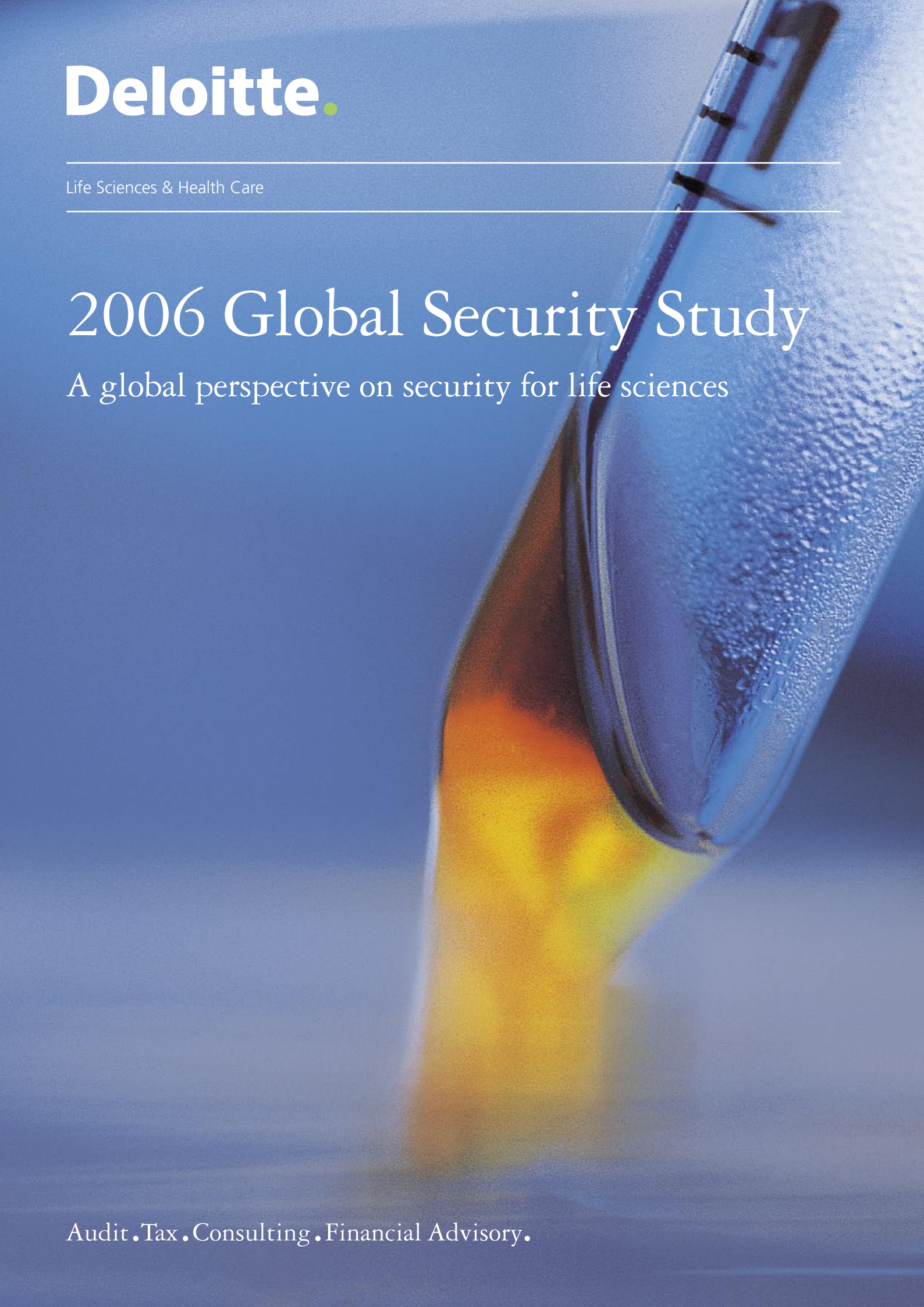
Deloitte.

Life Sciences & Health Care

2006 Global Security Study

A global perspective on security for life sciences



Audit . Tax . Consulting . Financial Advisory .

Contents

F

A newspaper columnist was quoted as saying, "Begin somewhere; you cannot build a reputation on what you intend to do[1]." In an effort to better understand the emerging themes around security and related issues in the life sciences industry, Deloitte Touche Tohmatsu (DTT) has undertaken to survey a global representation of leading company executives. After many months of poring over percentages and findings, the results are contained in this inaugural study. DTT hopes to continue to produce this study annually.

At first glance, the strategic challenges facing the life sciences industry may not appear to be very different from those of other industries. For many reasons, however, there are areas where life sciences stands alone — and faces unique regulatory and marketplace pressures.

What has emerged from the findings of the DTT study is that security is a topic on the business agendas of numerous organizations, as they grapple with issues that go far beyond the scope of the traditional security function. Many organizations are coming to the realization that pragmatic, program-based efforts are more sustainable — and more effective — than isolated fire-fighting tactics that address only the compliance need of the moment.

In addition to direct responses to questions, the DTT study presents industry trends, security considerations that go beyond the realm of IT, and issues such as business continuity management, privacy and the management of cross-border data.

For responses to the questions, DTT member firms polled Chief Security Officers and their designates, as well as the executive management teams from the pharmaceutical, biotech and medical device manufacturing industry organizations around the world. DTT thanks the participants sincerely for the time they spent and the candid and forthcoming manner in which they participated in the discussion. And, of course, thanks goes to the Deloitte member firm practitioners, who engaged these industry executives in informed conversation on timely industry issues.

Participation in the DTT study comes from Europe, North America, and Asia Pacific. The study will be translated into French, German and Japanese. The hope is that executives will use this report as a tool to stimulate conversation, not only within their organizations but with external partners as well, with the purpose of addressing security-related exposures that may impact the financial well being of the business.

With this study, DTT is embarking on an important undertaking for the life sciences industry. DTT member firms are excited at the thought of what lies ahead for life sciences.

Terry Hisey
Deputy Managing Principal
Life Sciences and Health Care
Deloitte Consulting LLP

Amry Junaideen
Global Life Sciences
Leader for Security & Privacy
Deloitte & Touche LLP

[1] Liz Smith (1923 - ____) US columnist, "The Speaker's Electronic Reference Collection," AApex Software, 1994

Executive summary

Evolutionary changes challenge life sciences industry

The strategic challenges facing the life sciences industry[2] are not hugely different from those of other industries. Across the board, successful organizations must excel in such areas as product innovation and commercialization, manufacturing excellence, cost efficiency and time-to-market. However, in certain areas, life sciences stands alone, facing regulatory and marketplace pressures unheard of in most other industries.

Greater drug trial disclosure requirements, heightened public focus on product pricing and marketing activities, increased litigation coupled with soaring liability and compliance with new financial and corporate governance laws represent just a few of the external factors that have increased scrutiny and pressure on the industry. In order for life sciences organizations to achieve success, they need reach for a bar that is being set ever higher.

Among the most onerous changes in the new environment are the enactment of strict data privacy and security regulations. These regulations, despite varying requirements on a per-country (and sometimes even a per-state) basis, need to be thoroughly understood and addressed in order for the organization to compete successfully in its respective markets.

The emerging picture for life sciences is one of an increasingly burdened industry prone to internal and external pressures from a myriad of sources. Savvy and successful organizations are beginning to proactively pursue risk-reduction strategies to deal with these strains that threaten to disrupt business as usual. There are distinct advantages to integrating security and privacy risk management into the organization's day-to-day operations, which many of the study's respondents intend to do in the near future. The real shift will be in strategy rather than in operations, as more forward-thinking entities view security and privacy not as a cost, but as a value proposition — one that results in brand protection, safeguarding of superior intellectual property, product and consumer confidence.

[2] In this report, DTT collectively refers to organizations in the pharmaceutical, biotech, generic and medical devices manufacturers industries as the life sciences industry. Although DTT recognizes there are differences between the industry segments, the risks and concerns associated with security and privacy are similar cross-industry.

Key findings

Deloitte member firms surveyed a global representation of leading company executives in an effort to better understand the emerging issues and innovative approaches around security and privacy (See "About the Study"). This study explores a variety of interrelated dimensions including:

- leadership
- strategy
- operations
- management
- budgeting
- investment
- compliance
- risk management
- awareness
- training
- data privacy
- business continuity

Three key themes emerged from the data:

1. Security, information protection, and data privacy are commanding greater attention from senior management and the board. In ever-increasing numbers, life sciences organizations are emphasizing the proper "tone at the top," adopting enterprise-wide views of security, and embracing the protection of information assets. Although significant challenges remain, these life sciences organizations recognize the need to have an enterprise security program led by a senior security professional, along with a strong governance framework for decision-making and delineation of accountability.

More life science organizations are appointing chief security officers (CSOs) or the equivalent positions, with two-thirds of respondents having already done so. There is no leading organizational structure for the security function. Hierarchical lines of reporting and job responsibilities vary, from the more "traditional" IT security function to responsibility for privacy, and business continuity management. While respondents cite strong executive-level support, common obstacles to success include business-unit-level buy-in, insufficient budgets, and lack of qualified resources.

Creating an integrated security function by merging the physical aspects (i.e., corporate security office) with information technology (IT security) are on the "wish lists" of many of those surveyed but is not yet reality for the majority of organizations surveyed. Less than one in three respondents indicate plans to merge the two functions or have achieved progress towards that goal.

The role of chief privacy officer (CPO) and related privacy programs continue to evolve, albeit at a less rapid pace than the role of the CSO. Thirty-nine percent of respondents reported that their privacy programs are in the "early phases" while only 7% stated that their privacy programs were in a "mature phase."

2. Organizations are achieving mixed results in implementing security and privacy protection programs. Virtually all respondents have security awareness programs with varying degrees of inclusion of employees, contractors, management, and other executives, including board members. A number of respondents do not extend their awareness program to third parties, such as outsourcers and external business partners or alliance members. There is often no effective method of measuring awareness or effectiveness based on the education program.

Organizations cite the increasing sophistication of technology threats (i.e., IT-based technical attacks) as a top security challenge and identify cyber-terrorism and maintaining privacy of customer data as lower priorities. Meanwhile, one in four respondents also report that their systems were breached in the past year, either via external or internal sources.

From a global perspective, convergence of security and privacy standards across the European Union, North American, or Asia-Pacific countries is not going to occur in the immediate future. Instead, organizations need to truly understand and accommodate the different standards rather than wait for convergence. Study respondents demonstrated mixed results in complying with local and global standards. However, many countries require similar product, process, and corporate standards in their respective markets. By "leveraging" universal standards and their own country-specific compliance efforts into new market regions with similar requirements, an opportunity exists for multinational organizations operating in foreign markets.

