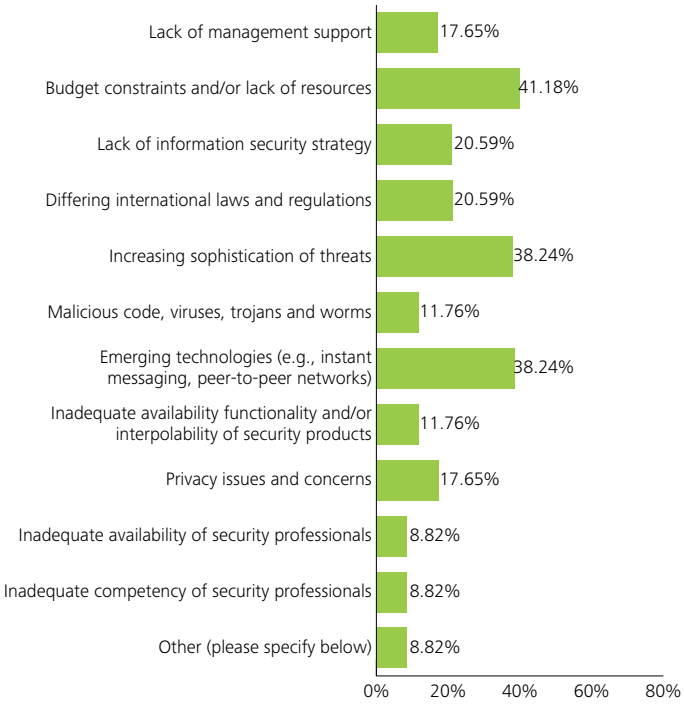



**Figure 14 (LS) – Barriers to implementing IT security**



security measures to protect sensitive financial and medical information.

### Internal/external audit findings

The top five internal and external audit report findings within the last 12 months are (with the first three tied for first place): DRP/BCP documentation/currency; lack of audit trails/logging; segregation of duties; lack of clean up of access rules following a transfer or termination; and lack of DRP/BCP testing.

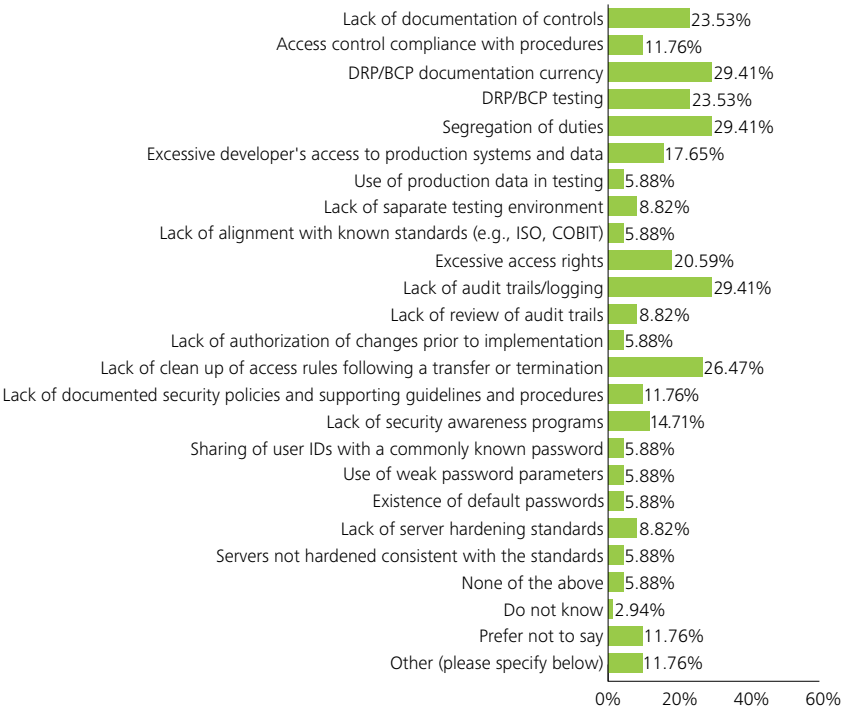
A large number (66%) of organizations state that business continuity plans are not in place or in place for only a limited number of departments. Experience with life sciences organizations has shown that companies who take a laissez-faire approach to mandating business continuity plans are typically unpleasantly surprised when a disruption to a company's critical operations reveals how ill-prepared they are for rapid recovery and resiliency.

Lack of sufficient audit trails and logging (to show who accessed the system and what operations he or she performed during that time) goes hand in hand with excessive access rights, a top ten audit finding and a top operational initiative for organizations.

Segregation of duties is an important information security control. There is a lack of segregation of duties when one individual has access to responsibilities that are inherently in conflict with one another. For example, the same person should not accept cash, record deposits, make deposits, and reconcile the bank account. It is a lack of segregation of duties that allows some individuals to undertake embezzling schemes that go unnoticed for years.

When it comes to excessive access rights, auditors and regulators have an expectation that organizations will assign access only to those individuals and to those applications that are needed to perform their jobs. And when those rights are no longer needed to perform the job, they expect those rights to be revoked in a timely fashion. But what should be a relatively simple undertaking is continually complicated by changing job responsibilities, a more mobile workforce, employee turnover, and corporate reorganizations and mergers, with the result that excessive access rights remain an ongoing thorn in the sides of many organizations.

**Figure 15 (LS) – Top five internal/external audit findings**




### Top expenditures covered under the information security budget

The top five expenditures covered under the information security budget in order of the greatest spending are:

1. Security consultants
2. Infrastructure protection devices/products
3. Desktop and gateway anti-virus
4. Personnel and organizational costs
5. Awareness/communication costs

It is encouraging to note that awareness and communication are in the top five expenditures under the security budget, since an increase in awareness and communication often translates to better understanding of security risk and, therefore, greater allocation of funding. However, it is unclear how much of the security budget is directed to strategic planning versus tactical implementation, which would provide greater insight into whether organizations have the right strategy to mitigate its most critical risks.

Incident response is relatively far down the list of priorities covered by the information security budget, raising the question of whose budget it is coming out of. In addition, business continuity management is a low priority, which makes it appear as a separate issue from security.

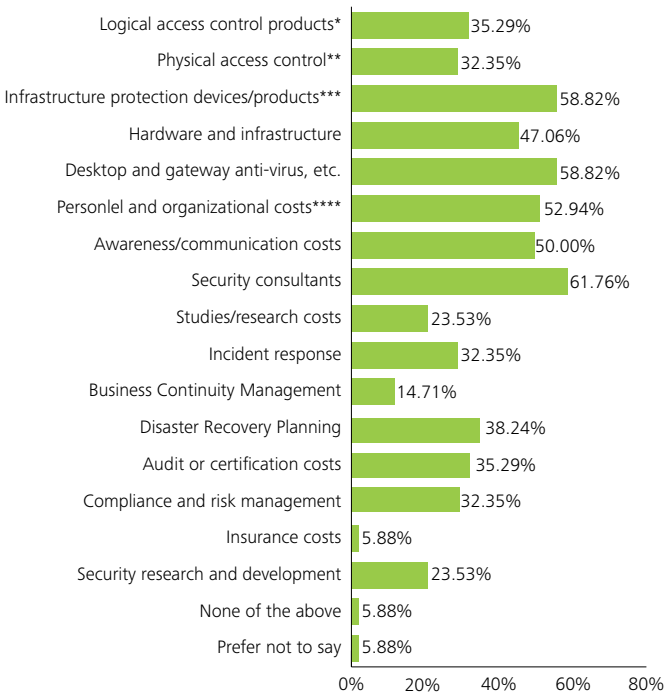
Interestingly, the top five security initiatives for which respondents indicate they will spend money in 2009 (e.g., data leakage protection and identity and access management) do not align with the top five expenditures that respondents say are covered under their security budgets.

### Budgets and funding to address regulatory requirements and IT security projects

Respondents see security projects funding as an issue. Of the organizations surveyed, only 56% say that security projects are "adequately funded" to effectively address regulatory requirements; 29% say that projects are "not adequately funded" and the other 14% do not know or did not respond.

Respondents admit that their people (which includes third parties) are organizations' biggest security worry—83% are equally or more concerned with internal security threats than with external threats.

**Figure 16 (LS) – Expenditures covered under the information security budget**



### Information security budget as part of IT budget

Only 30% of the organizations surveyed have a separate budget for IT security projects—65% say that security projects are merged in with the main IT budget. This finding is consistent with Deloitte member firm in-field experience and harkens back to a key finding: although the security environment becomes more complex and regulation continues to increase, security budgets are simply not getting the profile they deserve, losing out to projects that are perceived as having a greater effect on furthering the business.

### Percentage of IT budget dedicated to information security

When asked what percentage of the overall IT budget is dedicated to information security, 67% of respondents indicate that less than 10% of their overall IT budget is dedicated to information security. This is consistent with the finding that security budgets are not keeping pace because security is not getting a high enough percentage of the overall IT budget. Of the 67%, 45%, by far the largest group of respondents, indicate the smallest percentage increase, 1-3%. Only 9% of respondents indicate a budget greater than 11%, while a full 12% of organizations surveyed say they have no budget dedicated to IT security. It is not clear how this 12% operates without a budget—projects would have to be buried by the business or lumped in with another group.

Globalization, service orientation and outsourcing have changed the requirements from those of the last two decades. Because information is what is valuable now, data protection is where the focus must lie.

**Figure 17 (LS) – Information security budget as part of IT budget**

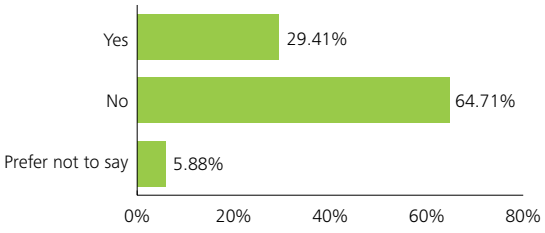
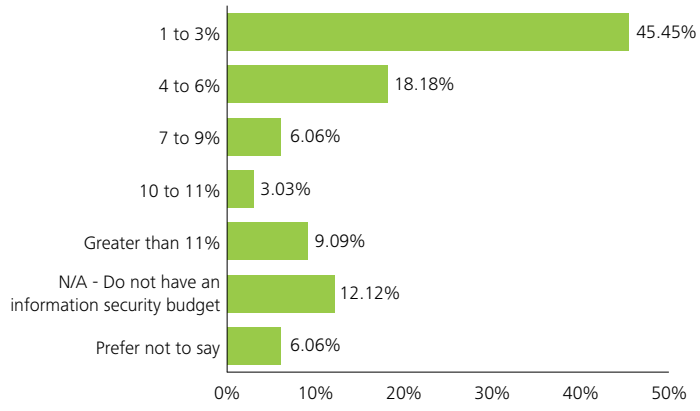



**Figure 18 (LS) – Percentage of IT budget dedicated to information security**



### Increases in information security budget

While 60% of respondents indicate an increase in their security budgets year over year, reflecting an increased focus on security, by far the largest percentage of respondents (38%) still indicate a budget increase in only the smallest category (1-5%).

### Sources of additional information security funding

While it is no surprise that the IT function is identified by respondents as the top source of additional information security funding for IT security projects and initiatives, it supports the continuing theme that management sees security as an IT problem. While the security budget itself may be low, other functions also contribute to security initiatives. The other four funding sources, in descending order, are legal function/ budget; lines of business; compliance/regulatory function; and project sponsors.

### Information security projects that deliver as promised

Security projects appear to be delivering as promised in most cases, as the highest percentage of respondents (29%) indicate that security projects fail to deliver only between 1 to 15% of the time. However, when it comes to measuring the success or failure of IT security projects, 21% of respondents indicate that they do not measure, which raises the issue of whether respondents truly know whether or not their projects succeeded or failed.

### Reasons projects fail

Respondents indicate that the top reasons projects fail are due to a lack of resources and integration problems. A stated lack of resources is to be expected in hard economic times; it is also the universal lament of most functions, particularly so when projects do not achieve the expected results.

**Figure 19 (LS) – Year-over-year increases in information security budget**

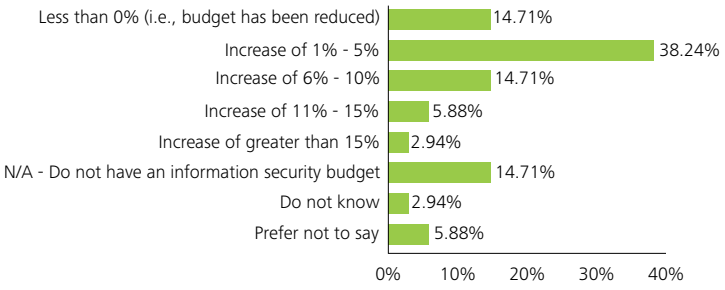



**Figure 20 (LS) – Information security projects that deliver as promised**

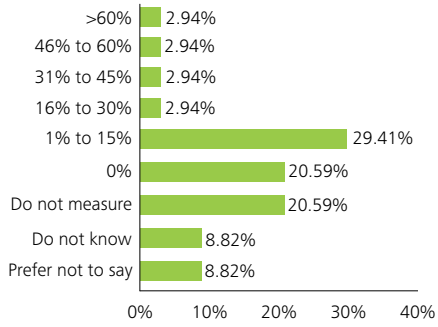
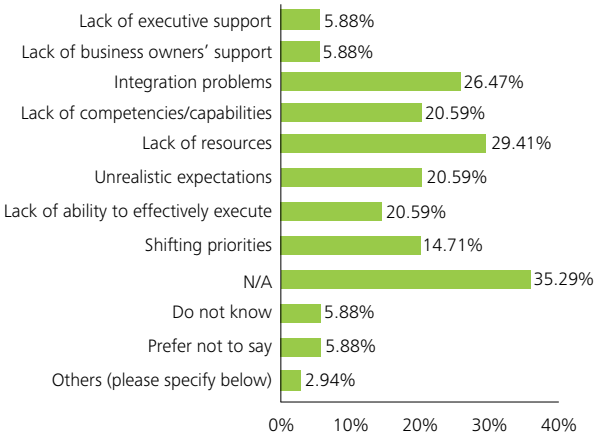



**Figure 21 (LS) – Causes of failure of information security projects**



## Levels at which information security is considered a key imperative

Respondents indicate that the levels within an organization that most consider information security a key imperative are (in descending order): executive management, IT leads, Board of directors, middle management and business unit leads.

It is clear from the responses that information security is considered key to executive management. However, the disconnect comes when the responsibilities for delivery tend to be given to IT management. Management may see information security as being a key consideration of other business functions but the funding is simply not backing this up.

## Meeting the needs and expectations of the organization

Although feedback from most functions is positive, it is still only a small majority (56%) that sees information security as "somewhat effective" in meeting the needs of this business. This response could mean that most functions do not know the risks and may not know if the security policies and commensurate investment are truly meeting requirements.

In addition, although IT is considered where the imperative for information security lies, other functions could well consider the delivery of IT security as effective to a large degree. And this may mean that the business does not see the need to invest in security. The issue of security effectiveness is very much a question where the jury is likely to be out for a long time.