The complexity drivers

1. Regulations
Life sciences organizations face the complex challenge of complying with worldwide country-specific regulations. Any life sciences entity selling products in the US market needs to comply with US FDA regulations. Similarly, organizations that sell products globally need to comply with regulation of other countries, such as the U.K.'s Medicines and Healthcare Products Regulatory Agency, Japan's Ministry of Health, Labour and Welfare, and Australia's Therapeutic Goods Administration. In addition, governing bodies such as the FTC have become active in issuing "consent decrees" against organizations that have violated trade practices and applicable laws.

2. Supply chain security & nascent standards
A major issue facing life sciences organizations is the security of their supply chains, specifically drug identification, counterfeiting and grey markets. Interdependent supply chains put organizations at greater security risk, by virtue of multiple partners and "handoffs" in production and distribution. Global organizations are increasingly dictating operational standards and assessing business partners against these standards on an ongoing basis. For example, major retailers are requiring suppliers to use technologies such as radio frequency identification (RFID) to track product through the supply chain. Proposed "e-pedigree" standards mandate tracking of commercial drugs for improved consumer safety and help organizations stem fraud-related losses. There are emerging government initiatives such as C-TPAT[3], which, although not currently mandatory, may become law in the near future. However, most of these standards are nascent and under development.

3. Intellectual property (IP)
The importance of safeguarding corporate assets, including physical product, intellectual capital, and other confidential business information, is widely recognized. Failure to protect these assets can compromise an organization's ongoing viability, competitive advantage and brand. Cases involving stolen customer data and compromised corporate systems have resulted in legal action and additional financial ramifications for the affected corporation.

4. Data privacy
Privacy laws vary in their "strictness" and enforcement by country, region, and culture. On a global basis, regulatory restrictions on the use of personally identifiable information (PII) have put the onus on multinational organizations to better manage their data processes. For example, organizations in the European Union are prohibited from sharing PII with non-EU organizations unless they can demonstrate privacy practices commensurate to EU privacy laws.

5. Outsourcing and the "Extended Enterprise"
Globalization brings more participants into the supply chain. These participants include foreign manufacturers and their supplier networks, foreign transportation, and government regulators, increasing the possibility for theft and for exposure to substandard labor practices. An expanding network introduces more uncertainty on both the demand and supply side. Integrating fundamentally sound security and privacy practices across the extended enterprise is a difficult and time-consuming process, further complicated by entities with complex corporate structures and extended geographical boundaries. Add to this mix an environment of ever-increasing alliances, Merger & Acquisition activity and global licensing, and it is clear that few organizations would want to acquire, or do business with, an entity that lacks vigilant and vigorous security and privacy practices.

[3] US Customs-Trade-Partnership Against Terrorism. Currently, organizations comply voluntarily to demonstrate security standards within their supply chains. Compliance can result in benefit such as reduced inspection time of goods at US borders.

Differentiation opportunities may exist for organizations able to distinguish themselves by providing reliable and secure storage and transmission of information and products on a global scale. By embracing the right security strategy, governance model, and controls, organizations can better manage their various points of risk and boost their competitiveness. Furthermore, in today's global economy, where life sciences organizations routinely outsource clinical trials, research, product manufacturing and finishing, and other functions to business partners globally, it is not sufficient to look at security and privacy solely within the walls of an enterprise. Life sciences organizations should ensure that their business partners have acceptable standards and processes in place to protect [information] assets and to assure compliance with regulatory mandates.

> One in four respondents also report that their systems were breached in the past year, either via external or internal sources.

3. Organizations are adopting uniform standards and international frameworks and leveraging technology, all of which can enable them to comply "smarter." Respondents indicate that the primary focus of the security budget is regulatory compliance. In fact, compliance-related spending increased from the prior year for the majority of organizations. In terms of technology investment, one in four respondents plan to introduce biometric security measures over the next 18 months, while one-third will pilot public key infrastructure (PKI) solutions, and over 40% will pilot smart cards in the short term. Many organizations are considering increasing investments in radio frequency identification tags (RFID) technologies. Study respondents indicated a ten-fold increase in pilot projects for RFID.

Balancing business needs while satisfying ever-growing security, privacy, and regulatory compliance requirements is a source of frustration for many organizations. However increasingly sophisticated technology together with the right "top down," or enterprise–wide, perspective can potentially allow an entity to meet compliance needs more efficiently.

Life sciences organizations understand the most critical risks to the business and respond to them via the adoption of more effective technologies that simplify, automate, and account for those risks. DTT's study indicates that identity management safeguards are being increasingly deployed by life sciences organizations to allow them to realize benefits such as compliance with regulations, enhanced security, granular access control, and centralized administration.

Organizations should attack compliance costs by applying the principles of risk. By establishing an integrated control framework from the top down, and examining the highest risks first, organizations can "do more with less". Top down frameworks are more effective than bottom up methods that give equal weight to risks of varying intensity. Stated another way, "smart compliance is an opportunity to redefine and streamline business processes, increase operational efficiencies and reduce duplication of effort".

Conclusion: so what does this all mean?

As stated earlier in this report, the competitive forces in the life sciences industry are compelling organizations to look at creative approaches to stay ahead of the competition, as well as to continue to produce strong shareholder returns. As such, organizations will likely continue to engage in outsourcing, out-licensing, international partnerships/ alliances, and technology spin-outs. These approaches create security, privacy, and intellectual property risks. If these risks are not adequately addressed, the result could be a variety of negative events, such as failed alliance agreements, patent disputes over business critical IP, enforcement actions by regulatory agencies, or a lower-than-expected valuation for an acquisition candidate.

For the major drug entities that want to differentiate themselves, the appropriate levels of security and privacy will help to secure opportunities for additional sales and profits. However, there is no "one-stop" or "off-the-shelf" security and privacy solution that fits all. While the study shows that CSOs and CPOs are making significant progress, the road ahead is not without its bumps. Following are leading practices that can help organizations to further their security and privacy goals.

> Europe has a very different philosophical basis for personal information privacy than the US.

1. Establish awareness of the "value creation" potential of security investments versus the traditional return on investment approach. When it comes to security and privacy initiatives, perception can become reality. That is, if key people within the organization see the program as a drain on resources and an expense with little return, success will be elusive. The skeptics who disagree with the notion that security creates value need to be won over. This area is a key challenge faced by many organizations, as illustrated by the study, conversations with member firm clients, and through focus groups.

Establishing a measurable return on investment is a common concern voiced by many CSOs. Their quandary is formidable: If there are no security or privacy breaches, then people become complacent about the value of security. If there is a problem, then all fingers quickly point to those they believe are responsible.

Properly implemented security and privacy programs can become key business enablers. Security and privacy needs to become a part of both operational and strategic processes. Organizations can begin by gaining an understanding of all of their risks and aligning the impact of those risks to their business functions and technology components.

Progress is being made, and the concept of value creation continues to gain credibility. Fueling this trend are recent well-publicized incidents of compromised security and privacy at prominent and respected organizations. Executives are realizing that such incidents can have a major impact in terms of publicity, reputation, and, ultimately, shareholder value.

> Organizations that are too compliance-focused may be placing themselves in peril by not focusing on the true risks to the business.

2. Align with organization goals and implement an effective governance structure and organizational model. Successful information security and privacy programs depend on sponsorship from executive-level management and leaders from each line of business. These programs should be aligned with the mission, goals, and objectives of the organization. As the security and privacy program matures, a key success factor for security and privacy leadership will likely be direct access to mechanisms that can raise their visibility and profile within the organization. Lacking this model, security and privacy programs will likely be seen as a burden or expense, rather than an enabler of the organization's mission and strategy.

Organizations are recognizing that the cost of inadequate or inappropriate security and privacy policies, standards, and practices is far more than an "IT problem." A broader governance framework should improve the integration of security and privacy risks into the overall enterprise risk management profile.

While alignment is important, the study also shows that a growing threat to the security and privacy agenda is being hijacked by a "compliance agenda." Given the increase in the number of regulations that affect the life sciences industry, it is not surprising that compliance is a heavy focus. Organizations that are too compliance-focused may be placing themselves in peril by not focusing on the true risks to the business.

3. Establish an integrated control framework that manages risks from an "extended enterprise" view. Risks to security and privacy have taken on an increasingly prominent profile in recent years. Potential disruptions arise from every direction. Threats include socio-environmental issues (earthquakes, pandemics, terrorism); information technology breaches (viruses, spyware, data theft or loss); physical property theft; product diversion and counterfeiting; and much more. Many of these threats exist across the global supply chain as organizations partner with suppliers, distributors, and other service providers. It is, of course, difficult to adopt a common risk framework for all these diverse entities, but it is important: a negative impact in any of these areas can adversely affect the brand as a whole.

Organizations should move away from protecting and preserving their information assets within isolated "silos," be they departments, functions, or lines of business. Today's world may be too networked and complex to sustain any physical strategy of separation.

> Protecting company IP is a need when doing business in emerging markets.

Corporations often find it easier to transfer responsibility for risk management: retailers offload it to suppliers; organizations buy insurance from third parties; even within businesses, they may seek to transfer responsibility to security officers, privacy officers, the legal department, and elsewhere without fully understanding the impact to the business, inadvertently creating even greater exposure. The effort to establish a real dialogue and a common, agreed-upon framework is likely much harder, but is a better way to address, quantify, and manage risks.

Ultimately organizations should be willing to span the entire business and create connections between "silos", with the goal of defining and managing all of their risks. Creating an atmosphere of "risk intelligence" that accounts for risk scenarios and the interaction of multiple risks — above and beyond the risk of non-compliance with regulations — will produce the environment most likely to foster success.

The world has evolved. Security and privacy concerns have moved to the forefront as a critical capability that all life sciences organizations will need to master in order to survive and prosper. In an environment where the pressure to prolong life and enhance the quality of life, keep prices affordable, improve service and assure safety, drive previously unheard of transformation throughout the industry, security and data privacy are now an absolute necessity.