**Figure 22 (LS) – Levels at which information security is considered a key imperative**

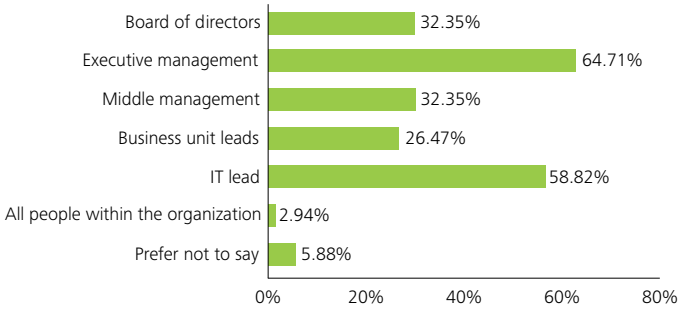
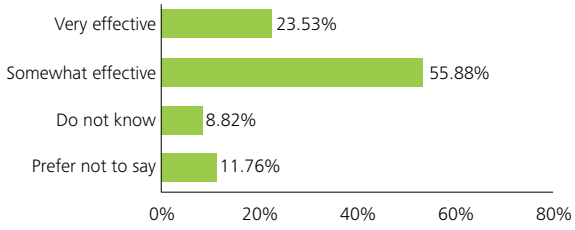



**Figure 23 (LS) – Effectiveness of information security in meeting the needs of the business**



# Risk

### Internal/external security threats

Confirming once again that people are an organization's greatest asset as well as its greatest weakness, 44% of respondents have a greater level of concern regarding the conduct of internal people than they do regarding external people (18%).

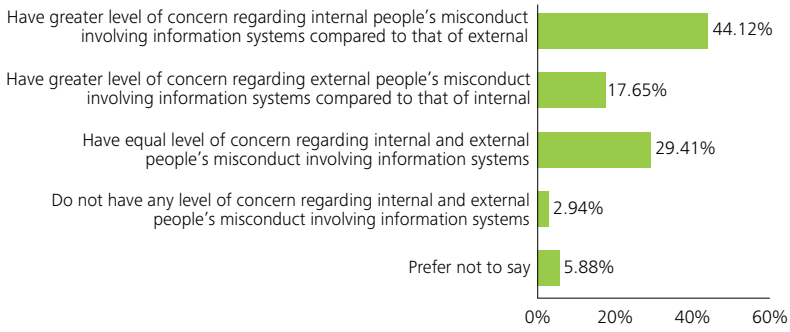
Organizations are more confident about protecting information assets from external breaches than from internal breaches. Respondents indicate that inappropriate use of sensitive data and information leakage rate high as a threat in terms of impact and likelihood. Interestingly, the places where organizations are spending their money, e.g., regulatory compliance, do not align with their stated greatest threats.

The crucial question for an organization is how to give your own resources access to the right information while, at the same time, making sure the information is used appropriately. This is particularly relevant in hard economic times, when employees are likely to be more desperate and more disgruntled. In a web-based survey, the Ponemon Institute found that "59 percent of ex-employees admit to stealing confidential company information, such as customer contact lists. The results also show that if respondents' companies had implemented better data loss prevention policies and technologies, many of those instances of data theft could have been prevented."*

Surprisingly, 3% of respondents have no concern about either internal or external people, which indicates a state of denial since people are at the heart of virtually all security breaches.

**CIO.com "Laid off Workers as Data Thieves?" by Bill Brenner, February 24, 2009; retrieved from http://www.cio.com/article/482413/Laid_Off_Workers_As_Data_Thieves on April 8, 2009*

**Figure 24 (LS) – Level of concern about internal versus external people**




### Frequency of internal breaches

Respondents reveal the nature and frequency of internal breaches that occurred in the past 12 months (ranked in order of frequency of reported incidents):

- Loss of customer data/privacy issues (information leakage)
- Virus/worm outbreaks
- Wireless network breach
- Phishing/pharming
- Internal fraud.

### Frequency of external breaches

Respondents reveal the nature and frequency of external breaches that occurred in the past 12 months (ranked in order of frequency of reported incidents):

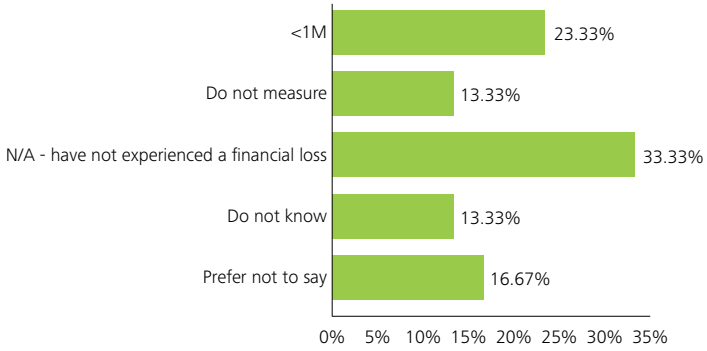
- Virus/worm outbreaks
- Employee misconduct
- Physical breach
- Phishing/pharming
- Social engineering
- Malicious remote access
- Website defaced
- Zombie networks.

### Impact of breaches

Of the organizations who reported a breach:

- 23% report direct costs (e.g., clean up and recovery) and indirect costs (e.g., loss of brand) of US$1 million or more
- 32% have not had a loss
- 13% do not measure loss due to a breach
- 13% do not know the loss amount resulting from a breach.

**Figure 25 (LS) – Total damage as a result of breaches**




The constant balancing act for organizations is providing convenient access for employees while maintaining strong access control to information.

Nearly 27% of organizations surveyed either do not measure or do not know about the impact of their security breaches. This means that these organizations likely do not know what data has been exposed. In addition, many organizations are not aware that the cost of breaches is on the rise. A 2007 report* shows a 43% rise in costs compared to 2005. The total average cost of a data breach grew to $197 per compromised record and the average total cost per reporting company was more than $6.3 million per breach.*

*SearchSecurity.com "Data Breach Costs Soar" by Bill Brenner, November 29, 2007; retrieved from http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1284140,00.html on April 8, 2009*

### Top three root causes of failure

Study respondents reveal that the top three root causes of information system failures (e.g., breakdowns, incidents, breaches, interruptions, outages) are human error; operations; and technology, tied for third place with lack of documented processes.

It is clear that organizations view breaches as caused by human error; therefore, a lack of training has to play a role in the failure.

### Outsourcing and third-party/vendor relationships

An organization's people include not just its employees but its third parties and vendors as well. In the context of a preceding graph, respondents express concern about their internal people and the extent to which they consider them a greater threat to the organization than external people. A sub-set of that is managing third-party information sharing, which organizations say is their second greatest privacy concern.

A full 77% of organizations have their information systems set up to provide access to authorized third parties. Almost the same percentage review the security of vendors and third parties before exchanging data with them. However, 9% do not. Of the companies surveyed, 22% do not require data to be encrypted in transit between vendors/third parties—a factor which is going to present issues for organizations covered under the revised HIPAA security and privacy rules. Once the initial review of vendors is complete, 15% of organizations do not review the vendor on an ongoing basis to identify additional threats.

Once a vendor has been engaged, the most common ways that organizations ensure vendor activities are adequate are to control the access that the vendor has to systems and data (44%) and to address information security issues in a contract (41%).

**Figure 26 (LS) – Top three root causes of failure**

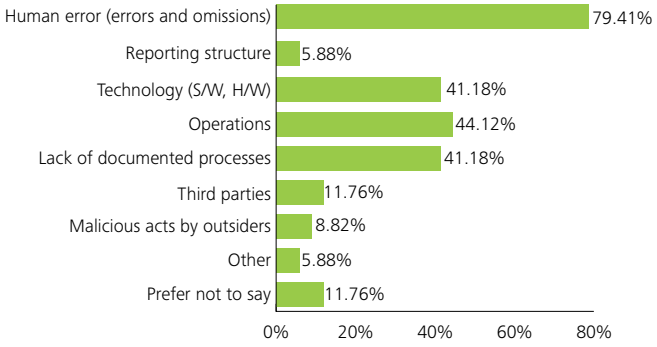
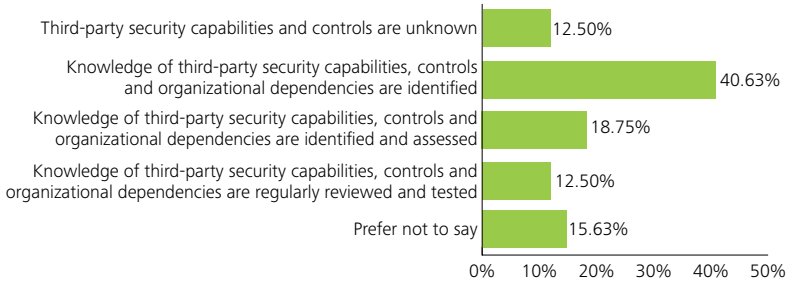



**Figure 27 (LS) – Knowledge of third-party security capabilities and controls**



# Use of Security Technology

### Deployment of technologies

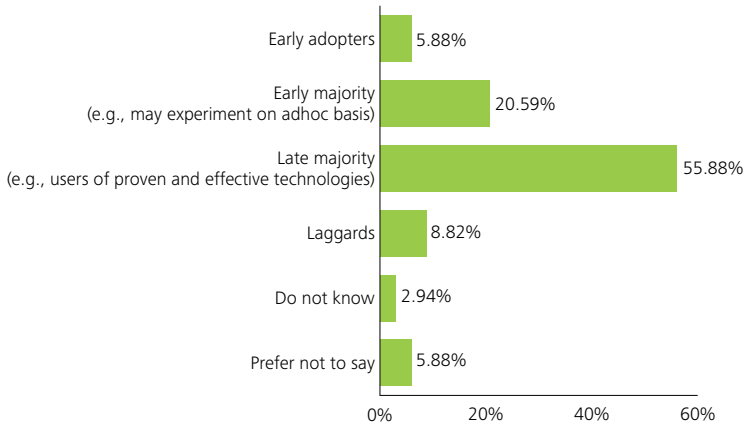
In terms of adopting new technologies, 6% are "early adopters"; 20% are "early majority" (e.g., may experiment on ad hoc basis); 56% are "late majority" (e.g., users of proven and effective technologies); and 8% are "laggards".

The well known security and privacy countermeasures appear to be deployed for the majority of organizations (94%, firewalls; 91%, antivirus; 89%, spam filtering solutions; 82%, VPNs; 71%, wireless security). However, several notable countermeasure deployments are under-deployed. For example, only 8% have data leakage protection solutions; only 8% have fraud protection systems; only 8% have federated access; only 20% have provisioning solutions; only 20% have instant messaging solutions; and only 55% have Intrusion Detection Systems (IDS)/Intrusion Protection Systems (IPS) solutions.

However, those organizations that have not deployed countermeasures plan to deploy the following within the next 12 months: data leakage protection technology; single sign-on; vulnerability management strategy & solution; provisioning systems, RFIDs; log management software; federated access; and web-services security.

Data leakage protection technologies are clearly a priority for organizations. Although few respondents have this technology currently deployed, an increasing number of organizations indicate that they plan to adopt data leakage technologies over the next 12 months.

**Figure 28 (LS) – Level of adoption of security technologies**



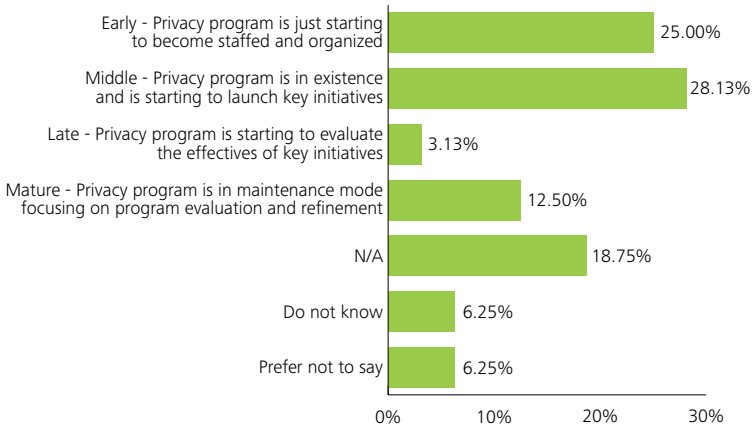

As in other industries, there is constant pressure on IT departments within life sciences and health care organizations to not only maintain services but improve upon them while controlling expenses.

# Quality of operations

### Security Training Program

While 55% of organizations have a formal security training program and have enforced training for each employee within the past 12 months, 35% of organizations do not offer training nor is it mandatory for the entire organization. Few respondents offer online awareness programs.

**Figure 29a (LS) – Stage of development of the privacy function**




# Privacy program

Of the organizations surveyed, only 12% have a mature privacy program. Over half of respondents say that their organizations' privacy programs are in the earlier or middle stages of development. This is not surprising, given the relatively recent emergence of privacy and data loss legislation as an important compliance and risk issue for organizations.

Since the regulatory environment is becoming more complex and the exposure to an organization for failing to comply with privacy laws is becoming significantly greater, the expectation is that these programs will become increasingly more developed in the coming years for certain groups of companies, such as small life sciences organizations or those with a mostly U.S. presence. Global life sciences organizations have been dealing with privacy for years through the Data Protection Directive, a European Union (EU) directive which regulates the processing of personal data within the EU.

### Chief Privacy Officer or equivalent

Respondents from over one third of U.S. organizations polled state that they have a Chief Privacy Officer (or an executive charged with protecting the privacy of information). Since the recent enactment of certain provisions of ARRA (specifically the HITECH Act) which adds significant rigor to existing HIPAA legislation, Deloitte member firms are noticing a significant increase in the hiring of privacy professionals in the life sciences industry.

### Reporting relationship of the privacy executive

According to respondents, the majority of organizations have their Chief Privacy Officers reporting to General Counsel although several Chief Privacy Officers have a solid or dotted line reporting relationship to the CEO or the Chief Technology Officer. Although Chief Privacy Officers are often located in the Office of General Counsel—because organizations have traditionally viewed this function as driven by legal and compliance concerns—it is becoming increasingly common to see this office aligned with the enterprise risk function.

### Responsibility of the privacy executive

Since privacy departments are typically comprised of relatively few staff, the privacy executive is often required to wear many hats. Deloitte member firm in-field experience has shown that unlike many executives whose function is primarily concerned with strategic initiatives, Chief Privacy Officers are often the only individuals within an organization who can consult about privacy issues and manage privacy incidents as well.

### Privacy drivers

Respondents are almost unanimous in stating that the avoidance of brand and reputational risk was as important a reason to protect personal information as compliance and the avoidance of fines and penalties. Clearly, respondents understand that protecting personal information is simply good business.

Respondents are almost unanimous in stating that the avoidance of brand and reputational risk was as important a reason to protect personal information as compliance

### Top three privacy concerns

The primary privacy concern of respondents is the fear of unauthorized access to personal information. Managing third-party information sharing and aligning operational practices with policies are distant second and third choices, respectively.

Companies are employing many different types of technical solutions to manage unauthorized access of personal information, from laptop and mobile media encryption technology to data leakage protection products. Identity and access management programs are also being implemented to mitigate risk by limiting access to data only to those within the enterprise with a legitimate business need.