Study findings and discussion

Security leadership and strategy

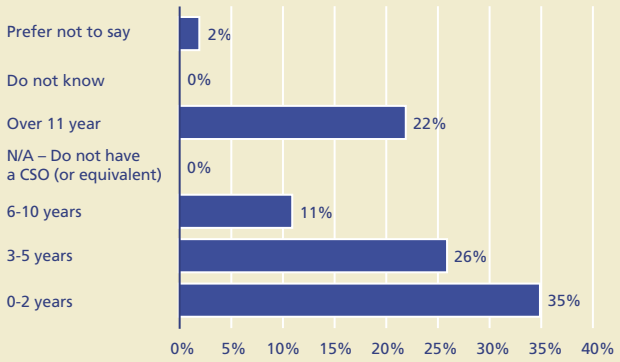
The new kid on the block: CSOs (and CISOs)

Life sciences organizations have taken measurable steps toward enterprise security management by appointing one or more senior security officers. More than two-thirds (70%) of organizations studied have established a chief security officer (CSO) or equivalent executive position. However, there appears to be no typical reporting structure for such positions. The CSO, for example, most frequently reports to the chief information officer (CIO), but can also report to other executives in the C-suite. In addition, the executive in charge of business continuity management most commonly reports to the CIO or CEO. And the chief privacy officer most frequently reports to either the CEO or general counsel.

The CSO position is a relatively new player in the life science industry — organizations reporting a CSO position have increased three-fold compared to a decade ago.

At least half of respondents report that responsibilities of their CEOs include the implementation of security policies, processes and technology (67%), security strategy (63%), and management and administration of the security function (50%). A third (37%) of the respondents say that their CSO also has responsibility for business continuity management (BCM). About 20% report that their CSOs oversee enterprise privacy (24%) and physical security (20%).

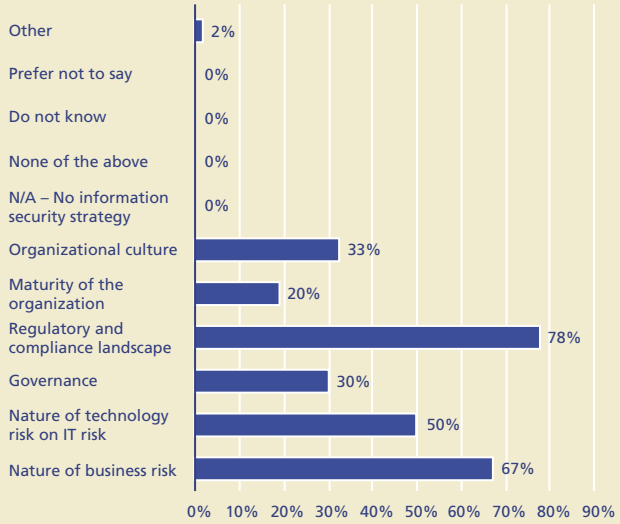
Figure 1. Tenure of the CSO



The findings suggest that security is no longer a technology issue. More than half the organizations state that C-suite executives constitute up to 50% of the leadership team that approves enterprise security program initiatives. Of the organizations that have a CSO or equivalent, the majority participate in executive committees such as IT committees or risk management committees.

The responses above point to the industry taking a more strategic, holistic approach to security via a "true CSO" role and not just adopting a narrow technical scope of IT security. Recent trends in the life sciences industry — including global supply chains, increased regulatory pressures, process outsourcing, and importance of brand reputation — necessitate that the "true CSO" position is a vital factor in the success of any organization in this industry.

Figure 2. Security program influencers



Security as a sustainable, risk based, enterprise wide program

Businesses are increasingly recognizing the need in today's environment for an "enterprise security program": an end-to-end approach to security, including centralized, enterprise-wide policy management, ongoing monitoring, and reporting. Study respondents say that the primary factors that influence the need for an enterprise security program include:

- regulatory & compliance landscape
- nature of business risk
- nature of technology risk

These factors are in alignment with key drivers and trends in the life sciences industry.

> The CSO has to act both as business advisor and security interpreter, understanding trends in the Global Life Sciences industry and ensuring the security strategy is aligned with the business to best meet executive management's goals.

The concept of an enterprise security program seems established, although the execution is still in "build out" phase. All organizations surveyed indicate that they have an enterprise security program in place or are in the process of establishing such a program. From an operational point of view, over 60% of respondents say that their security programs are hybrid in nature. i.e., policy development is centralized, but execution and day-to-day operations are left to business units or divisions

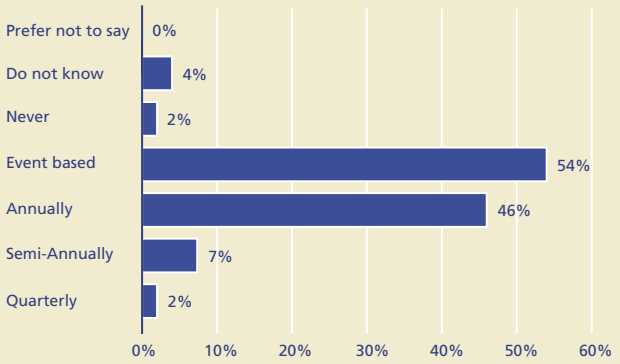
Looking ahead, the study respondents cite a variety of obstacles to security program success. The most prevalent obstacles are:

- insufficient budgets
- lack of business-owner buy-in
- integrating security into existing systems
- unrealistic timelines
- lack of qualified personnel

The status of risk assessments as an integral component to a sustained security program is also unclear. About 24% of respondents say that risk is fully integrated into their IT strategies, while 72% report that integration is still in progress. In contrast, only 9% of the organizations surveyed conduct risk assessments more frequently than once a year, while 46% perform them annually. Fifty-four percent of respondents assess risk on an "event basis."

These results suggest that a continuous risk assessment and response development approach is not fully integrated into security programs. DTT believes that the organization that successfully integrates a proactive risk assessment component into its security program will likely achieve competitive advantage in bringing product reliably and safely to market. These organizations also stand to benefit from outsourcing trends by becoming the preferred partners for other life science organizations that seek assurance over outsourced processes and evidence of consistent risk management practices.

Figure 3. Risk assessment within life science organizations



In terms of buy-in from the businesses, 70% of respondents indicate that business unit leaders have responded positively to their organization's security and privacy policies. But executives should ask whether their policies have been effectively translated into sustainable programs, and whether the business unit leaders recognize the corresponding value. The successful CSO should position the security program under a broader IT governance umbrella and demonstrate the ROI of good security practices in every business function, be it research, development, manufacturing, distribution, or back office operations.

RFID technology has proven to be valuable to supply chain management and is being increasingly mandated for suppliers by large-scale retailers. However, RFID is not in itself a panacea; life sciences executives should be aware of RFID-enabled product security and patient privacy concerns. Companies need to address the potential risks of implementing RFID, including the possibility of invading patient privacy via data collection and profiling, as well as the inventory management risks posed by electronic eavesdropping, denial of service attacks, and inventory jamming.

Security technology investment and ROI

State of technology as solution to security problems

Study respondents expect significant security technology development to occur within their organizations over the next 18 months. "Strong authentication" solutions including smart cards, biometric devices, and public key infrastructure (PKI) are among the leading areas of investment. One in four respondents plan to pilot biometrics over the next 18 months, while one-third will pilot PKI solutions and 41% will pilot smart cards in the short term. Contrast this to existing deployments: respondents report that current use of PKI or smart cards in a fully deployed state exists in less than one in four organizations. No respondents reported full deployment of biometric technology at the time of this study.

Identity and access management systems are currently entrenched, and organizations indicate plans to further utilize these technologies. The need to establish and safeguard a person's "virtual identity" is obvious in today's virtual business environment. Traditional security controls — "real world" corporate boundaries, security firewalls, and private access networks — no longer apply to the same extent. Organizations are increasingly creating extended logical and physical networks to conduct business efficiently and in an integrated manner with their partners. Consequently every customer, contractor, employee, supplier, or alliance partner that is part of the extended network also presents a security risk to the organization. If the external party's virtual identity is compromised, there is little likelihood that a network firewall can prevent a potentially malicious user from gaining access to the organization's assets. Perhaps in recognition of this risk, a third of the study respondents plan to pilot single sign-on technologies (32%) and/or access management systems (34%) in the short term.

The proprietary information leakage risks in the life sciences industry are unique. An organization invests heavily — and for prolonged periods — in the research and development of new drugs before the information is made public via patent application. The potential losses from early leakage of this information can have significant impact on the financial success of the product

Growing use of RFID

Investment in radio frequency identification tags (RFID) is expected to increase more than tenfold in the next 18 months. The use of RFID pilots in life sciences organizations may be the emerging industry-wide standard, one that it being proposed by an increasing number of US states. This standard is meant to assign accountability for a drug throughout its life cycle, from manufacturing to end delivery. RFID technology is one potential solution considered by drug makers to verify the drug's "chain of custody" through the myriad of global touch points in the supply chain.

Study results suggest that heightened regulatory standards also present operational and strategic benefits to organizations that adopt early compliance via RFID, combined with appropriate security and privacy safeguards. Operationally, technologies that track products electronically can streamline shipping and receiving, allow better inventory management, and expedite returns processing, all the while guaranteeing the quality and content of the shipments. Strategically, tracking mechanisms reduce the risk of product diversion and counterfeiting, allow precision of drug recall, and help protect the organization's brand reputation at a time of increasing concern over counterfeit drugs and the unfortunate human consequences.

Figure 4. Study respondents identified technology interest

Technologies	Fully deployed	Plan to pilot over next 18 months
Strong authentication		
Smart cards	16%	41%
Biometrics	0%	25%
Public key infrastructure	18%	34%
Identity and access management		
Single sign-on	25%	32%
Access management systems	30%	34%
Provisioning systems	5%	18%
Directories	50%	14%
Other technologies		
Wireless security products	30%	41%
Anti-virus	98%	18%
Voice Over IP (VoIP)	20%	39%
Radio Frequency Identification (RFID)	2%	34%
Vulnerability management systems	30%	25%

Security breaches in life science organizations

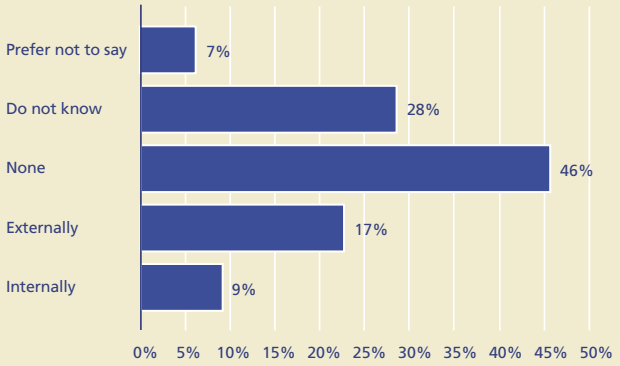
The convergence of responsibility for both "physical" security — the use of physical access restrictions such as security guards, badges, and alarm systems — and "logical" security — i.e., "online" or electronic mechanisms to safeguard information and computer applications — is a potential trend to watch for in the future. While 59% of organizations surveyed plan to maintain separate IT and corporate security functions, nearly a third (31%) say they have plans to merge the two functions or are already in-process of doing so.

Our study asked executives to name the top security challenges in today's environment. While nearly half (46%) of the organizations cite the increasing sophistication of technology threats (i.e., IT-based technical attacks) as a top challenge, a nearly equal share (48%) claim lack of employee awareness of security procedures and protocols as an important issue. Budget constraints are also cited as a challenge (35%), followed by staffing shortages (22%), virtual identity management concerns (20%), and lack of an overall security strategy (17%).

A quarter of respondents report that their information systems were breached in the past 12 months, either via internal or external sources. Almost half of the organizations indicate that their systems were not breached, the rest were not sure (28%) and about 7 percent "prefer not to say".

The Insider Threat Study conducted by the Secret Service National Threat Assessment Center (NTAC) and CERT, (http://www.cert.org/archive/pdf/insidercross051105.pdf) concluded that insiders will typically test the security capabilities of the organization many times before launching their attack. If an organization is complacent about the insider threat, it will generally have a lower rate of incident detection and therefore miss these test attempts, only to get hit hard when the real attack occurs.

Figure 5. Cause of security breaches



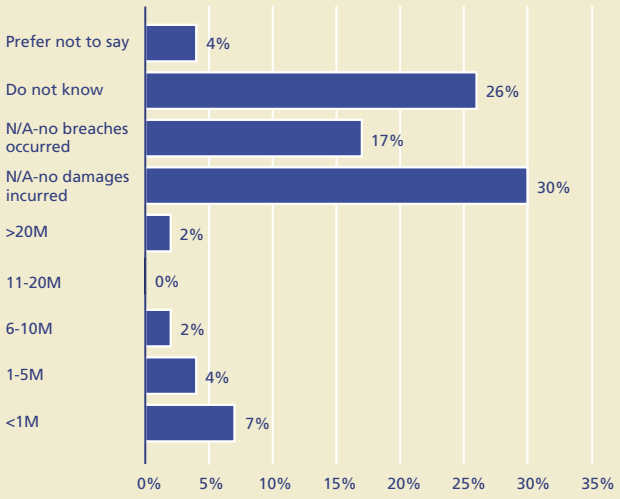
Impact of security incidents and measuring ROI of "good" security

Few organizations report economic loss as a result of security breaches, perhaps because they could not measure the impact of the breach. About one-third state that no losses occurred and that they cannot estimate the financial damage. Among organizations that could measure their losses, damages ranged from less than $1 million to over $20 million.

Measuring the economic cost of security breaches is an area for improvement by life sciences organizations. There is a need to develop metrics — other than direct revenue loss — to measure the impact of security incidents. Possible measurements include the calculation of system downtime; the cost of resources used to identify and remediate the security gap; and the potential impact from reporting the breach to management and regulatory agencies — both from a personal and a corporate perspective. Government regulations and industry standards are trending towards not only stricter security and privacy measures, but also demonstrable evidence, combined with management's assertion, that no actual breaches have occurred.

Use of enterprise security accountability mechanisms by the organizations is mixed. Only 48% report that all information assets in their organization have identified owners, while another 28% say that they are in the process of identifying such assets.

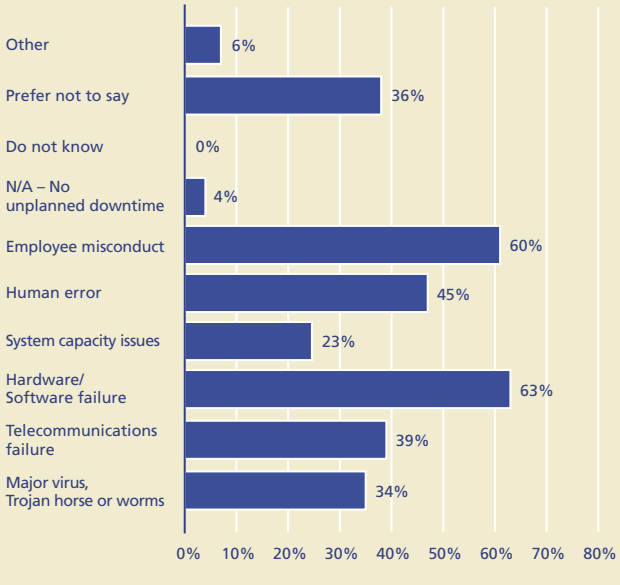
Figure 6. Economic cost of security breaches



The study found that the top three causes of unplanned downtime in critical business systems are:

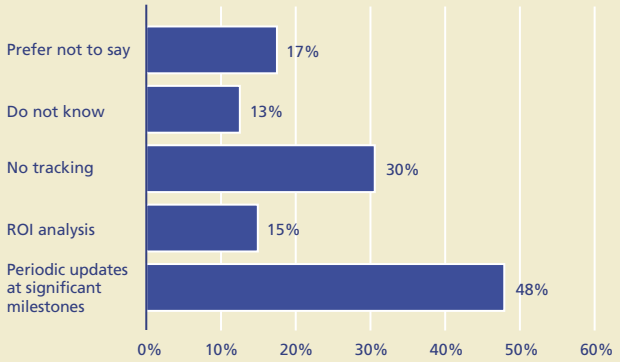
- hardware or software failure
- employee misconduct, and
- human error

Figure 7. Causes of downtime in critical business systems



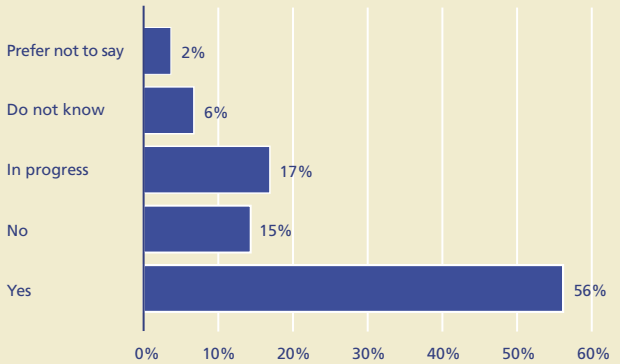
Only 56% of respondents say that they do have an effective mechanism in place to track their investments in security. Of the organizations that track security investments, they employ mechanisms such as periodic updates and ROI analysis.

Figure 8. Security investment tracking



Annual attestation, for example third party audits on the effectiveness of IT security controls is more common. More than half provide such attestation, and 17% are in the process of doing so.

Figure 9. Security performance measures



Adoption of other security measures reflects a similar, uneven pattern among the organizations studied. Only 35% have conducted a full audit of their information assets in the past 12 months, and just 52% maintain a complete inventory of software installations by application. Less than half (39%) perform trend analysis on IT security reports, perhaps reflecting a weakness or a gap in their security programs that makes conducting such analyses difficult.

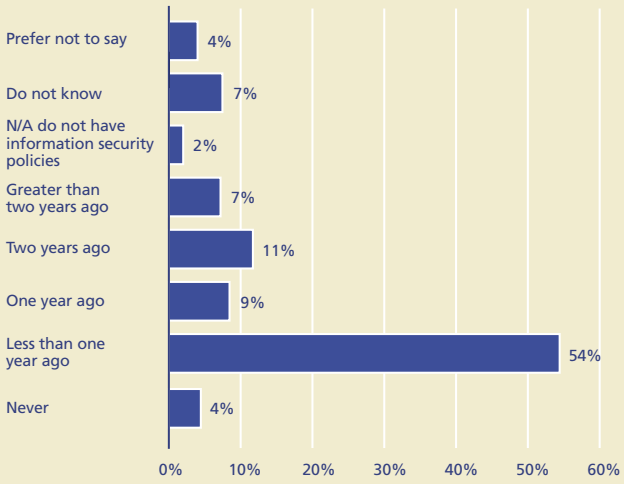
Overall, relatively few organizations have effective processes to measure the return on security investments (ROSI) or other impact of their security programs, as well as any breaches that may occur.

Measuring ROSI is a dilemma that faces CIOs and CSOs everywhere. There appears to be limited consensus as to how to quantify the benefits of "effective" security, i.e., the tools and procedures in place that allow organizations to successfully avoid or combat security threats. In lieu of numbers, information executives may tend to rely on soft ROSIs — explanations of returns that are obvious and important but impossible to verify. A true ROSI should contain qualitative as well as quantitative factors. Security weaknesses can emerge from, and impact, various functions of the organization — research and development, marketing, payroll, sales and distribution. It is important to have common measurement criteria in place to create acceptance and understanding of the value of security across all functions.

Security policy maintenance

Life sciences organizations appear to be keeping their security policies up-to-date. Most organizations report that they last reviewed their security policies for compliance with applicable laws less than a year ago, while only a few have never reviewed their security policies.

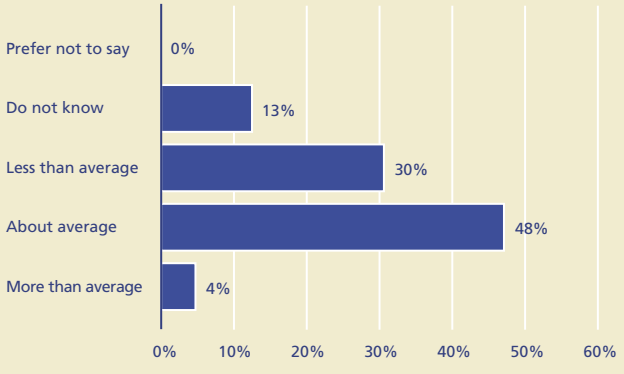
Figure 10. Security policy updates



Security budgeting and investment

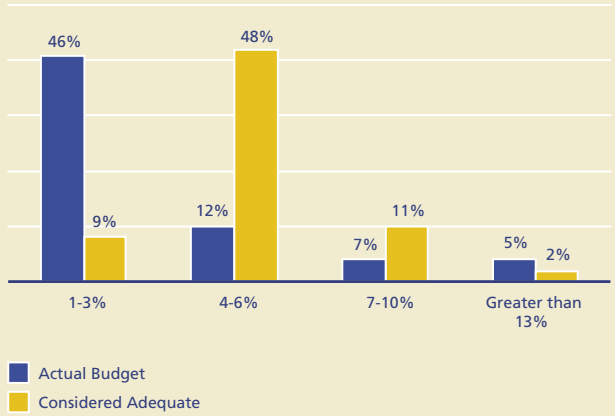
About half of the organizations (48%) say their security spending relative to their peers is about average. Most of the other organizations (43%) say that the amount spent on security is less than average or don't know how it compares.