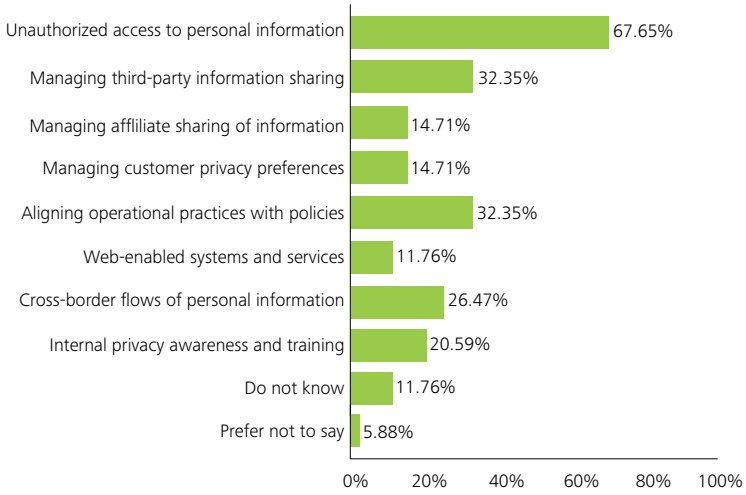
Large life sciences and biotechnology organizations with operations in EU countries have to be particularly cognizant of protecting information when it comes to their obligations under the EU Directive on data privacy. It is illegal to transport EU personal data across EU and non-EU country borders without an adequate level of data protection. While U.S. companies can self-certify their adherence to data privacy principles under a framework known as Safe Harbor, it does not protect them from the possibility of a criminal or civil complaint originating in Europe.

### Status of inventory of personal information (e.g., a data flow analysis of personal information collection, usage, storage, sharing and destruction practices)

While many organizations claim to have some sort of privacy program, almost none of the respondents indicate that their organizations have actually conducted an inventory of their personal information.

An inventory of personal information is a foundational component of any privacy and data loss program. Unless an organization knows the data that it is collecting, where the data is stored, with whom the data is shared, and how the data is protected, the entity leaves itself vulnerable to leaks and eventual breakdowns in its data protection levees.

**Figure 29b (LS) – Top privacy concerns**



# Business continuity planning

### State of business continuity planning

Almost 68% of respondents state that their business continuity plans are not in place or are in place for only a limited number of departments. This is a troublesome finding because experience has shown Deloitte member firms that life sciences companies that take a laissez faire approach to mandating business continuity plans are typically unpleasantly surprised when a disruption to a company's critical operations reveals how ill-prepared they are for rapid recovery and resiliency. Only 11% have plans in place to recover mission-critical processes.

### Top three key drivers behind the establishment of business continuity planning

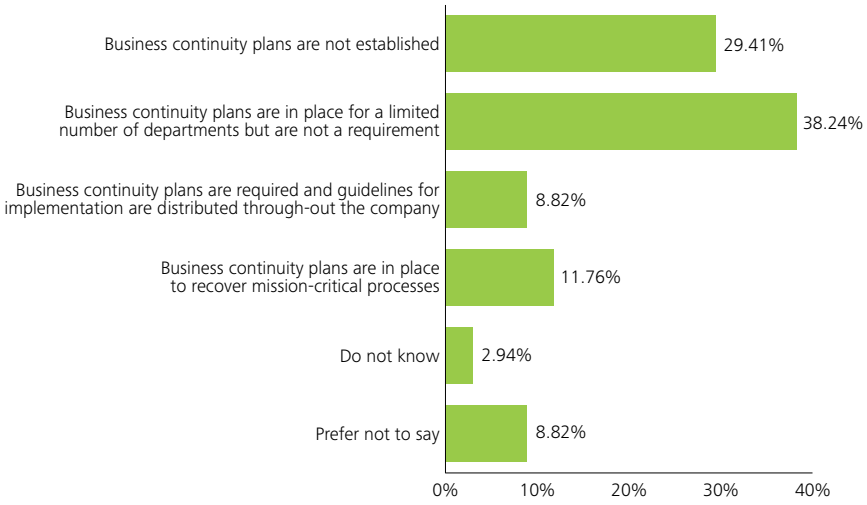
Most organizations have to experience a disaster or near miss to be "instant believers" in building business continuity and disaster recovery programs. Past events also help to raise awareness—2008 saw a significant number of natural disasters, including floods in Midwestern United States, hurricanes, and civil unrest.

Respondents indicate that the three major drivers for business continuity planning are:

- Executive/senior management's accountability for risk management
- Operating management's accountability for risk management
- Ensuring operational resiliency and availability.

Interestingly, each of these drivers requires that executive management is made aware of business continuity capabilities or deficiencies. However, experience has shown Deloitte member firms that life sciences companies are often apprehensive about making senior executives aware of the risks and deficiencies and, as a result, there are many cases of gaps between business expectations for business continuity and actual recovery capability.

**Figure 30 (LS) – State of business continuity planning**



### Extent of senior management involvement in business continuity planning

Almost 63% of respondents state that senior management is aware of the importance of, or has approved, the business continuity program. However, there is somewhat of a disconnect when you consider that 29% of respondents state that their companies have no business continuity program and 37% state that it is only limited to certain departments. Based on the experience of Deloitte member firms, this is an ongoing inherent problem: managers and staff of life sciences organizations do not build a case for improving or enhancing the program but nonetheless believe that executives are aware of the extent of it.

While 11% of respondents say that business continuity guidelines are distributed among departments, experience shows that typically, without clearly articulated policies and a modest testing/exercise program, this is not effective. When an organization distributes a guideline in a vacuum, it typically gets ignored, even when it is released following an audit.

### Frequency of testing with regard to business continuity

When it comes to testing of the business continuity plan, 37% of organizations say there is no testing. Only 23% of companies perform some level of regular testing. Another 22% of companies say that only "intermittent" testing is performed, with the result that 60% of respondents indicate either no, or only intermittent, testing. Most senior executives would maintain that they are uncomfortable with that risk position.

These outcomes suggest that:

- employees do not know their roles and responsibilities in the event of a disaster
- organizations have not validated the effectiveness of their business continuity plans
- organizations do not know if their systems or applications will be available during an outage or disruption.

These findings translate to practical issues that could be devastating to an organization in the event of a crisis.

Since the information security strategy is a plan as to how the organization can mitigate risks while complying with legal, statutory, contractual, and internally developed requirements, those organizations that do not have one are likely to be at a distinct disadvantage going forward. A security strategy is a foundational step towards protecting PII as well as PHI and intellectual assets.

# Study findings and discussion – Health Care Providers

## Governance & Reporting

### Defined information security governance framework

Respondents indicate that 45% of their organizations have an information security governance framework that is being executed. This may mean that the documentation of security management and the planning that is correlated to security management is becoming more prevalent.

### Information security framework

Of the organizations surveyed, 60% indicate that they adhere to a commonly accepted security framework. But 35% of respondents indicate that they either do not, or do not know if they adhere to a commonly accepted security framework. These organizations may have significant security gaps they are unaware of and not currently managing because they have not assessed their current state against an established benchmark.

The common security framework, HITRUST, mainly covers industry standards, e.g., COBIT, ISO27001/27002, CCOW, HITSP/TN900; compliance regulations, e.g., HIPAA, Sarbanes-Oxley Act (SOX); and internal policies and standards.

The majority of respondents, roughly 79%, indicate that a common security framework would be beneficial to the industry.

Only 28% of organizations leverage their framework to prioritize efforts. It is clear from this response that the framework is not a preferred tool for deciding when, and in what order, compliance topics are to be addressed.

### Information security model structure

A majority (67%) of those surveyed indicate that their security model is structured as a centralized management group, likely a core security team within the organization that works as a contiguous unit when creating and defining security management initiatives. This unit creates the security policies and standards that then get pushed out to the business groups from a centralized point, allowing for a uniform implementation of security.

**Figure 1 (HC Providers) – Adherence to a commonly accepted security framework**

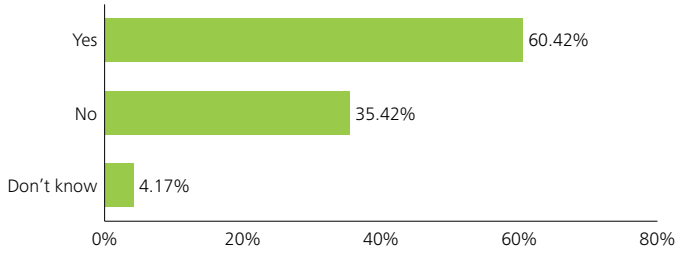
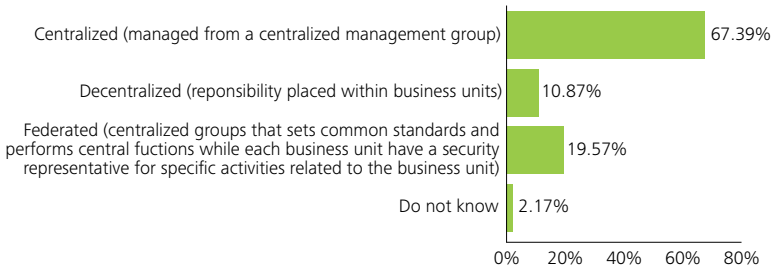



**Figure 2 (HC Providers) – Information Security Model Structure**



## Strategy to sustain compliance

Of the organizations surveyed, 47% indicate that they have a strategy in place to sustain compliance; 38% do not. The presence of compliance sustainment tools indicates an established information security management foundation, one with the ability to accommodate future regulatory requirements. This is going to be an issue for health care providers as there will be significant pressure on all organizations to meet the challenges of EHR technologies under the HITECH ACT of ARRA.

Nearly half (44%) of organizations do not see value in, or do not require alignment with, the ISO international IT security standard.

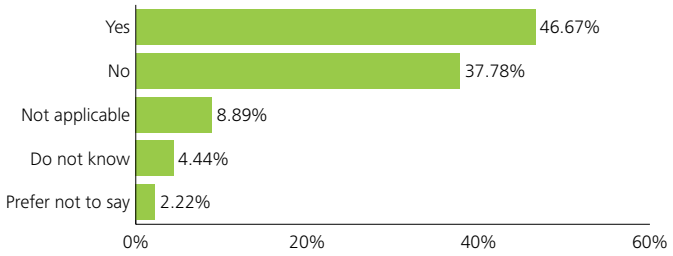
With regard to policy review for compliance with relevant laws and regulations, 77% have reviewed their policies to ensure compliance within the past year and 19% have reviewed their policies a year ago or more.

The majority of respondents feel that regulatory security requirements improve their security posture against data breaches, which demonstrates a solid alignment between regulatory security compliance requirements and the requirements that would be considered if regulatory mandates were not in place.

As expected, 31% of organizations surveyed state that HIPAA will continue to be a driver over the next two years; 43% of respondents report dealing with this compliance standard. However, many organizations appear unclear as to coming regulatory challenges after HIPAA, e.g., ARRA and strengthened HIPAA security and privacy rules; 22% state that they do not know. SOX is also at the forefront of regulatory initiatives, with 16% reporting that they are still managing SOX compliance requirements.

Health care regulatory compliance spending will increase, as indicated by 64% of respondents. The trend to draw from this is that, while budgets may shrink and the global economic situation may continue to decline, spending on regulatory compliance will remain a high priority.

**Figure 3 (HC Providers) – Presence of a strategy/process/methodology to sustain compliance**




### Alignment with industry security standards

Only 34% of organizations have had their security policies reviewed for alignment with industry security standards. In addition, nearly 50% of them have never had their policies reviewed for alignment with industry standards.

### Payment Card Industry Data Security Standard (PCI DSS) compliance

While 15% of respondents are currently compliant with PCI DSS, nearly 22% of respondents do not think they need to comply. Another 43% say they need to be in compliance presently but are not, or they do not need to be presently but will need to be in the future.

The varying responses are likely attributable to the types of health care organizations involved in the study, i.e., those that are more customer facing may need to process credit card transactions, while those less customer facing likely comprise the 22% category.

However, there is a very real issue in that some providers may not know that they are processing credit card transactions in clinics or departments within their organizations which may well fall within the criteria for PCI DSS compliance. As evidence, 17% state that they do not know if their organizations need to comply with PCI DSS. But there is an added benefit of compliance—nearly 32% feel that their approach to complying with PCI DSS contributes to a broader understanding and application of information security concepts, which has an effect on information security management within the organization.

### Executive support

With regard to senior executive support of security projects to address regulatory and legal requirements, only 31% of organizations say that they are receiving adequate funding and support for projects, while 44% indicate that they are receiving support but inadequate funding; only 2% say that there is neither commitment nor funding.

### EHR

Of organizations surveyed, 71% state that they share EHR with their business partners, a practice which necessitates common security management around the transfer, storage and data duration management (e.g., destruction after a specified number of years, encryption of files for transfer, etc.). As many organizations have discovered the hard way, the network is only as strong as its weakest link.

**Figure 4 (HC Providers) – PCI DSS Compliant**

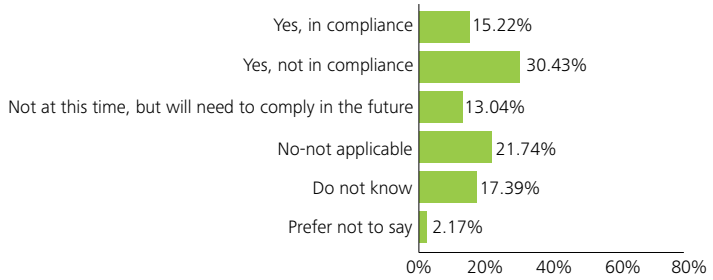
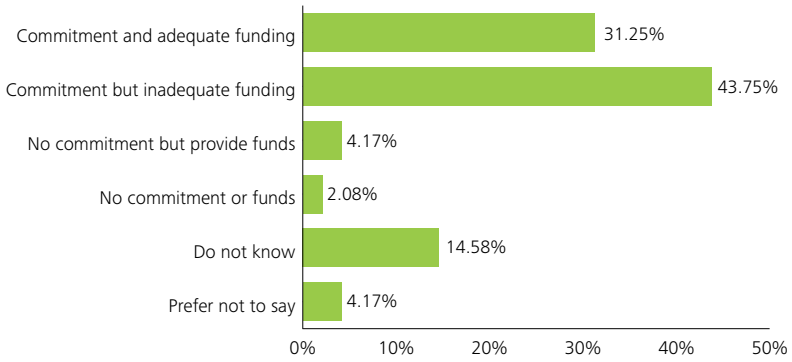



**Figure 5 (HC Providers) – Senior executive support for projects that address regulatory or legal requirements**



# The information security function and the role of the CISO

### The existence of a CISO within the organization

Health care providers are clearly seeing the need for more mature security functions—71% of those surveyed have a CISO role within their organization.

In terms of organizational structure, the reporting relationships for the CISO or equivalent position vary. The most common reporting relationship is a direct report to the CIO. Security functions within the scope of a CISO are found to be weighted heavily towards the "soft" side of security (planning, governance, administration, architecture and ITRM), which is to be expected from a position at the C-suite level.

Network infrastructure components are the most common IT assets protected under the CISO's responsibility, with network hosts (laptops and desktops) trailing closely behind.

Most organizations do not manage security at a comprehensive, organization-wide level and allow information security to be managed separately from physical security. This approach could result in security gaps where there is a need for both types of security to be considered.

**Figure 6 (HC Providers) – Existence of a CISO within the organization**

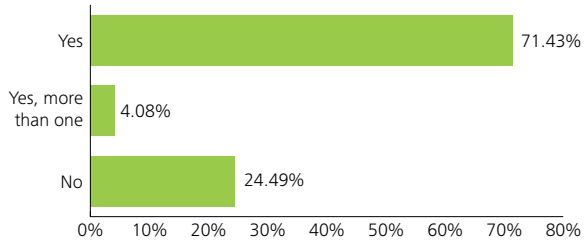
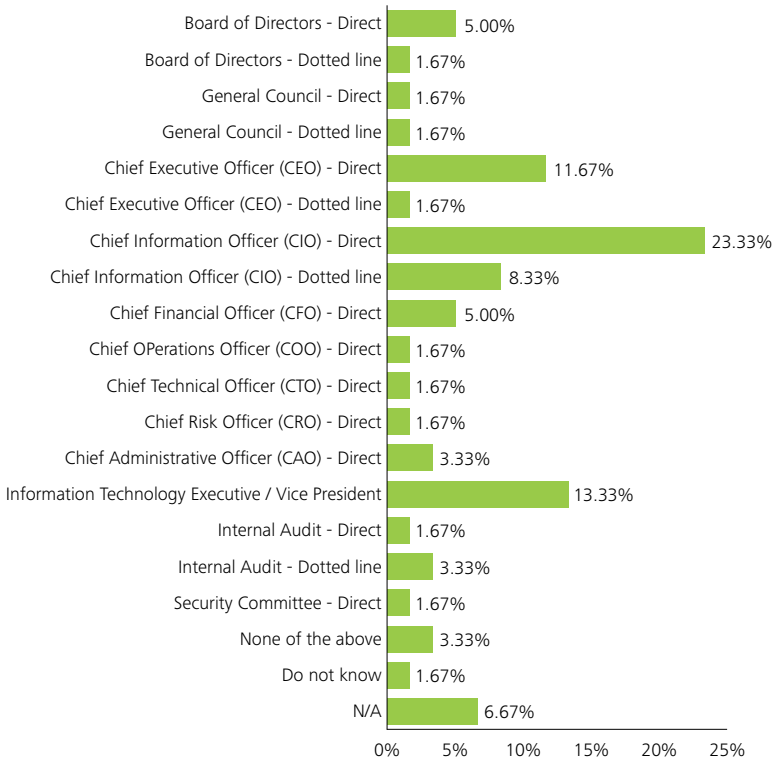



**Figure 7 (HC Providers) – Reporting relationship of the CISO**



### Convergence

More than half of organizations surveyed (59%) have not performed any activities to converge their information and physical security functions. Only 10% have fully converged the two security functions, but 20% have either kept the functions separate but have them report into one common executive, or have kept the functions separate but have started collaborating more to facilitate knowledge enablement and information. Finally, 8% are intending to converge in the next 12-24 months.

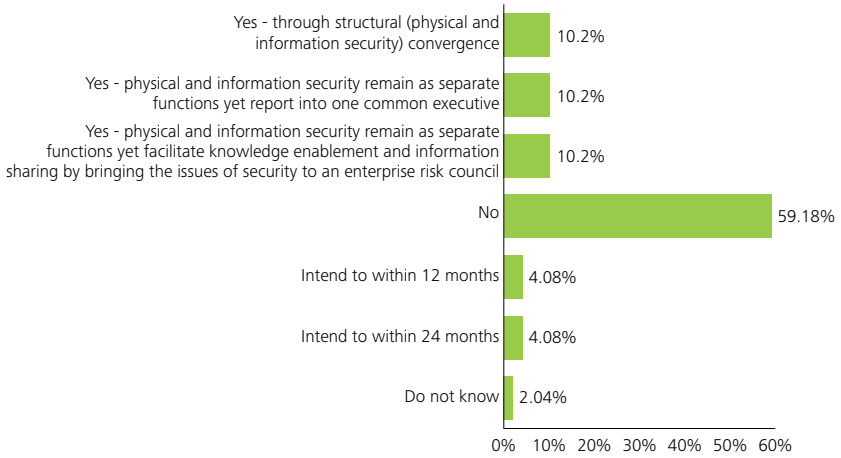
One of the issues that may be a factor in the high percentage of respondents who have done nothing to converge is that most people typically view convergence as an all or nothing proposition—and a massively expensive and complex undertaking—rather than a series of small steps, such as the establishment of risk councils, etc. For example, of the 59% of respondents who state they have done nothing to converge, it is possible that many did not consider the steps they have taken that are actually a move towards convergence, such as reporting into one common executive and facilitating knowledge enablement and information-sharing through risk councils.

### Security professionals

More than 85% of organizations surveyed employ between 1 and 50 full time information security professionals. Additionally, nearly 46% of respondents employ 1 to 50 other employees who perform a liaison role between their core job and information security.

Information security hiring is ongoing but 55% of organizations are choosing to work with their current pool or resources. Only 4% of those surveyed indicate that they have had to reduce their information security headcount in the past 12 months.

**Figure 8 (HC Providers) – Convergence of information security and physical security**




…most people typically view convergence as an all or nothing proposition—and a massively expensive and complex undertaking—rather than a series of small steps…

### Information security and expectations

A large number of organizations (39%) feel that they are missing competencies but they are closing the gap well enough to meet expectations. Only 27% feel that they have all the required competencies and are able to response effectively and efficiently to security needs. However, this number may always be in the minority by virtue of the fact that any organization that experiences a security breach could therefore be perceived as not having the competencies to respond effectively and efficiently before the fact.

### Information security strategy

An organization that is proactive about security and privacy typically demonstrates this through the development of a strategy and establishment of a framework with defined responsibilities, and polices and procedures. Of organizations surveyed, 65% have either a formally documented or a drafted information security strategy. Another 20% are intending to have one in the next 12 months.

A large number of organizations reveal that their information security strategies are focused on high-level tasks, such as defining the security hierarchy, defining roles, conveying awareness and discussing information security requirements.

**Figure 9 (HC Providers) – Level of competencies to handle present and future requirements**

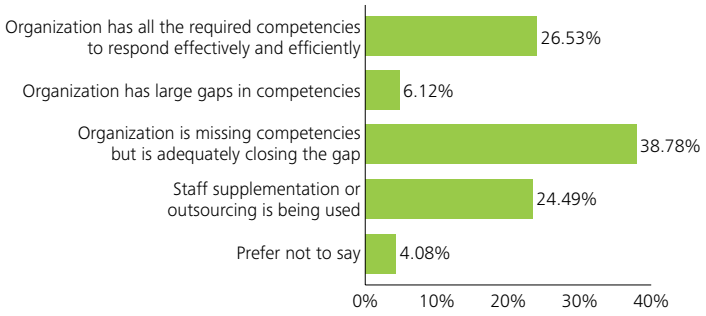
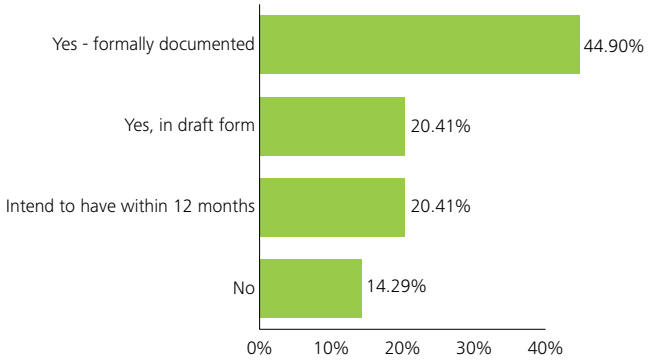



**Figure 10 (HC Providers) – Presence of a defined information security strategy**



## Support for the security strategy

The existence of a security strategy is one thing; support for and recognition of it is quite another. Less than 25% of respondents feel that their business lines embrace the security strategy. This could be due to a lack of communication and training around the strategy, a perceived lack of value in the strategy or an overly complex presentation of the strategy.

The good news is that over 50% of functional executives provide input to the security strategy and over 40% are involved in approving the strategy. This data conveys a heavy involvement from executives, a factor that is likely to foster synergy between information security and the core business being supported by the strategy.

## Measuring ROI in security

Of organizations surveyed, only 4% have established formal metrics to measure return on information security program investments and 21% are working on establishing formal metrics. The rest (70%) either do not measure at all or perform only minimal measurement.

## Top five security initiatives

Most organizations rate security regulatory compliance initiatives as their primary concern, followed by data leakage protection tied for second place with identity and access management. Reporting and measurement and employee misconduct are the fourth and fifth initiatives, respectively.

Identity and access management in the number two spot is indicative of the ongoing struggle of organizations to provide ready access to information while fulfilling their requirements to protect information as well.

The presence of data leakage protection, also in the number two spot, is likely fuelled by media reports of high-profile data leakage-related breaches over the past two years and the resulting law suits. At only 8%, cyber terrorism is seen as a minimal threat by respondents

**Figure 11 (HC Providers) – Level of involvement of executives in information security strategy**

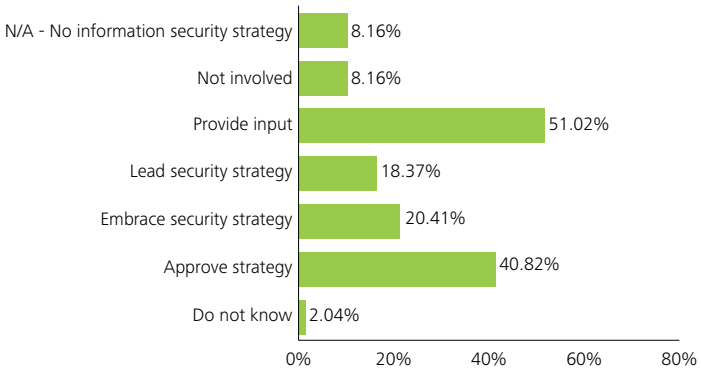
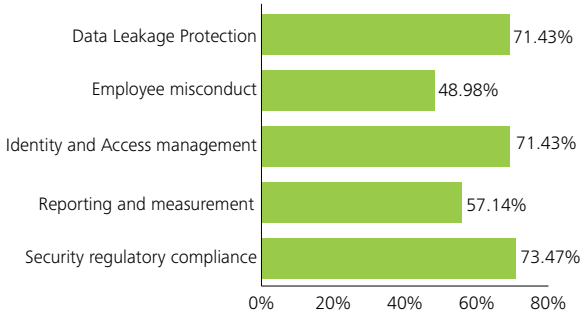



**Figure 12 (HC Providers) – Top security initiatives: organizational, operational, threat-based**



but it is a topic to watch, given that it is a "hot button" for U.S. President Obama's new administration and has been analyzed and reported to the President in "Securing Cyberspace for the 44th Presidency" by CSIS.*

** Broadband DSL Reports.com; "Securing Cyberspace for the 44th Presidency" by CSIS; retrieved from http://www4.broadbandreports.com/forum/r21602044-CSIS-report-Securing-Cyberspace-for-the-44th-Presidency on April 8, 2009.*

### Barriers to implementing IT security

The majority (60%) of respondents in this sector indicate that budget constraints and/or lack of resources is one of the top barriers for organizations in ensuring information security. Given the current economic conditions, budget constraints are expected to weigh heavily on the minds of IT security management. Emerging technologies are cited as the second greatest barrier.

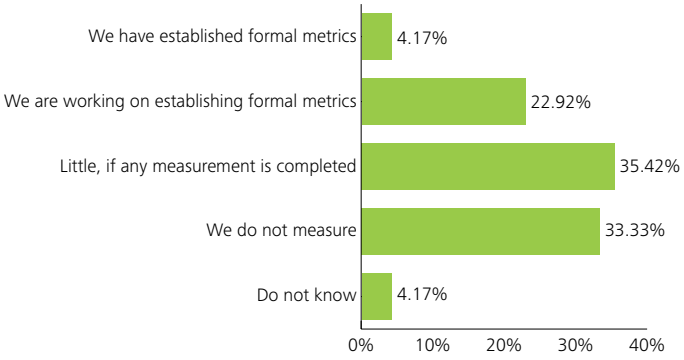
### Measuring the success or failure of IT security projects

Only 4% of organizations state that they have established formal metrics, with a full 35% reporting that little if any measurement is completed. This finding would appear to demonstrate that organizations struggle with defining and capturing measurable results with regard to ROI for their efforts towards information security programs. Almost the same number again (35%) appear not to measure at all.

Almost 30% of organizations produce ad-hoc reports as needed, while only a combined 29% produce reports for review on a monthly, quarterly or annual basis.

**Figure 13 (HC Providers) – Barriers to implementing IT security**


**Figure 14 (HC Providers) – Measuring success or failure of IT security projects**



## Reasons projects fail

The major causes for failure of information security projects identified by respondents are (in descending order):

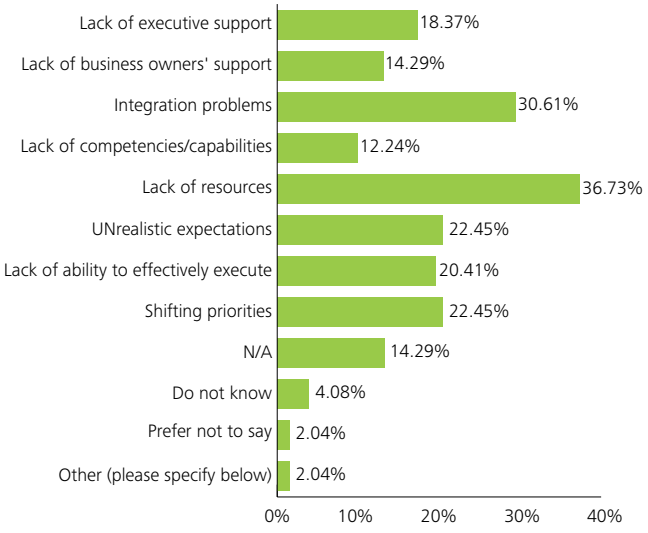
- Lack of resources
- Integration problems
- Shifting priorities (tied with)
- Unrealistic expectations

However, based on the earlier finding that only 4% of organizations are formally measuring why IT projects fail, it would seem that all of the major causes are not fully understood. Based on Deloitte member firm experience, some other reasons include lack of adequately trained resources; lack of a formal software development life cycle (SDLC) methodology and lack of discipline in following the SDLC methodology.

## Commitment from senior executives

Only about 6% of organizations feel that they receive "little to no commitment" from senior executives in their support of regulatory security projects. This means that the majority of senior-level management is aware of the requirements and consequences of not complying with regulatory requirements and they actively support the need to allocate funding and resources in an effort to remain or attain compliance.