Figure 11. Security spend



How much of the IT budget do organizations consider adequate for security? Nearly half (48%) say between 4% and 6% is adequate. In reality, only 1- 3% of the IT budget for most organizations is currently allocated to security.

Figure 12. Security budget adequacy

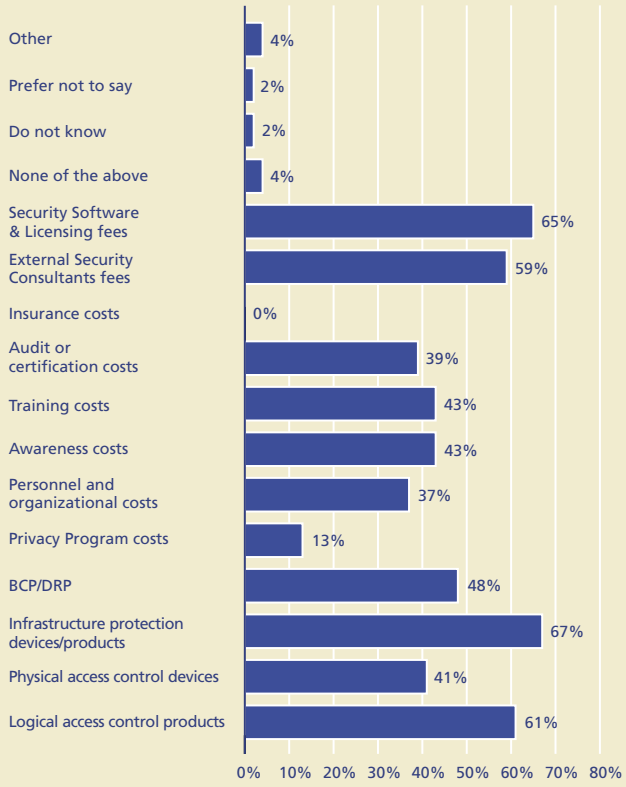


Most organizations studied say that funding for security projects needed to address regulatory requirements is either "somewhat adequate" (48%) or "very adequate" (22%). Only 9% believe the funding level is "somewhat inadequate."

About half of the organizations studied cite security training (54%), hardware and software infrastructure improvement (48%), and regulatory compliance (48%) as the top areas of security resource allocation in 2006, followed by enterprise security programs (39%), identity management (33%) and IT governance structure (24%).

However, respondents security budgets do not necessarily address these "pain points." For instance, less than half of the organizations included awareness and training costs in their budget. For most, security budgets included the following categories:

Figure 13. Budget coverage

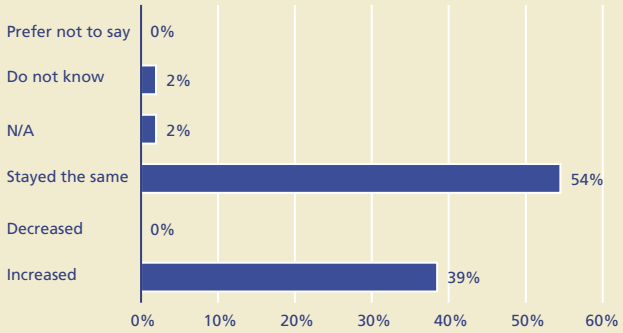


Almost all the organizations studied report an increase in their security budgets. One-fifth say that their security budgets grew 5% or less.

Regulatory compliance accounts for a substantial portion of security budgets. Nearly two-thirds allocate up to half of their budgets to regulatory compliance. When asked about Sarbanes-Oxley compliance, less than half assign 50% of their security budgets to Sarbanes-Oxley and one third do not allocate any funding for Sarbanes-Oxley compliance.

Over the past 12 months, the organizations studied either increased their security staffing or kept it at the same level. None reported that they decreased security staffing.

Figure 14. Staff investment



Key areas to consider while constructing a security budget request:

- Tangible and intangible costs of security incidents
- Quantitative and qualitative risk assessments
- Defense in depth — protect, detect, and recover
- Decision frameworks for security
- Methods to reduce the uncertainty of security investments

When asked which security measures are their highest and lowest priorities, respondents offer a variety of answers. Terrorism is the most cited priority, sighted as moderately high or the highest priority by 65% of organizations.

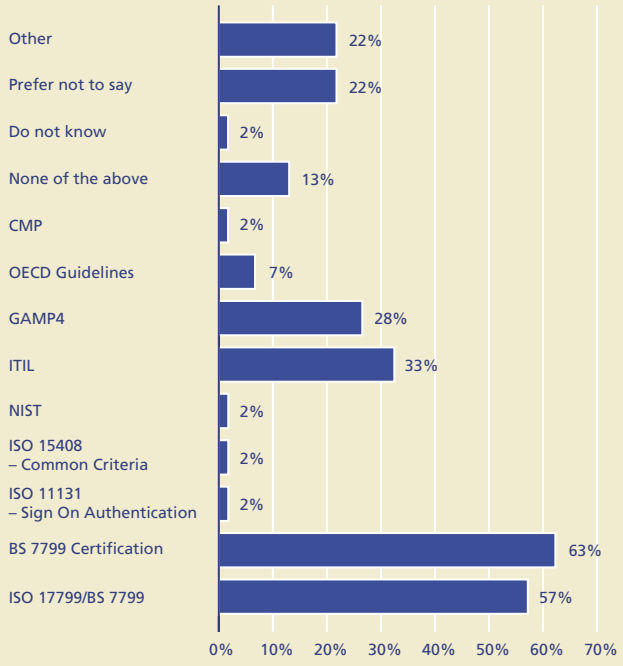
Figure 15. Security priorities

Security priorities	Not a priority	Moderately low	Moderately high	Highest priority
Financial fraud involving information systems	5%	65%	15%	15%
Supply chain security	0%	54%	40%	6%
Patch management	0%	66%	30%	4%
Software quality	0%	40%	55%	5%
Identity management	6%	48%	36%	7%
Maintaining customer privacy	0%	72%	22%	5%
Preventing intellectual property theft	0%	61%	30%	9%
Employee & business partner misconduct	0%	50%	40%	7%
Cyber-terrorism (vicious code, malware, viruses, etc)	0%	75%	22%	3%
Terrorism (not cyber)	17%	18%	45%	20%
Business continuity	2%	50%	40%	6%

Security compliance and risk management

Most organizations studied have adopted a variety of industry security standards. The top standards adopted are: ISO 17799/ BS 7799, ITIL, and GAMP4. Figure 16 illustrates the adoption of industry standards.

Figure 16. Adoption of industry standards



Despite inadequate reporting mechanisms, life sciences organizations we studied said that they distribute security reports to executive management (72%), their audit committee (24%), board of directors (9%), and regulators (7%). More than a quarter (28%) do so at least quarterly and 35% distribute such reports on an ad hoc basis. Only 15% say they never distribute security reports.

Non-compliance with regulations, laws, codes of conduct, etc, could potentially negatively affect companies in areas like:

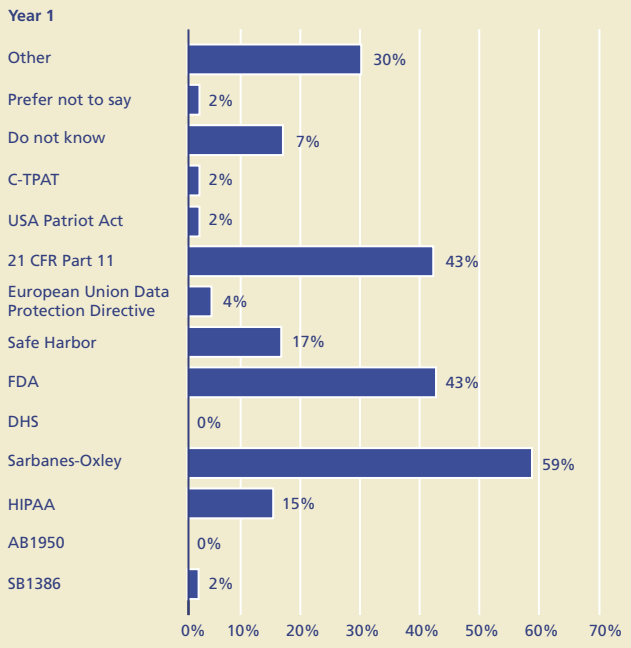
- Revenue (erosion of market share due to non compliance)
- Operating expense (fines and litigation expenses)
- Capital (asset efficiency and risk)
- Expectations (brand and reputation risks)

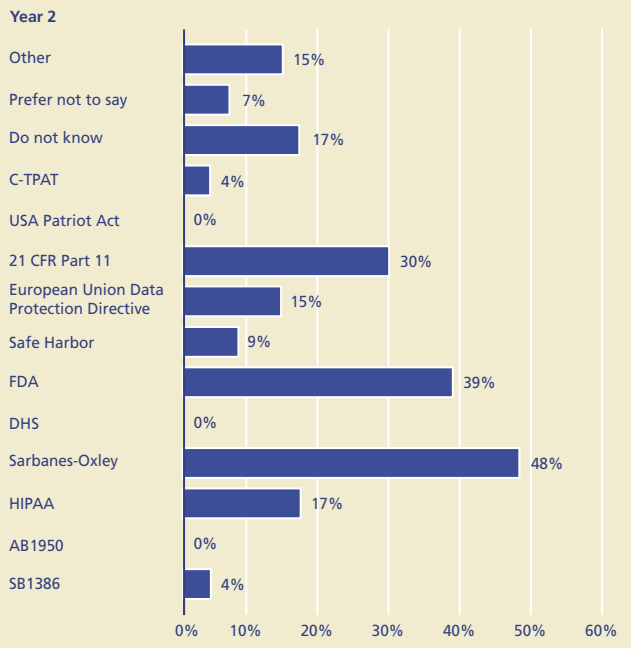
Fewer respondents expect to undertake major regulatory initiatives, such as Sarbanes-Oxley and the Food and Drug Administration's 21 CFR Part 11, in 2005 (year 2) than in 2004 (year 1). The level of effort they will expend in year two is expected to be less.