**Figure 15 (HC Providers) – Causes of failure of information security projects**




## Internal/external audit findings

Respondents indicate that the top five internal/external audit findings (in descending order) are:

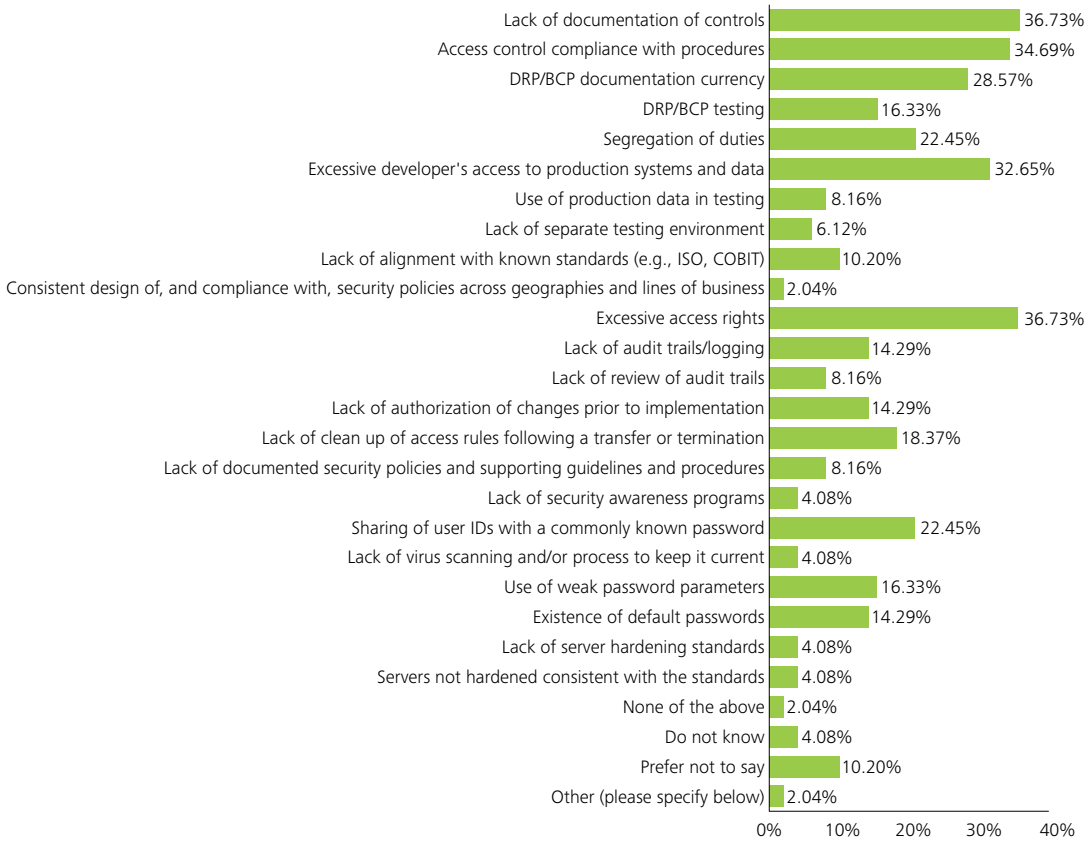
1 & 2) Excessive access rights tied with lack of documentation of controls

3) Access control compliance with procedures

4) Excessive developer's access to production systems and data

5) DRP/BCP documentation/currency.

**Figure 16 (HC Providers) – Top five internal/external audit findings**



## Budgets and funding to address regulatory requirements and IT security projects

Of the organizations surveyed, 47% say that security projects are adequately funded to effectively address regulatory requirements; 41% say that projects are not adequately funded.

Only 21% of organizations surveyed have a separate budget for IT security projects and 79% have merged security projects in with the main IT budget.

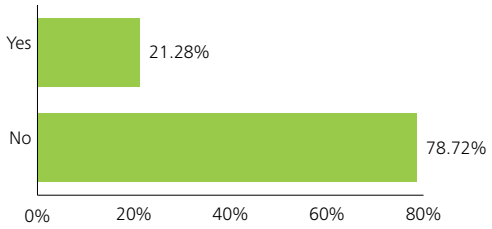
For those who have merged IT and security budgets, 33% state that IT security accounts for 1-3%, 19% say security accounts for 4-6%, 17% say that security accounts for greater than 7% and the remaining 31% don't know what percentage IT security is of their IT budget.

More than half of respondents have a portion of their information security budget focused on hardware and infrastructure, desktop and gateway anti-virus, infrastructure protection devices/products, logical access control products, and security consultants. Based on these spending priorities, it is evident that protecting the organization's information assets is a top driver around security spending.

Although 75% of respondents are devoting only 1 to 6% of their company's IT operating budget to IT security, there is a definite trend towards spending more on IT security. Almost 25% of respondents are either devoting 10-11% or greater than 11% of their overall IT budget to security.

Furthermore, almost 25% of respondents have increased their security spending by either 6%-15% or by greater than 15% from year to year. The majority (58%) increased their security spending by 1%-5% from year to year.

**Figure 17 (HC Providers) – Information security budget as part of IT budget**



The areas most frequently covered under information security budgets are (in descending order):

- Hardware and infrastructure
- Desktop and gateway anti-virus, etc.
- Infrastructure protection devices/products
- Logical access control products
- Security consultants

The sources for information security funding (in descending order) are:

- IT Function
- Project Sponsors
- Compliance/Regulatory Function
- Lines of Business

### Information security as a key imperative

In nearly half of organizations, information security is considered a key imperative at the executive and middle management levels. Security is more likely to have the attention of executives who understand the impact of security incidents on the business.

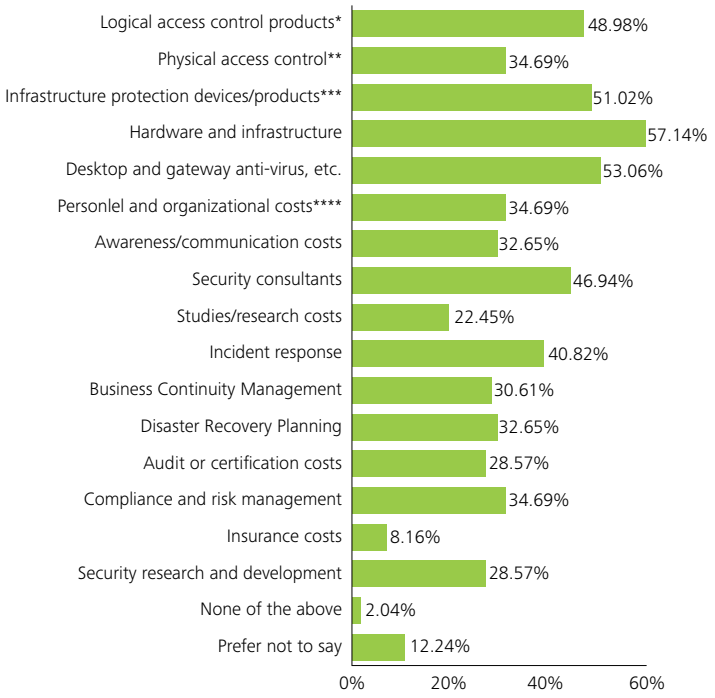
### Information security and expectations

A majority of organizations (64%) indicate that their information security functions are only "somewhat effective" in meeting organizational goals and expectations. This finding illustrates the need for increased business focus for the information security function to address the issues and challenges faced by the organization.

### Alignment of information security and business initiatives

The majority of organizations (68%) do not have their information security and business initiatives aligned. Only one quarter of organizations surveyed consider that they are aligned.

**Figure 18 (HC Providers) – Expenditures covered under the information security budget**



# Risk

### Application development directives

About one third of respondents indicate that they do not have well defined development directives for secure application development but maintain that those in place are practical. About one quarter of respondents state that they are "under development". Based on these responses, it appears that well defined development directives are not widely adopted.

Only about one half of organizations incorporate application security and privacy as part of their SDLC depending on the project. Therefore, security and privacy are not consistently considered for all projects. In addition, the number of organizations that include security and privacy in their SDLC as an afterthought is roughly equivalent to the number of organizations that do not incorporate them at all.

### Outsourcing and third-party relationships

Respondents cite "managing third-party information sharing" as one of their organization's top five privacy concerns. A full 81% of organizations provide access to authorized third parties. There is a general trend towards outsourcing to third parties, either as a cost-saving measure or because a specialized skill set is not available in house.

One of the primary challenges organizations face with regard to outsourcers and third parties is the process of ensuring that the outsourcer is compliant with the organization's information security policies. This is more of an issue in the current environment with the enhanced HIPAA security and privacy rules under ARRA, which includes "business associates" as part of an organization's people.

While 47% of organizations conduct an independent review to evaluate their security policy, 34% do not. While virtually all organizations (85%) include a data protection clause in their contract with third parties, a startlingly high 15% state that their third-party's security capabilities and controls are unknown.

**Figure 19 (HC Providers) – Application development directives**

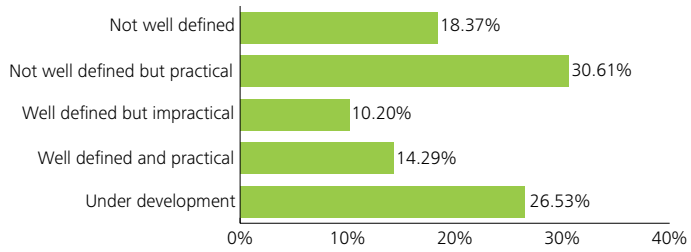
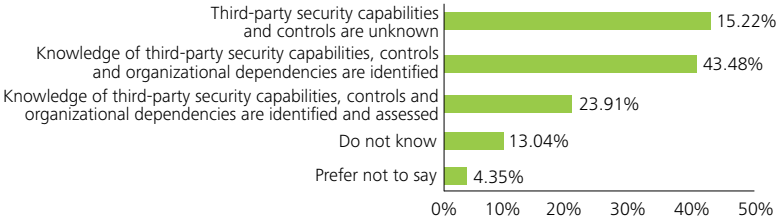



**Figure 20a (HC Providers) – Knowledge of third party security capabilities and controls**



The two most common ways of ensuring the security activities of vendors and third parties are by addressing them in a contract (61%) or by controlling the access that the vendor or third party has to systems and data (59%).

Most organizations (65%) rely on a "right to audit" clause in the contract as a basis to establish reliance on third-party data protection efforts. Some organizations (19%) rely on SAS 70 Type II and organizations are beginning to take a serious look at technologies such as SysTrust. Overall, there is a high degree of trust in the claims made by third parties regarding their security postures.

While most organizations (73%) have a segregation of duties process, many do not review roles for segregation of duties conflicts on a periodic basis. Therefore, segregation of duties conflicts are likely to occur as employees change roles and access is not checked or reviewed.

The majority of organizations (55%) do not have an ability to systematically enforce segregation of duties or roles. So while most organizations have a process to ensure segregation of duties or roles, many lack the ability to enforce them systematically or detect conflicts.

Only 38% of organizations terminate access within one day after it is no longer required and 27% of organizations take more than two weeks. This time lag provides a window of opportunity for misconduct by employees.

The other issue regarding third-party relationships is the vested interest on the part of the third party not to bite the hand that feeds it—most suppliers are very aware that their relationship with the organization they contract with depends upon their impeccable conduct. However, since most breaches are due to inadvertent and careless behaviour, third parties are subject to the same internal people issues as the host organization.

## Internal/external security threats

Like one's family, an organization's people are the source of its greatest pride and its greatest worry. Among respondents, there is a greater level of concern regarding internal people (50%) than external people (15%)

Of respondents, 57% are "somewhat confident" and only 16% are either "very confident" or "extremely confident" that information assets are protected from internal attacks. A Ponemon Institute study found that 60 percent of dismissed employees admitted to stealing confidential information from their employees.*

**Figure 20b (HC Providers) – Ensuring adequacy of vendor security activities once they are engaged**

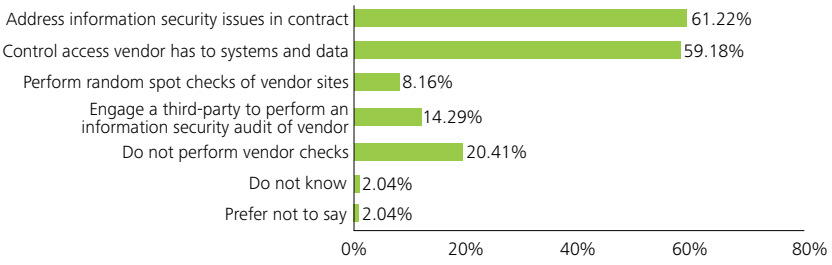
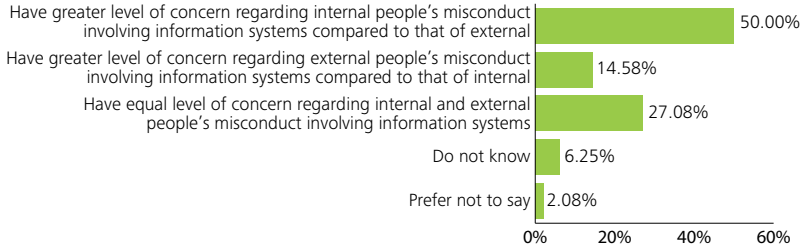



**Figure 21 (HC Providers) – Level of concern about internal versus external people**




**CIO.com "Laid off Workers as Data Thieves?" by Bill Brenner, February 24, 2009; retrieved from http://www.cio.com/article/482413/Laid_Off_Workers_As_Data_Thieves on April 8, 2009*

For external attacks, 31% are "somewhat confident" but the majority (57%) are either "very confident" or "extremely confident" that information assets are protected. This may indicate too high a priority being given to security measures to protect against external threats when the majority of security incidents come from internal sources.

While about one half of organizations rate viruses/worms, e-mail attacks, adware, spyware, website defacement, phishing and wireless network breaches as "average threat" or "somewhat low threat", an equal number of organizations rate cyber terrorism and online extortion as "no threat" or "low threat". Overall, spyware, DoS attacks, loss of customer data/privacy issues and inappropriate use of sensitive data are rated the highest threats.

Medical identity theft, using an individual's personal information without their knowledge to collect money, prescription drugs, medical goods or health services, is a major threat to providers. It can be financially damaging and can also be dangerous from a health perspective. It is believed to be on the rise, which prompted the U.S. state of California to update its California Security Breach Notification Act (SB 1386) in 2008 to include health information. New phishing schemes and worms, such as Koobface, are being planted on users' desktop computers via social networking technologies.

### Impact of threats

More so than the other two sectors, health care provider respondents have experienced greater monetary loss due to breaches, with 47% indicating losses greater than $US1 million. However, 26% have not experienced a financial loss.

### Root causes of failure

Human error was cited overwhelmingly (92%) as the root cause for failures of information systems. At 65%—not even a close second—is technology followed by lack of documented processes at 45%.

Respondents indicate that identity and access management is a top operational initiative, and there is a strong indication that it will remain a priority for the foreseeable future.

**Figure 22 (HC Providers) – Total damage as a result of breaches**

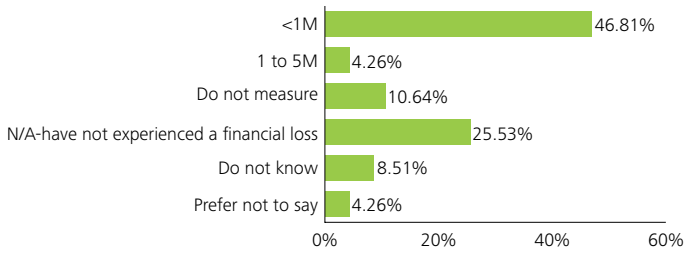
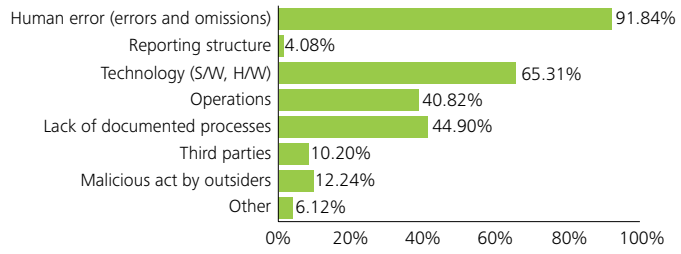



**Figure 23 (HC providers) – Top three root causes of failure**



The problem with falling budgets for security and privacy is that the bad guys never seem to be affected by cost-cutting—the parade of creative breach ideas continues and grows, with each one more sophisticated than the previous. Data leakage protection is the technology indicated by the highest percentage of respondents when asked which technologies they plan to deploy or pilot over the next 12 months.

### Frequency of external breaches

Virus/worm attacks (21%) lead the list of external security breaches most experienced by organizations in the last 12 months. This is followed by accidental instances (18%) and website defacement (16%).

Other significant breaches indicated by respondents include:

- Wireless network breach (12.2%)
- Theft or leakage of intellectual property (12.2%)
- Employee misconduct (12.2%)
- Malicious remote access (10.2%)
- Phishing/Pharming (10.2%).

The breaches that reoccur most frequently are (in descending order):

- Email attacks (e.g., spam, etc.)
- Employee misconduct
- Virus/Worm outbreaks
- Spyware

A sobering 48% of organizations surveyed indicate their breaches to be related to consumer data; 20% indicate the breach was related to personnel data and the other 30% or so do not know or did not disclose this information.

### Frequency of internal breaches

Study respondents indicate that the following internal breaches (ranked in descending order of number of reported incidents) occurred in the past 12 months:

- Loss of customer data/privacy issues (information leakage)
- Accidental data loss
- Wireless Network Breach
- Virus/worm outbreak
- Internal financial fraud involving information systems.

Virus/worm outbreaks are the most frequently recurring internal incident followed by loss of customer data/privacy issues (information leakage), accidental data loss and theft of intellectual property.

When it comes to breaches of consumer data, 48% of organizations experienced such a breach compared to breaches of personal data (20%).

### Management of security incidents

A majority of organizations (55%) have all servers in scope for log and incident management. This number compares to 39% for network components and 31% for mainframe systems. Supervisory control systems and compliance and regulated systems are least likely to be in the scope of log and incident management. While a majority of companies have centralized log management of dashboards (63%), log and incident monitoring at most companies is ad hoc (47%) or via paging and email alerting (43%). As a result, while many companies have invested in log and incident management capabilities, they do not have commensurate organizational capabilities to match. There is a tendency to incorporate security functions with the Network Operations Center (NOC).

Another 38% do not know if they tracked this metric at all. Only 38% of organizations surveyed have a central log management solution and less than 10% have a log forensics tool.

### Security incident reporting

Over one half of organizations (53%) conduct vulnerability scanning either quarterly or annually while more than one third of organizations do so on an ad hoc basis (39%). Penetration testing and application code reviews are conducted less frequently than vulnerability scanning—40% to 50% of organizations do so on an ad hoc basis.

A full 19% of organizations never provide a regular report on information security status or security incidents; 23% provide this report on an ad hoc basis; 15% provide it annually; 6% provide it semi-annually and 15% provide it quarterly.

# Use of Security Technology

## Deployment of technologies

In terms of adopting new technologies, 16% of the organizations surveyed are "early adopters", 30% are "early majority" (e.g., may experiment on ad hoc basis), 47% are "late majority" (e.g., users of proven and effective technologies), and 6% are "laggards".

Most organizations (61%) implement and encourage the use of secured technologies for wireless LAN capabilities and have policies on acceptable business use for storage devices (49%) and mobile devices (41%). The majority of organizations prohibit the use of social networking (49%) and instant messaging technologies (35%), demonstrating that they have weighed the risk versus the business productivity gain for these technologies.

Overall, security technologies including firewalls (96%), antivirus (94%), Virtual Private Networks (88%) and spam filtering solutions (88%) make up the top technologies that respondents indicate are fully adopted by their organizations.

Among the top technologies being piloted by organizations are:

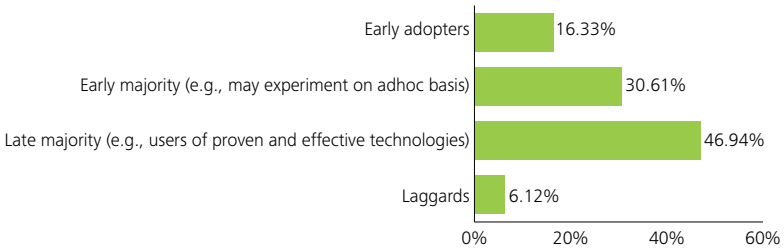
- Radio Frequency Identification tags (RFID) (24.5%),
- Encryption (22.4%)
- Security compliance tools (20.4%)
- Intrusion Prevention Systems (IPS) (20.4%)
- Voice Over IP (VoIP) (20.4%)

Those technologies that are to be fully deployed or piloted within the next 12 months are:

- Vulnerability management systems (26.5%)
- Smart cards (26.5%)
- Active Network assessment tools (scan run on an ad hoc basis) (22.4%).

The rate of adoption of newer security technologies, such as federated access, fraud detection and biometrics is lower than traditional security technologies but some of them appear to be gaining traction.

**Figure 24 (HC Providers) – Level of adoption of security technologies**




There is clearly a continued reliance on password-based mechanisms for authentication on the web; 47% of organizations use password-based authentication for end user transactions over the internet. But there is progress being made—35% of organizations have moved beyond password-based authentication for either some or all of their end user transactions.

In summary, recurrences of a breach out-pace the plans to roll out countermeasures. Organizations report a fair number of repeat incidents while a smaller percentage has fully deployed countermeasures or has a plan to deploy them.

# Quality of operations

### Training

Most organizations report having a greater level of concern about internal people's conduct involving information systems than they do about the conduct of external people. About a quarter of organizations have equal concern for both, which may indicate a lack of appropriate level of security measures for insider threats relative to the risk.

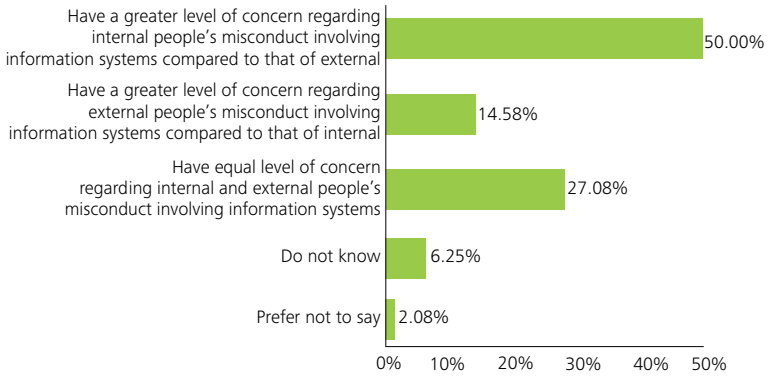
A full 69% of organizations train employees on identifying and reporting suspicious activities; a quarter of them do not.

The majority of respondents indicate that their employees have received at least one training or awareness session on information security and privacy issues and statutory compliance in the past 12 months.

Customized training by job role and function is most likely to be offered on an ad hoc basis or not offered at all for all job roles. Executives and contractors are least likely to receive such training. The results indicate a "one size fits all" or ad hoc approach to security training.

Very few companies (12%) have offered their online customers awareness programs on information security and privacy issues in the past 12 months. Some have done so for only a segment of customers (10%).

**Figure 29 (HC Provider) – Level of concern of internal versus external people**




Some health care providers may not know that they are processing credit card transactions in clinics or departments within their organizations which may well fall within the criteria for PCI DSS compliance.

# Privacy program

### Existence of a Chief Privacy Officer

Most organizations have a Chief Privacy Officer or equivalent. Of the organizations that do, for only 6% is the role handled by the CSO/CISO. The need for a dedicated role for privacy officer that is separate from security is increasing as privacy evolves as a function.

### Reporting relationship

The reporting structure for the privacy executive seems to range from the CEO to CAO. However, most privacy executives report to C-suite executives, demonstrating the increasing importance of this role and its visibility at the top of organizations.

### Responsibilities of the privacy executive

Developing privacy strategy (71%), reporting to management (71%) and analyzing regulations (67%) are the top three responsibilities of the privacy executive. These are followed closely by conducting training and communications (includes development) (63%); enforcing policies (includes development and implementation) (61%); and consulting to the organization (61%). The primary driver for privacy within organizations appears to be regulatory compliance.

Most organizations have a centralized privacy model that scales effectively. Others have either a decentralized or federated model.

### Stage of development of the privacy function

Of the organizations that have a privacy program, 31% are at a "late stage", that is, starting to evaluate the effectiveness of key initiatives, and 29% of organizations are in a "mature stage". Privacy programs have matured with increased attention from senior executives. Only a few organizations have privacy programs in early stages.

While most organizations claim to have privacy programs that are in either late or mature stages, only 33% of them have performed an inventory of personal information (e.g., a data flow analysis of personal information collection, usage, storage, sharing and destruction practices) and 18% have it in progress. There is a gap between having a program and policies in place and measuring their implementation and effectiveness.

**Figure 25 (HC Providers) – Existence of a Chief Privacy Officer**

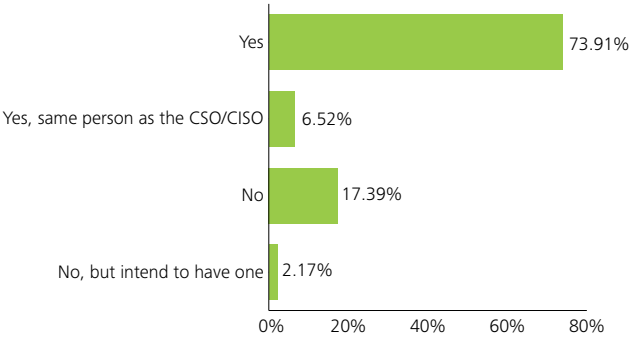
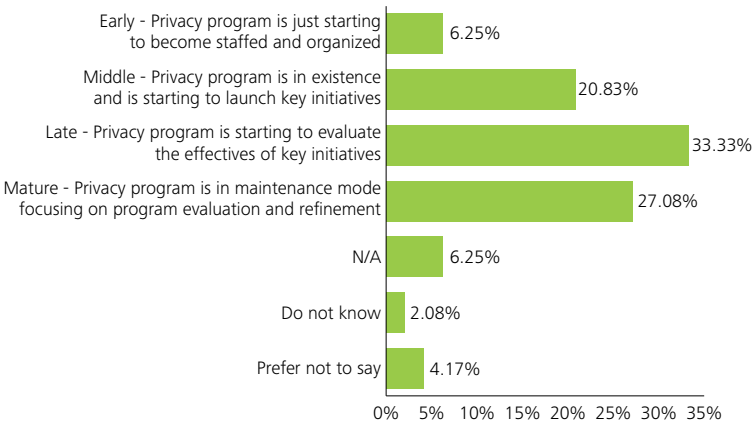



**Figure 26 (HC Providers) – Stage of development of the privacy function**



## Privacy drivers

Respondents indicate that the greatest driver of privacy initiatives is regulation, followed by reputation and brand. Legal liability is a close third place.

## Privacy concerns

Unauthorized access to personal information (88%), managing customer privacy preferences (53%) and aligning operational practices with policies (49%) are the top three privacy concerns for organizations.

Most organizations have a privacy program, a written privacy, fair information practices or data collection policy, formal policies in place with respect to the destruction of personal information and a formal process in place to deal with complaints about its personal information management practices or policies.

Only 21% of organizations have concerns about conflicts between security regulations and privacy regulations. Most organizations either do not have such concerns or are not aware of any conflicts.

## Business Continuity Planning

More so than in any other sector, organizations (35%) have business continuity plans in place to recover mission-critical processes. About the same percentage have business continuity plans in place for a limited number of departments but they are not a requirement. Business continuity plans are required and guidelines for implementation are distributed throughout the organization for only 16% of organizations surveyed. There is no clear trend across organizations.

The top three key drivers behind the establishment of business continuity planning are the need to ensure operational resiliency and availability (57%), executive/ senior management's accountability for risk management (45%) and regulatory compliance (35%)

The majority of organizations do not have active and consistent executive involvement in setting and driving business continuity planning in its annual review. Senior management involvement at most organizations is limited to simply being aware of the importance of business continuity planning or approving the programs.

**Figure 28 (HC Providers) – Top three privacy concerns**

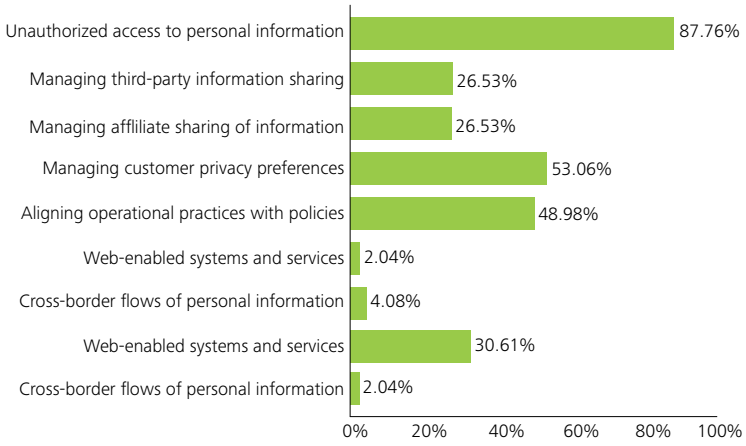
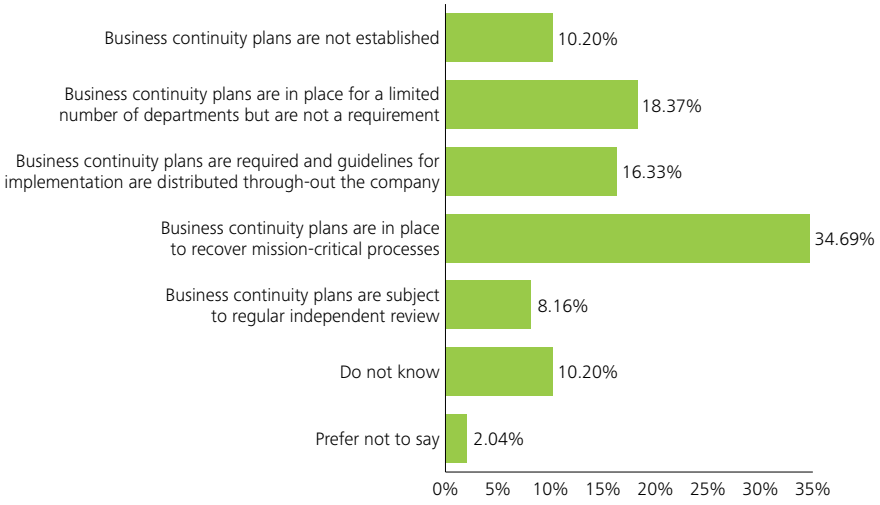



**Figure 27 (HC Providers) – State of business continuity planning**




Only 10% of organizations perform regular testing for all business continuity components or have independent facilitation of regular testing of all business continuity components. About 75% of organizations have no testing conducted or the testing is either intermittent or for limited components. So, while most companies have some degree of planning in place, most do not test their plans on a regular basis.