Only 15% and 17% of respondents indicate HIPAA as one of their major regulatory initiatives in year 1 and year 2, respectively. Over the next few years, life science organizations — especially biotech firms that have relationships with covered entities, hospitals, and physicians — will likely need to comply with HIPAA.

Seventy-two percent of respondents report that they spent more time on regulatory compliance in 2005 than in 2004. Only 9% say they spent less time while 65% use primarily manual methods, such as spreadsheets, to monitor compliance. Half of the respondents are using some automated methods, such as enterprise dashboards and other software tools, to supplement manual tracking. Life science organizations use both internal (85%) and external (67%) parties to perform reviews and assess security compliance with applicable laws and regulations.

Figure 17. Regulatory initiatives





Global regulations and integrated compliance systems

Requirements for electronic records have generally been harmonized between the European Union and the United States. These requirements are contained in:

- The Good Manufacturing Practice for Medical Products in the European Union — GMP Guide Annex 11: Computerized Systems, and
- United States Code of Federal Regulations, Title 21 Food and Drugs, Part 11 Electronic Records / Electronic signatures

Both requirements call for a broad-based set of controls that encompass all facets of the IT organization, from staffing to operations to system development activities and continuous monitoring and audit.

Asia is increasingly adopting European GMP standards in an effort to improve their owe regulations. Global organizations should be cognizant of all to compete in major markets.

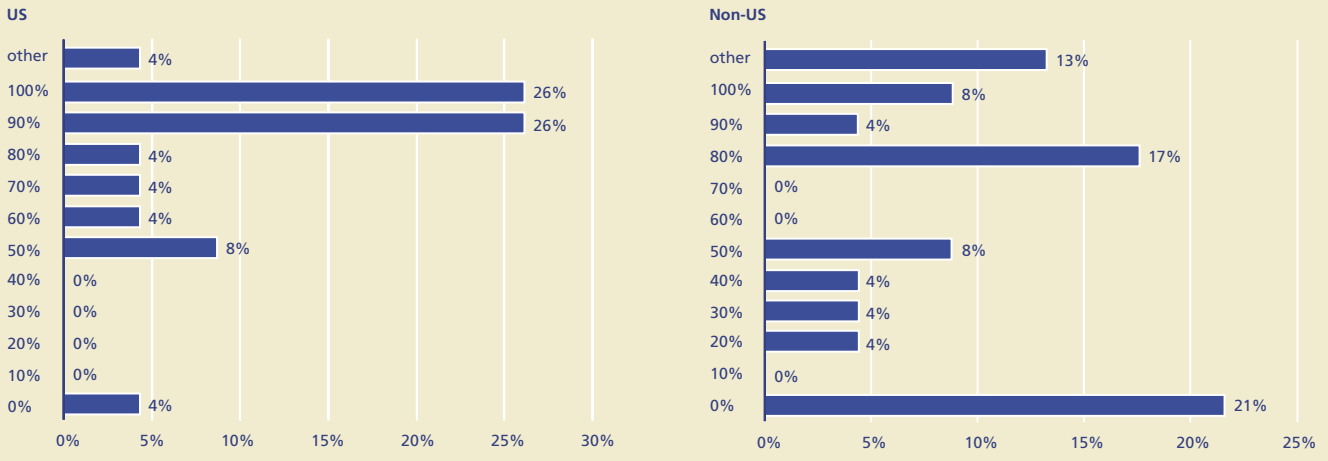
Both non-US and US organizations must be compliant with the FDA's 21 CFR Part 11 regulation in order to sell product in the US (the EU has a similar regulation called "Annex 11"). The study indicates that of organizations headquartered in the US, over half reported between 80% - 100% compliance with FDA's 21 CFR Part 11. A lower level of non-US based organizations report a similar level of compliance.

While organizations must comply with FDA in the US, they also must comply with regulatory bodies in other countries, such as Bundesgesellschaft fuer Arzneimittel (BGA) in Germany, Medicines and Healthcare products Regulatory Agency (MHRA) in the UK, and Ministry for Health and Welfare (MHW) in Japan.

In fact, almost every country has some kind of regulatory program overseeing the life sciences industry. For example, China's State Food and Drug Administration (SFDA) passed a regulation in 2004 requiring GMP certification for all of the country's pharmaceutical manufacturing sites.

Demonstrating compliance across the different regulatory bodies may be a leverage point, allowing organizations to more quickly bring products to market on a global level. Most life sciences organizations have robust quality programs in place. Executives should consider introducing organization-wide compliance management programs, incorporating not just product compliance, but compliance with applicable leading practices in security, privacy, and other functional or industry regulations and standards.

Figure 18. Regulatory compliance: US vs. Non-US

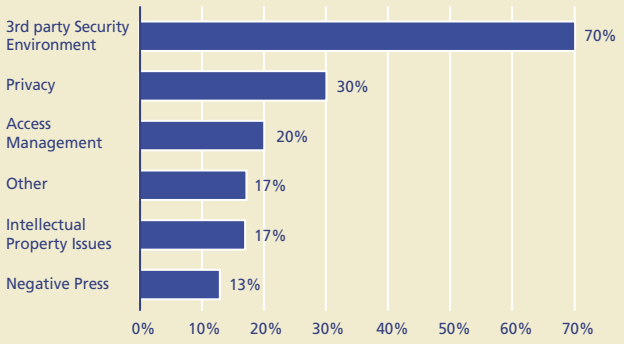


Outsourcing security functions

Most (87%) of the organizations studied outsource at least one or more of their IT security functions. According to respondents, the top three challenges associated with outsourcing are:

- third-party security
- privacy
- access management

Figure 19. Top outsourcing challenges



Only about half of the organizations studied (47%) conduct regular assessments of their IT outsourcers' compliance with their own information security policies. Only 37% of the organizations obtain from their vendors a third-party opinion, such as SAS 70 or BS 7799 certifications.

While 57% have classified their critical business assets in terms of value to the organization and identification of potential risks that could impact this value, 35% of respondents have not used this risk-management based classification. In addition, the majority of organizations (54%) have not classified their information assets by confidentiality, integrity, and availability (CIA). Information classification enables organizations to apply the appropriate level of controls to information and/or assets according to their sensitivity.

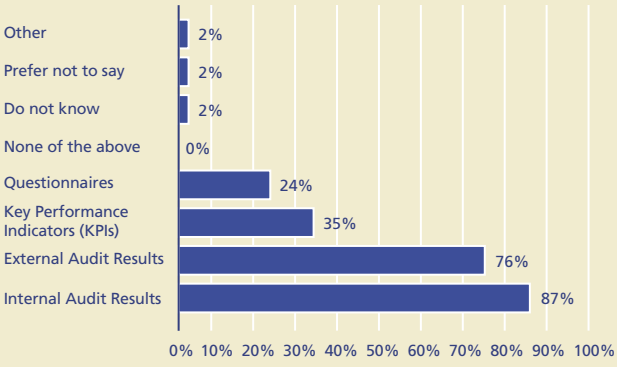
Most (59%) organizations report that they have incorporated security measures into their software development life cycle. Twenty-four (24%) have not incorporated such measures and 11% do not know whether or not they have. These responses indicate a trend in the right direction (even though progress is slow) given the increasing number of internet business applications, the move towards insourcing and outsourcing, and increasingly onerous security and privacy laws.

The role of security audits

Most organizations are placing heavy reliance on security audits to measure security compliance. More than three-quarters say they measure compliance using internal or external audit results. About one-third (35%) employ key performance indicators and about a quarter (24%) use questionnaires.

Organizations that tend to become complacent based on audits results should keep in mind that most audits measure the potential or "after the fact" evidence of security breaches, a measurement that does not necessarily reflect compliance with security policy or standards. The use of key performance indicators (KPI) can play an increasing role in the security and privacy arena, since they are designed to measure specific objectives of security compliance. Management should consider KPIs and standard KPI-driven scorecards that have become the barometer used by auditors (external as well as internal) to measure a program's effectiveness.

Figure 20. Reliance on security audits



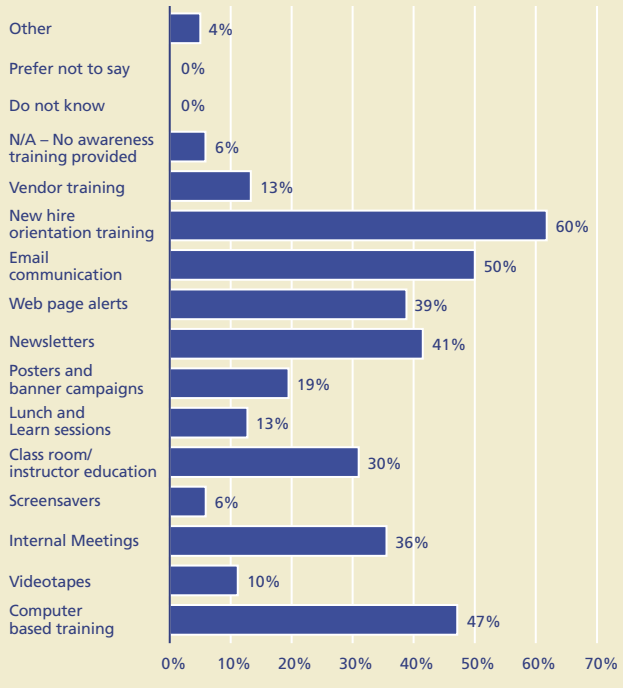
Security awareness and training

A large majority (85%) of the organizations studied have security awareness programs. Participants include employees (72%), management (63%), executives (52%), contractors (37%), and board members (26%).

The most frequently covered topics by security awareness programs are:

- password management (76%)
- viruses (70%)
- compliance with firm policies (67%)
- computer security (67%)
- handling sensitive documents (67%)

Figure 21. Methods of delivering security awareness



The most common methods of delivering security awareness are:

- orientation sessions for new employees (61%),
- e-mail communication (50%) and
- computer-based training (47%)

Approximately one in four (23%) respondents uses periodic studies to test employee awareness of security programs. However, nearly half of respondents (48%) have no measures in place to monitor employee awareness.

The "people factor" — not technology — is key to providing an adequate and appropriate level of security. A robust and enterprise-wide awareness and training program is a key factor in employees understanding their IT security responsibilities, organizational policies, and how to properly use and protect the IT resources entrusted to them.

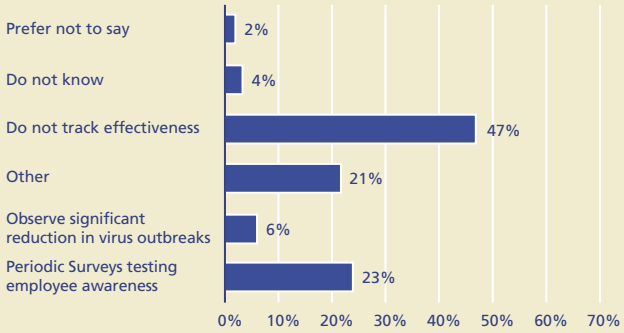
Difference between awareness and training

Awareness is not training. The purpose of "awareness" is simply to focus attention on security.

Training strives to produce relevant and needed security skills and competencies

Source: NIST SP800-16

Figure 22. Periodic testing of security awareness



Business continuity

Of the organizations studied, about one-fifth (22%) have a centralized business continuity management (BCM) operations model, where BCM development and execution are controlled from the central organization. Another 26% use a distributed model, where responsibility for BCM development and execution lies within business units. Another 37% follow a hybrid model, whereby BCM development is centralized and execution is distributed among business units.

According to respondents, a variety of executives are responsible for BCM. In approximately one-fifth, either a BCM executive or the CSO is responsible for the BCM function; for other organizations, the responsibility is managed by different functions.

Figure 23. BCM executive functions

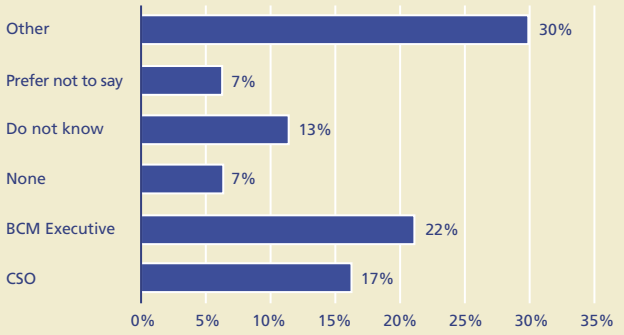
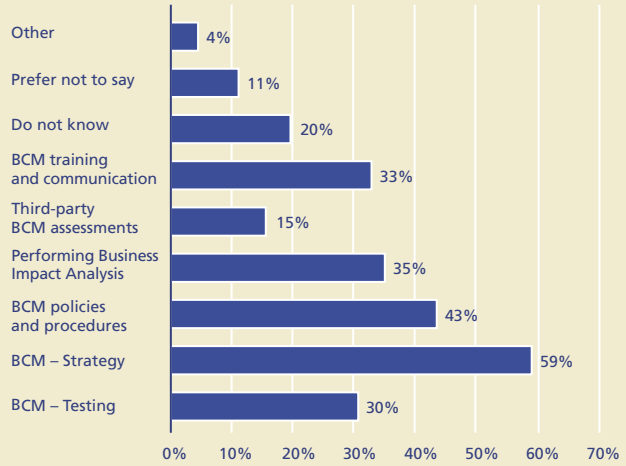


Figure 24. BCM responsibilities

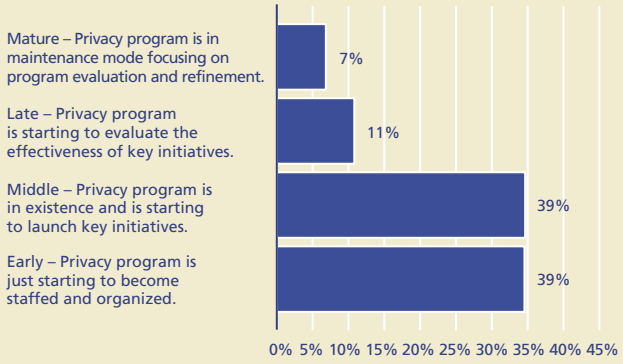


While operational resilience and fiduciary accountability remain key drivers, study results also identify regulatory compliance as a growing influence on management's decision to expand investment in BCM. Common responsibilities for the BCM position include developing BCM strategy, policies and procedures, business impact analyses, training and communication, and testing.

Data privacy

Organizations that use the personal information of individuals face the crucial task of maintaining strong controls over personally identifiable information (PII). This issue is made even more complicated by the fact that the relationship between information security and privacy protection disciplines is still largely undefined. Study results reflect this statement. Privacy is a relatively new function among the organizations studied and has a strong linkage to security in that there are data protection requirements for PII throughout the data life cycle. Only 22% of organizations have had a privacy function for three or more years.

Figure 25. Maturity of the privacy function



Consistent with these findings, organizations characterize the status of their privacy functions as "early phase" or "middle phase". Very few say their privacy function is in the "late" or "mature phase".

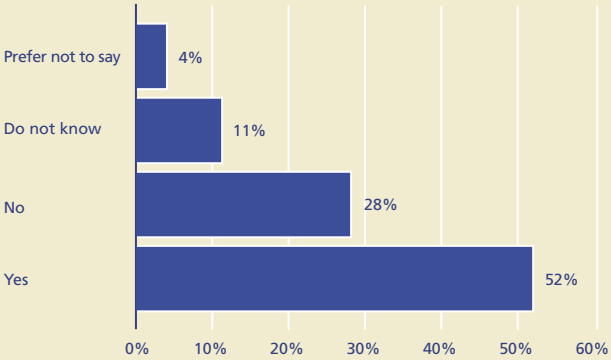
The emerging regulatory and compliance issues of privacy

The privacy issue is particularly relevant to the life sciences industry. Regulations in the US, such as HIPAA, mandate increased protection of patient medical records. Privacy regulations, such as those mandated by the federal government and enacted recently by California and over 20 other states, provide for stringent controls over financial data and public disclosure. On a global stage, privacy laws are even stricter than those in the US.

In order to bridge the privacy approaches between the EU and the US, and to provide a streamlined means for US organizations to comply with the EU Directive, the US Department of Commerce, in consultation with the European Commission, developed a "Safe Harbor" framework. The Safe Harbor — approved by the EU in July of 2000 — is an important way for US organizations to avoid interruption in their business dealings with the EU or to avoid facing prosecution by European authorities under European privacy laws.

The most commonly cited privacy responsibilities include responding to incidents (89%), developing privacy strategy (65%), reporting to management (65%), analyzing privacy regulations (63%), enforcing policies (63%), and conducting training and communications (57%).

Figure 26. Privacy programs



Of the two organizational models (centralized and hybrid) available to manage the privacy function, about 41% of respondents use a centralized approach and an approximately equal share (46%) use a distributed approach, where responsibilities lie within the business units.

More than half of respondents have a program for managing privacy compliance. Almost one third do not have an equivalent program.

About the study

Scope, questionnaire, data collection, analysis and participant profiles

The 2006 Life Sciences Security Study was designed with two purposes in mind: 1) to help respondents assess the state of information security within their own organizations; and 2) to allow executives to compare their organization's status with that of other life science industry institutions around the world.

Overall, the study attempts to answer the following questions:

- How do the security and privacy standards, practices and programs of individual organizations compare with those of the industry as a whole?
- How is the state of information security and privacy changing within organizations?
- Are the changes aligned with the evolution of the rest of the industry?

The 2006 Life Sciences Security Study reports on the outcome of focused discussions between security and privacy services professionals from DTT member firms and executives of top life sciences institutions; including not only security and privacy executives, but also other senior management. Discussions were structured to identify and record the present state of information security and privacy practices, with further focused discussions to gain the executive's insight on future needs of the organization and the industry vis-a-vis security and privacy.

Study scope

The study encompasses life science institutions that span the North America, Asia Pacific and European regions; in total 48 organizations from 10 countries are represented. To promote consistency and to preserve the value of the answers, the majority of these institutions were interviewed in their country of headquarters. The responding organizations consisted of biotech, pharmaceutical and medical device players. While industry focus was not deemed a crucial criterion in the participant selection process, attributes such as size, multi-national presence, and market share were taken into consideration.

Due to the diverse focus of institutions surveyed and the qualitative format of the research, the results reported herein may not be representative of each identified region. Also, due to the small sample size, the study does not present statistically significant data; however, the qualitative data gathered does permit us to understand directional trends and can serve as a vehicle for useful discussion. Notwithstanding that the study respondents total 48, over 90 percent of the major pharmas — those with revenue greater than $10 billion — are represented.

Survey instrument

The study consisted of a comprehensive set of questions developed by senior Deloitte & Touche LLP security and privacy services professionals in the US and Deloitte Research US. Questions were selected based on their potential to reflect the most important operating dimensions of a life sciences institution's processes or systems in relation to security and privacy. The questions were each evaluated for suitability, timeliness, and degrees of value.

The collection process

Once the questionnaire was finalized, the forms were distributed to the participating regions electronically. Data collection involved gathering selective quantitative and significant qualitative data related to the identified areas. In each participating region, senior members of DTT member firms security and privacy services practices conducted face-to-face interviews with the chief information security officer/chief security officer (CISO/CSO) or designate, and in some instances, with the security management team at the various life science institutions including "security steering committee" members such as Controllers, CFOs and other C-suite executives .

Results analysis and validation

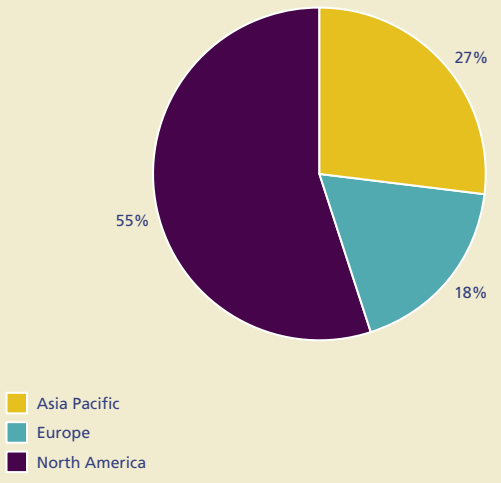
DeloitteDEX is a DTT family of proprietary products and processes for diagnostic benchmarking applications. The DeloitteDEX US team from Deloitte & Touche LLP was responsible for analyzing and validating the data from the study. The team used a variety of research tools and information databases to provide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

Additionally, professionals from Deloitte Research US assisted in the development of the study instrument, analysis of data, and creation of the findings in the study report.