# Study findings and discussion - Health Care Payers

## Governance

### Framework

More respondents in the health care payers sector (57%) state that their organizations have an information security governance framework being executed than in life sciences or health care providers sectors.

Governance and regulatory compliance is a primary focus for organizations in this sector. The majority of respondents have a strategy/process/methodology to sustain compliance (71%). However, there are challenges that keep organizations from effective compliance.

More than half of respondents (57%) feel that senior executives are committed to compliance initiatives but provide inadequate funding to effectively address legal and regulatory requirements.

**Figure 1 (HC Payers) – Presence of an information security governance framework**

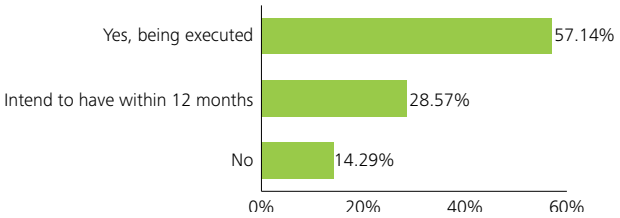
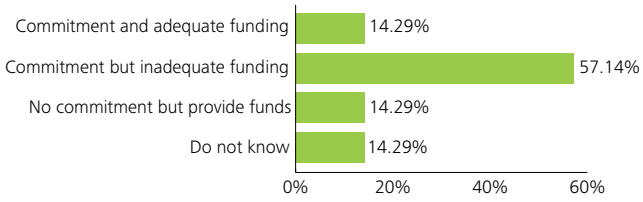



**Figure 2 (HC Payers) – Senior executive support for projects that address regulatory or legal requirements**



# The information security function and the role of the CISO

### Existence and reporting relationship of the CISO

The majority of organizations (57%) do not have a CISO. Of the organizations that have a CISO or equivalent function, 37% report to the CIO and 25% report to the Information Technology Executive/Vice President. The other reports for the CISO are dotted line to the Chief Privacy Officer (12%) and direct to the General Council (12%).

### Convergence

The majority of organizations surveyed (71%) have not converged the information security and physical security functions; it may well be that convergence never becomes necessary in the payer sector. However, the sector is taking small steps towards convergence: 29% of respondents continue to keep the functions separate but have started collaborating more to facilitate knowledge enablement and information.

### Information security strategy

The majority of respondents have an information security strategy that is either formally documented (57%), in draft form (14%) or intend to have one in the next 12 months (14%).

**Figure 3 (HC Payers) – Existence of a CISO within the organization**

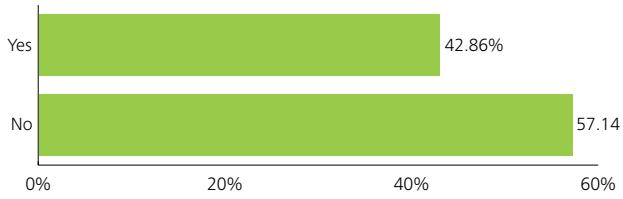



**Figure 4 (HC Payers) – Reporting relationship of the CISO**

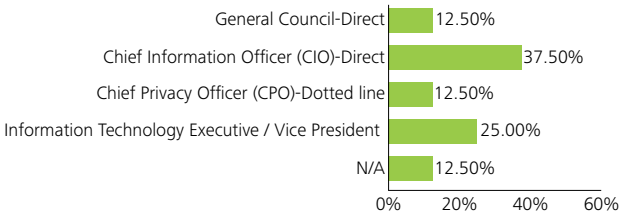



**Figure 5 (HC Payers) – Convergence of information security and physical security**

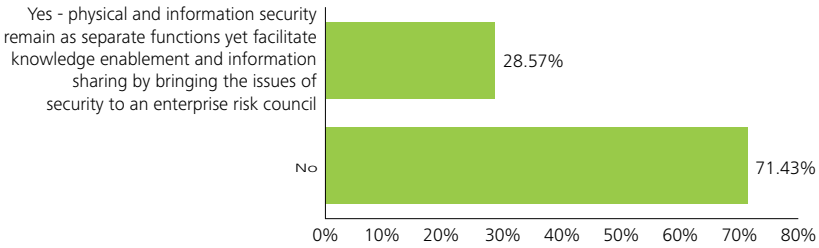
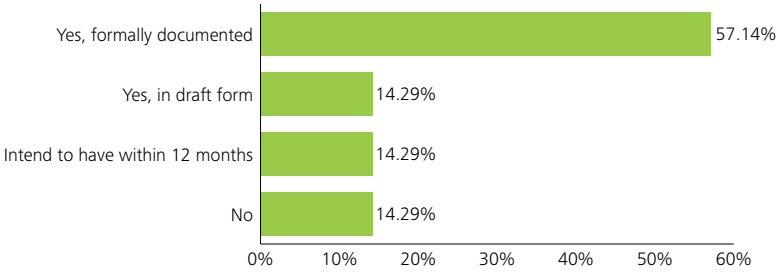


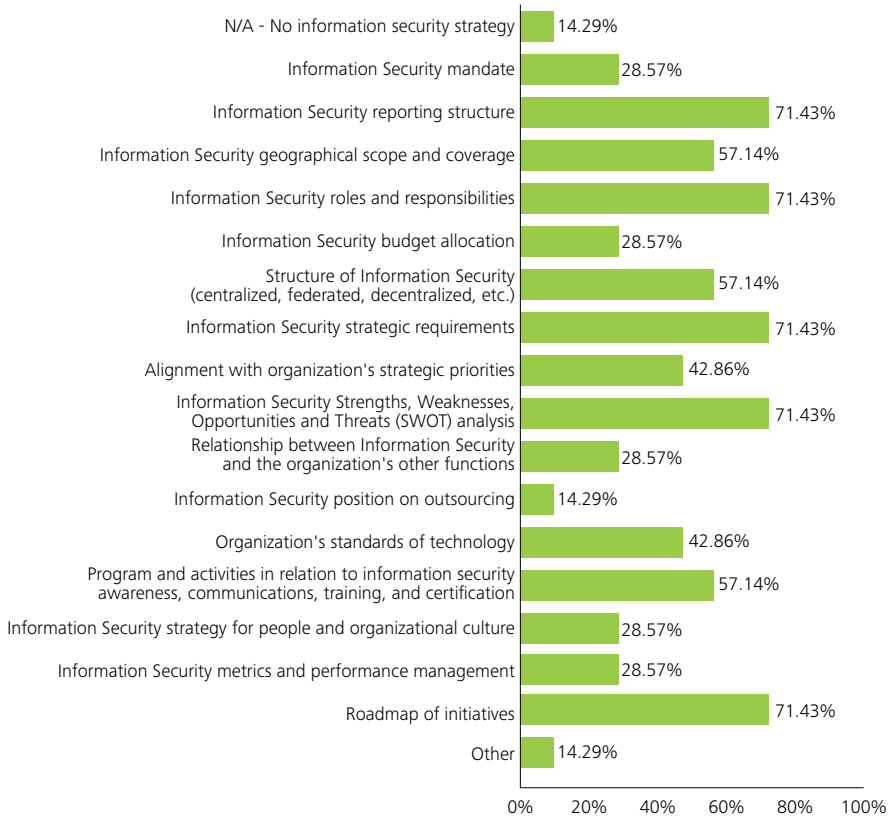

**Figure 6 (HC Payers) – Presence of a defined information security strategy**



The main areas of focus in respondents' security strategies are information security reporting structure, information security roles and responsibilities, information security strategic requirements, roadmap of initiatives and information security SWOT analysis. While these are all important, the areas that are most likely to bring visibility to the function, such as relationship between information security and the organization's other functions; information security strategy for people and organizational culture; and most importantly, alignment with organization's strategic priorities, are all at the low end of the responses.

One of the key challenges for information security professionals is the alignment of information security initiatives with business initiatives. A majority of respondents state that their information security and business initiatives are not aligned at all.

**Figure 7 (HC Payers) – Topic areas covered by information security strategy**



### Top security initiatives

When asked about their top four security initiatives, 86% of respondents indicate data leakage protection as their top initiative. Governance for security, security regulatory compliance and identity and access management are all tied for second place at 57%.

### Common security framework

Most respondents (71%) adhere to some type of common security framework. However, most of the frameworks do not cover industry standards, compliance regulations, and internal policies and standards.

The majority of respondents believe that a common security framework would be beneficial to the industry.

### Internal/external audit findings

A majority of respondents report segregation of duties as the top internal/external audit finding in the organization in the past 12 months. The four remaining audit findings, in descending order, are: excessive access rights, tied with lack of clean up of access rules following a transfer or termination; and lack of documented security policy and supporting guidelines and procedures tied with excessive developers' access to systems and data.

**Figure 8 (HC Payers): Top security initiatives: organizational, operational, threat-based**

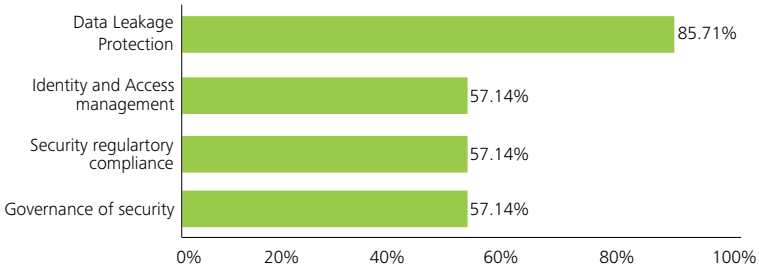



**Figure 9 (HC Payers): Adherence to a commonly accepted security framework**

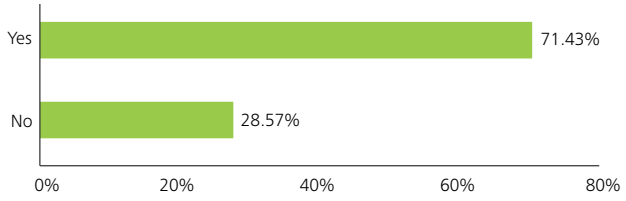
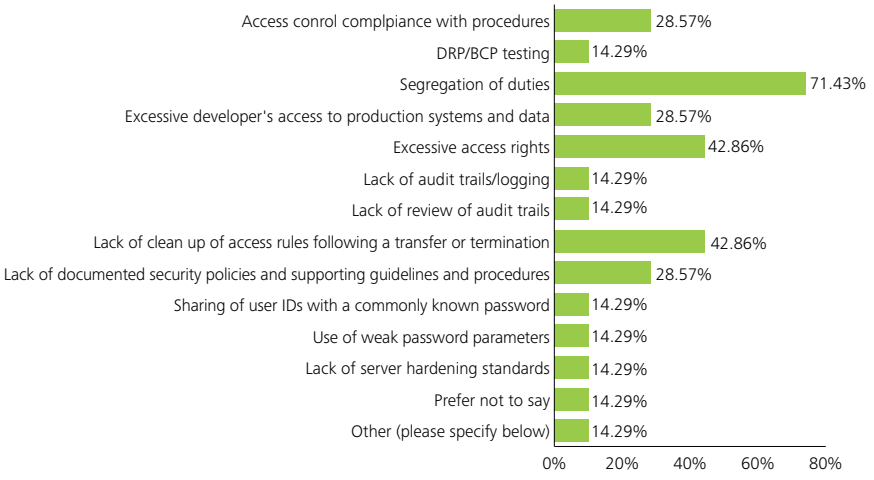



**Figure 10 (HC Payers) – Top five internal/external audit findings**



### Expenditures covered under the security budget

All of the organizations surveyed (86%) have the largest portions of their security budget dedicated to personnel and organizational costs, incident response, and security research and development. Security consultants are the next greatest expenditure.

Respondents indicate that 42% of organizations have increased their security spending by 1%-5% from year to year.

### Barriers to implementing IT security

A full 100% of respondents, by far the most definitive response to any of the questions posed by this study, feel that budget constraints and/or lack of resources is the top barrier for organizations in ensuring information security. Lack of management support was far behind with 43%.

**Figure 11 (HC Payers) – Expenditures covered under the information security budget**

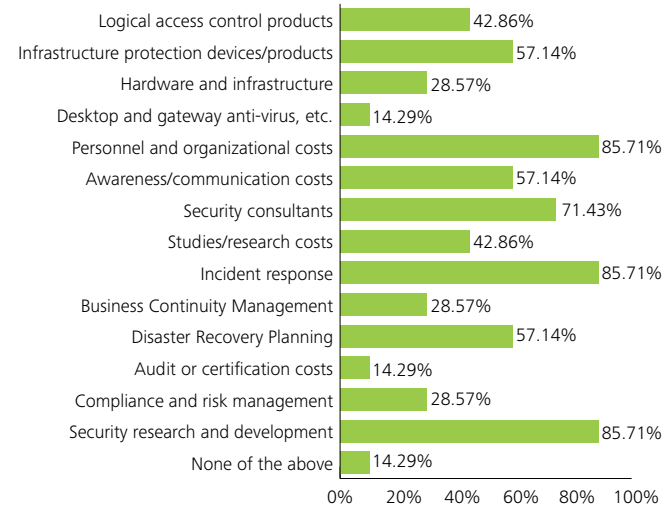
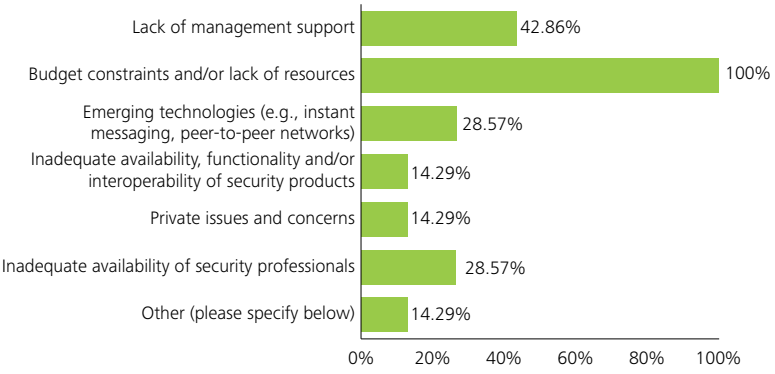



**Figure 12 (HC Payers) – Barriers to implementing IT security**



# Risk

### Outsourcing and third-party relationships

A major challenge organizations face with regard to outsourcers and third parties is the process of ensuring that they are compliant with the organization's information security policies. Only 14% of respondents conduct a regular assessment to ensure compliance.

Another challenge is the process of identifying, assessing, and testing third-party security capabilities, controls and organizational dependencies. Most respondents are knowledgeable of the third party's security capabilities, controls, and organizational dependencies but less than half of respondents go through the process of assessing, reviewing, and testing third party security capabilities on a regular basis.

### Internal/external breaches

Most respondents have experienced both external and internal security breaches in the last 12 months, with external breaches recurring most often. In terms of external breaches, spyware and employee misconduct are the most cited while accidental instances are the most common internal security breach.

In terms of challenges encountered when protecting data, a majority of respondents feel that human error is a primary root cause of failure of information systems in the organization. Some other key challenges include operations, technology, and the lack of documented processes.

For all respondents, the type of data breached was consumer-related data. Most respondents (63%) have not moved beyond password-based authentication for end user (e.g., customer) internet transactions. Only 14% have moved beyond password-based authentication for all end users and another 14% have done so for a group of selected users.

### EHR

One of the challenges in emerging areas such as EHR is that many of organizations share sensitive information with their business partners (86% of respondents). Organizations in this sector need to implement the appropriate safeguards to ensure the privacy and security of health information, especially the information that is shared with business partners.

**Figure 13a (HC Payers) – Status of assessment of IT outsourcer's compliance with organization's information security policies**

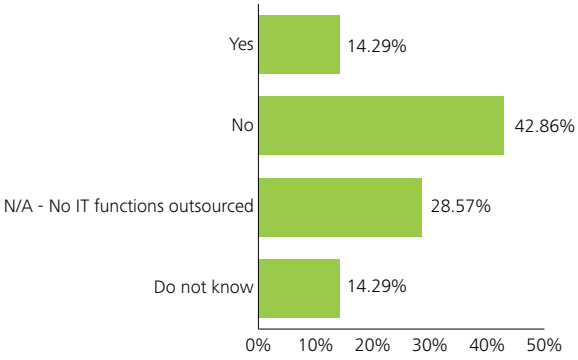
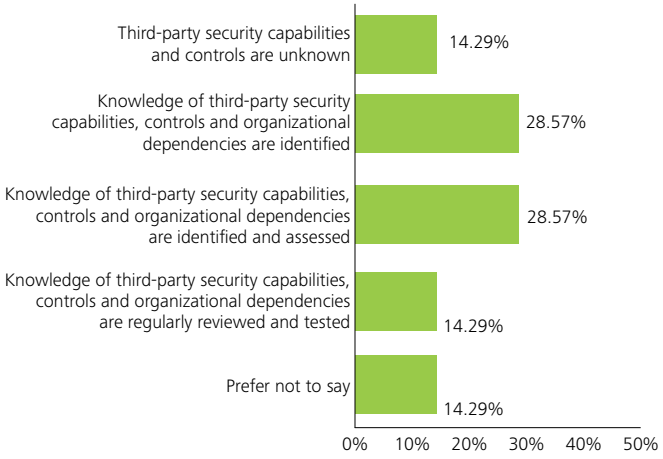



**Figure 13b (HC Payers) – Knowledge of third-party security capabilities and controls**



# Use of Security Technology

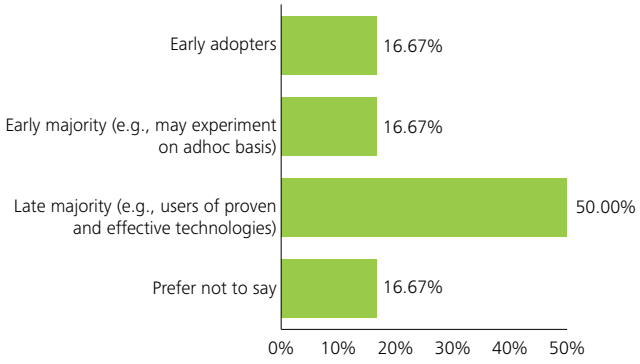
### Deployment of technologies

Respondents indicate that their organizations have a mixture of proactive and reactive solutions to meet their security and privacy needs. The majority of respondents have the following solutions fully deployed: firewalls, content filtering/monitoring, spam filtering solutions, antivirus, VPNs, and encryption.

Most respondents do implement and encourage the use of secured technologies such as storage devices, mobile devices, and instant messaging technologies. In terms of social networking technologies, less than half of respondents (29%) actually prohibit their use. The rest either offer employee guidelines on secure use or publish policies on acceptable business use.

Respondents vary in their level of adoption of security technology; 17% are early adopters while 50% are late majority.

**Figure 14 (HC Payers) – Level of adoption of security technologies**




# Privacy program

A majority of respondents have mature privacy functions; 86% have a privacy program that is either starting to evaluate the effectiveness of key initiatives or is in maintenance mode focused on program evaluation and refinement. Regulatory compliance is the main driver for the privacy program.

Overwhelmingly, respondents (86%) cite unauthorized access to personal information as their top privacy concern. With third-party organizations being the right arm of the payer sector, managing third-party information sharing is second at 57%. These responses support the finding of data leakage protection as one of top initiatives of organizations.

**Figure 15 (HC Payers) – Stage of development of the privacy function**

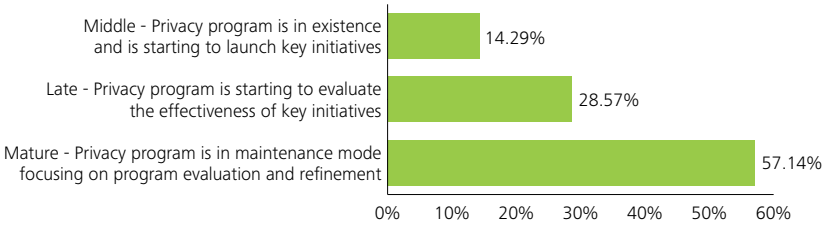
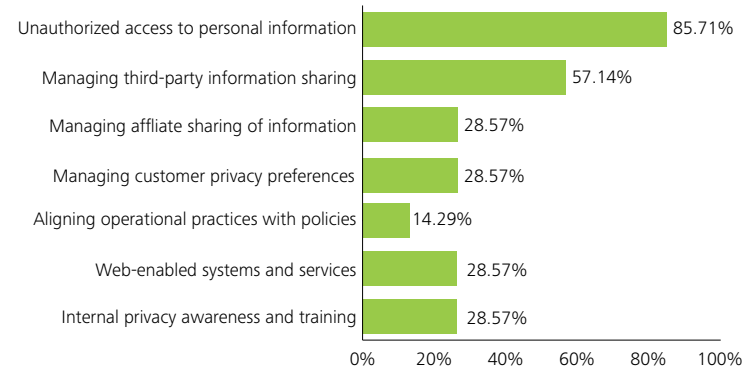



**Figure 16 (HC Payers) – Top privacy concerns of organizations**




# How DTT's Security & Privacy Services practices designed, implemented and evaluated the study

The 2009 Life Sciences and Health Care Security Study reports on the outcome of focused discussions between DTT Member Firm Security & Privacy Services professionals and Information Technology executives of global life sciences and health care organizations.

Discussions with representatives of these organizations were designed to identify, record, and present the state of the practice of information security in the life sciences and health care industry with a particular emphasis on identifying levels of perceived risks, the types of risks with which organizations are concerned, and the resources being used to mitigate these risks. The study also identifies which technologies are being implemented to improve security and the value life sciences and health care organizations are gaining from their security and privacy investments. To fulfill this objective, senior Deloitte member firm professionals within DTT Member Firm Security & Privacy Services practices designed a questionnaire that probed various aspects of strategic and operational areas of security and privacy.

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

# Acknowledgements

The member firms of Deloitte Touche Tohmatsu wish to thank all of the professionals of the life sciences organizations who responded to this year's study. Without such participation and commitment, Deloitte Touche Tohmatsu could not produce studies such as this and extends heartfelt thanks for the time and effort that respondents devoted to this project.

**Study development team**
**Amry Junaideen**, Deloitte & Touche LLP
**Pam Williams**, Deloitte & Touche LLP
**April Holder-Bedford**, Deloitte & Touche LLP

**Contributors**
AJ Armour, Deloitte & Touche LLP
John Bigalke, Deloitte & Touche LLP
Christopher Bullock, Deloitte & Touche LLP
Lyle Carlson, Deloitte & Touche LLP
Charles Cohen, Deloitte Touche Tohmatsu
Ken DeJarnette, Deloitte & Touche LLP
Ted Dezabala, Deloitte & Touche LLP
Juan Duque, Deloitte & Touche LLP
Robert Go, Deloitte Touche Tohmatsu
Terry Hisey, Deloitte & Touche LLP
Russell Jones, Deloitte & Touche LLP
Christopher Lee, Deloitte & Touche LLP
David McKeon, Deloitte & Touche LLP
Rena Mears, Deloitte & Touche LLP
Adel Melek, Deloitte & Touche LLP
Dave Melnick, Deloitte & Touche LLP
Bruce Murphy, Deloitte & Touche LLP
Julie Ng, Deloitte & Touche LLP
Ash Raghavan, Deloitte & Touche LLP
John Rhodes, Deloitte & Touche LLP
Russ Rudish, Deloitte & Touche LLP
Larry Samano, Deloitte & Touche LLP
M.J. Vaidya, Deloitte & Touche LLP
Damian Walsh, Deloitte & Touche LLP
Fiona Williams, Deloitte & Touche LLP
Andrew Wintermuth, Deloitte & Touche LLP
Amy Yates, Deloitte & Touche LLP
Keith Zielenski, Deloitte & Touche LLP

## Study Methodology, Data Analysis, Editing

**Olivier Curet**
Deloitte & Touche LLP
ocuret@deloitte.com

**Clare Galloway**
Wordcorp Communications Inc.
www.wordcorp.ca

**Sushant Gangadhar Gaonkar**
Deloitte India
sgaonkar@deloitte.com

**Prasad Kantamneni**
Deloitte India
pkantamneni@deloitte.com

**Sheila Celata**
Deloitte & Touche LLP
scelata@deloitte.com

**Cynthia M O'Brien**
Deloitte & Touche LLP
cynobrien@deloitte.com

## Marketing, Operations, Communications

**Patsy Bolduc**
Deloitte Touche Tohmatsu
pbolduc@deloitte.com

**Sarah Callihan**
Deloitte & Touche LLP
scallihan@deloitte.com

**Terry Koch**
Deloitte Touche Tohmatsu
tekoch@deloitte.com

**Ginger Kreil**
Deloitte & Touche LLP
gkreil@deloitte.com

**Terrie Perella**
Deloitte & Touche LLP
tperella@deloitte.com

**Pam Williams**
Deloitte & Touche LLP
pamewilliams@deloitte.com

# Contacts

## Leadership Team

**Sam Balaji**
Deloitte & Touche LLP
National Technology Risk Leader
sbalaji@deloitte.com

**Ted DeZabala**
Deloitte & Touche LLP
National Security & Privacy Leader
tdezabala@deloitte.com

**Robert Go**
Deloitte Touche Tohmatsu
Global Life Sciences and & Health Care Industry Leader
rgo@deloitte.com

**Mark Layton**
Deloitte & Touche LLP
Global Enterprise Risk Services Leader
mlayton@deloitte.com

**Adel Melek**
Deloitte & Touche LLP
Global Security & Privacy Leader
amelek@deloitte.ca

**John Rhodes**
Deloitte & Touche LLP
Global Life Sciences and Health Care Leader - LS & Audit
jorhodes@deloitte.com

## Security & Privacy Services

**United States**

**Amry Junaideeen**
Deloitte & Touche LLP
Washington D.C.
ajunaideen@deloitte.com

**Mark Ford**
Deloitte & Touche LLP
Detroit
mford@deloitte.com

**Rena Mears**
Deloitte & Touche LLP
San Francisco
renamears@deloitte.com

**Ed Powers**
Deloitte & Touche LLP
New York
epowers@deloitte.com

**Ken DeJarnette**
Deloitte & Touche LLP
San Francisco
kdejarnette@deloitte.com

**Bill Kobel**
Deloitte & Touche LLP
Dallas
bkobel@deloitte.com

**Rick Siebenaler**
Deloitte & Touche LLP
Chicago
rsiebenaler@deloitte.com

**Fiona Williams**
Deloitte & Touche LLP
Costa Mesa
fwilliams@deloitte.com

**Vishal Chawla**
Deloitte & Touche LLP
Wilton
vchawla@deloitte.com

**Sean Peasley**
Deloitte & Touche LLP
Costa Mesa
speasley@deloitte.com

**Lyle Carlson**
Deloitte & Touche LLP
Indianapolis
lylecarlson@deloitte.com

**Ann Litke**
Deloitte & Touche LLP
Costa Mesa
alitke@deloitte.com

**David Sarabacha**
Deloitte & Touche LLP
Seattle
dsarabacha@deloitte.com

**Adnan Amjad**
Deloitte & Touche LLP
Houston
aamjad@deloitte.com

**Irfan Saif**
Deloitte & Touche LLP
San Jose
isaif@deloitte.com

**Kelly Bissell**
Deloitte & Touche LLP
Atlanta
kbissell@deloitte.com

**Deborah Golden**
Deloitte & Touche LLP
Stamford
debgolden@deloitte.com

**Adnan Amjad**
Deloitte & Touche LLP
Houston
aamjad@deloitte.com

**Mike Wyatt**
Deloitte & Touche LLP
Austin
miwyatt@deloitte.com

**EMEA**

**Simon Owen**
Deloitte UK
sxowen@deloitte.co.uk

**Asia Pacific**

**Uantchern Loh**
Deloitte Singapore
uloh@deloitte.com

**Joshua Chua**
Deloitte Singapore
joshuachua@deloitte.com

**Japan**

**Mitsuhiko Maruyama**
Deloitte Japan
mitsuhiko.maruyama@tohmatsu.co.jp

**Bruce Daly**
Deloitte Japan
brdaly.maruyama@tohmatsu.co.jp

**Latin America**

Martin Carmuega
Deloitte Argentina
mcarmuega@deloitte.com.ar

**Andres Gil**
Deloitte Argentina
angil@deloitte.com.ar

## Life Science & Health Care Contacts

**United States**

**David Hodgson**
Deloitte & Touche LLP
Life Sciences & Health Care
dhodgson@deloitte.com

**Terry Hisey**
Deloitte Consulting LLP
Life Sciences & Health Care
rhisey@deloitte.com

**David Green**
Deloitte Tax LLP
Life Sciences & Health Care
davgreen@deloitte.com

**Pete Mooney**
Deloitte Consulting LLP
Life Sciences & Health Care
pmooney@deloitte.com

**Russ Rudish**
Deloitte Consulting LLP
Health Care Providers
rrudish@deloitte.com

**EMEA**

**Dean Arnold**
Deloitte UK
Health Care
deanarnold@deloitte.co.uk

**Stuart Henderson**
Deloitte UK
Regional
stuhenderson@deloitte.com

**David L. Jones.**
Deloitte UK
Life Sciences & Health Care
davidljones@deloitte.co.uk

**APAC**

**Keiji Watanabe**
Deloitte Japan
Regional
kewatanabe@deloitte.com

About the life sciences industry
The Life Sciences practices of the Deloitte member firms provide audit, consulting, financial advisory and tax services to industry leaders. Deloitte member firms serve three-quarters of the Fortune Global 500 life sciences and health care companies. Among the leaders in life sciences, Deloitte member firms serve each of the 10 largest pharmaceutical companies, as well as half of the 10 largest companies in the medical devices and biotech sectors. Due to regulatory and other reasons, certain member firms do not provide services in all four professional areas.

About security & privacy services
Deloitte member firm Security and Privacy Services professionals are positioned to design, develop and implement industry-leading information security solutions for businesses. Deloitte member firm services include:

Strategy & Management
Security and Privacy Services professionals help clients develop and implement enterprise strategies and programs for managing information and technology risk

Technology Integration
Security and Privacy Services professionals help clients select, develop, and implement security and privacy technologies or implement information and technology controls within systems and applications



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

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