Key participant demographics

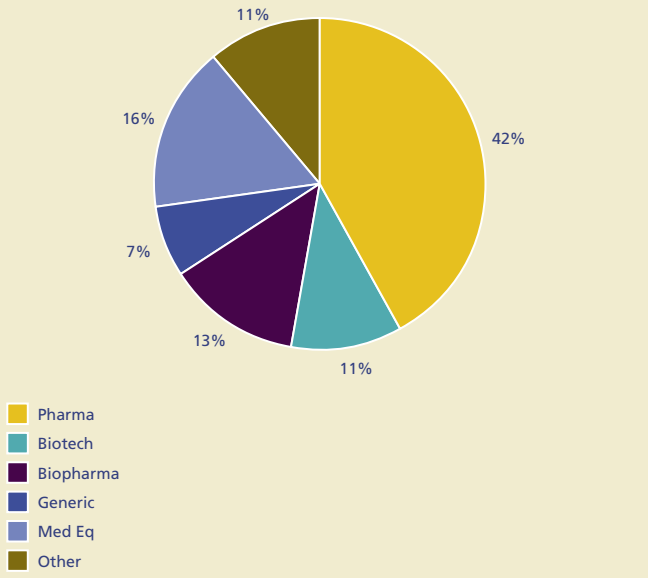
From a geographic perspective, the majority of respondent organizations were in North America, with Asia Pacific and Europe comprising the majority of the remainder, as illustrated in Figure 27.

Figure 27. Geographic participation



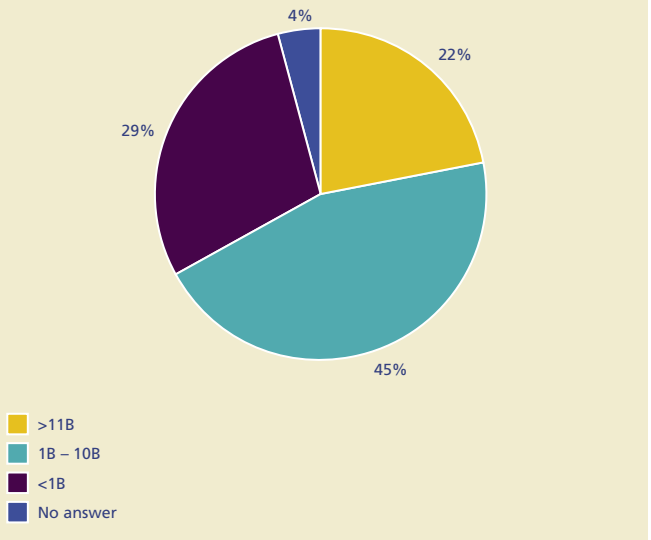
The pharma industry had the greatest participation, followed by biotech and biopharma (see Figure 28).

Figure 28. Industry participation



Participation in the life science study was greatest among organizations with revenues between 1B and 10B (45%).

Figure 29. Participating company revenues



Acknowledgements

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

Authors

Amry Junaideen
Terry Hisey
Russell Jones
Ash Raghavan
Suna Taymaz
Pam Williams

Contributors

Dr. Mike Breggar
Ted Dezabala
Clare Galloway
Christopher Lee
Adel Melek
Rena Mears
Pete Mooney
Jody Noon
George Serafin
John Rhodes
Steve Ross

Methodology, survey development and data analysis

Cabrini Pak
Deloitte Research
+1 617 437 3026
cabpak@deloitte.com

Olivier Curet
DeloitteDEX
+1 216 589 5448
ocuret@deloitte.com

Marc Mackinnon
+1 416 601 5993
mmackinnon@deloitte.ca

Marketing

Pamela Williams
Security & Privacy Services
+1 415 783 5719
pamewilliams@deloitte.com

Nicolas de Rooij
Security & Privacy Services
+1 416 601 5932
Nderooij@deloitte.com

Patsy Bolduc
Global Life Sciences
+1 213 688-4766
pbolduc@deloitte.com

Contacts

Global contacts

Robert Go
Global Life Sciences
and & Health Care Leader
+1 313 324 1191
rgo@deloitte.com

John Rhodes
Global Life Sciences
+1 973 683 7296
jorhodes@deloitte.com

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

Adel Melek
Global Leader for Security & Privacy
+1 416 601 6524
amelek@deloitte.ca

Amry Junaideen
Global Life Sciences
Leader for Security & Privacy
+1 203 708 4195
ajunaideen@deloitte.com

Life science & health care contacts

United States

John Rhodes
Life Sciences
+1 973 683 7296
jorhodes@deloitte.com

Terry Hisey
Life Sciences & Health Care
+1 215 246 2332
rhisey@deloitte.com

EMEA

Stuart Henderson
+44 1223 259392
stuhenderson@deloitte.com

APAC

Keiji Watanabe
+81 3 6213 3493
kewatanabe@deloitte.com

Security & privacy services contacts

United States

Christopher Lee
National
+1 408 704 4314
chrislee@deloitte.com

Ted Dezabala
New York
+1 212 436 2957
tdezabala@deloitte.com

Randy Conyers
Atlanta
+1 404 220 1463
Rconyers@deloitte.com

Mark Ford
Detroit
+1 313 394 5313
mford@deloitte.com

Raju Mehta
Houston
+1 713 982 2955
rmehta@deloitte.com

John Clark
Chicago
+1 312 486 3985
johclark@deloitte.com

Rena Mears
San Francisco
+1 415 783 5662
renamears@deloitte.com

Sean Peasley
Los Angeles
+1 714 436 7410
speasley@deloitte.com

Canada

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

Marcel Labelle
Montreal, Canada
+1 514 393 5472
marlabelle@deloitte.com

EMEA

Mike White
Johannesburg, South Africa
+27 11 806 5899
mikwhite@deloitte.co.za

Simon Owen
London, UK
+44 20 7303 7219
sxowen@deloitte.co.uk

Mike Madison
London, UK
+44 20 7303 0017
mmaddison@deloitte.co.uk

John Hall
London, UK
+44 (0)121 696 8653
johnrhall@deloitte.co.uk

Gerry Fitzpatrick
Dublin, Ireland
+353 1 417 2645
gfitzpatrick@deloitte.com

David Pike
Zurich, Switzerland
+41 44 421 6401
djpike@deloitte.com

Francois Renault
Neuilly, France
+33 1 55 61 61 22
frenault@deloitte.fr

Sven Hesselbach
Frankfurt, Germany
+49 (0) 69 75695 6449
shesselbach@deloitte.de

Asia Pacific

Uantchern Loh
Kuala Lumpur,Malaysia
+65 6216 3282
uloh@deloitte.com

Mitsuhiko Maruyama
Tokyo, Japan
+81 (3) 6213 1112
mitsuhiko.maruyama@tohmatsu.co.jp

Abhay Gupte
Mumbai, India
+91 22 5667 9405
agupte@deloitte.com

Latin America

Martin Carmuega
Buenos Aires, Argentina
+54 11 43204003
mcarmuega@deloitte.com

Life science and health care country leaders

Glen Sanford
Sydney, Australia
+61 2 9322 7230
gsanford@deloitte.com

Bob W. Leech
Toronto, Canada
+1 416 874 3229
bleech@deloitte.com

Jimmy Chan
Beijing, China
+86 (10) 8520 7750
jimchan@deloitte.com

Dominque Descours
Neuilly, France
+33 1 55 61 67 04
ddescours@deloitte.com

Thomas Northoff
München, Germany
+49 89 29036 8566
tnorthoff@deloitte.com

Joan O'Connor
Dublin 2, Ireland
+353 1 4172476
joconnor@deloitte.com

Kishore Kaushal
Delhi, India
+91 (11) 5562 2000
kaushalkishore@deloitte.com

Gerald Dekker
Netherlands
+31 10 880 14 35
GDekker@deloitte.com

Christopher Wellinger
Zurich-Oerlikon, Switzerland
+41 (0)1 318 71 11
cwellinger@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:

- Security Management
- Vulnerability Management
- Identity Management
- Application & Data Security
- Privacy & Confidentiality
- Business Continuity Management

Deloitte member firms offer knowledge and experience combined with national coverage and global reach. Combined member firm resources include over 600 Certified Information Systems Security Professionals (CISSPs) and access to technology solution sets developed through various long standing Deloitte Touche Tohmatsu and Deloitte member firm vendor alliances.

Item #6114

About Deloitte
Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, its member firms, and their respective subsidiaries and affiliates. Deloitte Touche Tohmatsu is an organization of member firms around the world devoted to excellence in providing professional services and advice, focused on client service through a global strategy executed locally in nearly 150 countries. With access to the deep intellectual capital of 120,000 people worldwide, Deloitte delivers services in four professional areas—audit, tax, consulting, and financial advisory services—and serves more than one-half of the world's largest organizations, as well as large national enterprises, public institutions, locally important clients, and successful, fast-growing global growth organizations. Services are not provided by the Deloitte Touche Tohmatsu Verein, and, for regulatory and other reasons, certain member firms do not provide services in all four professional areas.

As a Swiss Verein (association), neither Deloitte Touche Tohmatsu nor any of its member firms has any liability for each other's acts or omissions. Each of the member firms is a separate and independent legal entity operating under the names "Deloitte," "Deloitte & Touche," "Deloitte Touche Tohmatsu," or other related names.

Disclaimer

These materials and the information contained herein are provided by Deloitte Touche Tohmatsu and are intended to provide general information on a particular subject or subjects and are not an exhaustive treatment of such subject(s).

Accordingly, the information in these materials is not intended to constitute accounting, tax, legal, investment, consulting, or other professional advice or services. The information is not intended to be relied upon as the sole basis for any decision which may affect you or your business. Before making any decision or taking any action that might affect your personal finances or business, you should consult a qualified professional adviser.

These materials and the information contained therein are provided as is, and Deloitte Touche Tohmatsu makes no express or implied representations or warranties regarding these materials or the information contained therein. Without limiting the foregoing, Deloitte Touche Tohmatsu does not warrant that the materials or information contained therein will be error-free or will meet any particular criteria of performance or quality. Deloitte Touche Tohmatsu expressly disclaims all implied warranties, including, without limitation, warranties of merchantability, title, fitness for a particular purpose, noninfringement, compatibility, security, and accuracy.

Your use of these materials and information contained therein is at your own risk, and you assume full responsibility and risk of loss resulting from the use thereof. Deloitte Touche Tohmatsu will not be liable for any special, indirect, incidental, consequential, or punitive damages or any other damages whatsoever, whether in an action of contract, statute, tort (including, without limitation, negligence), or otherwise, relating to the use of these materials or the information contained therein.

If any of the foregoing is not fully enforceable for any reason, the remainder shall nonetheless continue to apply.

Deloitte
Touche
Tohmatsu