

COPING WITH CHANGE

SECURITY AND PRIVACY ISSUES

- Senior management involvement
- Mixed results from security awareness programmes
- Organisations adopting uniform standards and technology

The life sciences industry is under increasing pressure from a number of areas, which has huge consequences for security. Jim Banks asks Deloitte's John Hall and Mike Maddison what challenges the sector faces and how these can be overcome.



Contributors

John Hall is head of technology, assurance and advisory for life sciences at Deloitte, covering biotech through to public sector health. He has over 11 years' experience in the fields of IT operations, application development, project management, technology risk, information security and business continuity.

Mike Maddison, head of security and privacy services at Deloitte, has over 17 years' experience in the field of technology risk, information security, physical security, IT forensics and business continuity. He has been responsible for managing teams with corporate responsibility for all IT security consultancy, operations and policy.

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 life sciences industry. In order for organisations to achieve success, they need to 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 basis, need to be thoroughly understood and addressed for the organisation to compete successfully in its respective markets.

Risk management

The emerging picture for life sciences is one of an increasingly burdened industry prone to pressures from myriad sources.

Savvy and successful organisations are beginning to proactively pursue risk-reduction strategies to deal with the strains that threaten to disrupt business.

There are distinct advantages to integrating security and privacy risk management into the organisation's daily 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,' says Mike Maddison, head of security and privacy services at Deloitte.

Deloitte member firms surveyed a global representation of leading company executives (see graph, p5) in an effort to better understand the emerging issues surrounding security and privacy. Three key themes emerged from the findings.

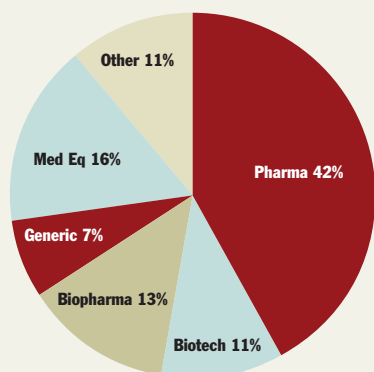
Security, information protection and data privacy are commanding greater attention from senior management and the board.

Increasingly, life sciences organisations are emphasising the proper 'tone at the top', adopting enterprise-wide views of security and embracing the protection of information assets. Although significant challenges remain, these organisations recognise the need to have an enterprise security programme led by a senior security professional, along with a strong governance framework for decision-making and delineation of accountability.

More and more life sciences organisations are appointing chief security officers (CSOs) or equivalent positions, with two-thirds of respondents having already done so. There is no leading organisational 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 cited strong support at an executive level, common obstacles to success include a 'buy in' at a business unit level, insufficient budgets and lack of qualified resources.

Creating an integrated security function by merging the physical aspects (corporate security office) with IT security is a goal for many, but it is not yet reality for most organisations. Less than one in three respondents indicate plans to merge the two functions or have achieved progress towards that goal.

Industry participation in Deloitte's security and privacy survey



'Businesses will need to efficiently demonstrate compliance across multiple jurisdictions.' John Hall

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

Organisations are achieving mixed results in implementing security and privacy protection programmes. Virtually all respondents have security awareness programmes with varying degrees of inclusion of employees, contractors, management and other executives, including board members. A number of respondents do not extend their awareness programme 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 programme.

Organisations cite the increasing sophistication of technology threats (for example, IT-based technical attacks) as a top security challenge and identify cyber-terrorism and maintaining privacy of customer data as lower priorities (see table, p6). 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 EU, North America and Asia Pacific countries is not going to occur in the immediate future. Instead, organisations 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 organisations operating in foreign markets.

'While the harmonisation of even common principles within privacy legislation is some way off, the importance of compliance is increasing,' says John Hall, head of technology, assurance and advisory for life sciences at Deloitte. 'One fact is certain; businesses will need to be able to efficiently demonstrate compliance across multiple jurisdictions.'

Organisations are adopting uniform standards and international frameworks and leveraging technology, all of which means they can 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 organisations. 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 solutions, and over 40 per cent will pilot smart cards in the short term. Many organisations are considering increasing investments in radio frequency identification tag (RFID) technologies. The companies surveyed 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 organisations. 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.

Organisations 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, organisations can do more with less. Top-down frameworks are more effective than bottom-up methods that give equal weight to risks of varying intensity – smart compliance is an opportunity to redefine and streamline business processes, increase operational efficiencies and reduce duplication of effort.

Security technology investment and ROI

So what is the state of technology as a solution to security problems? Identity and access management systems are currently entrenched, and organisations indicate plans to further utilise these technologies. The need to establish and safeguard a person's 'virtual identity' is obvious in today's virtual business environment.

Traditional security controls, such as 'real world' corporate boundaries, security firewalls and private access networks, no longer apply to the same extent. Organisations 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 organisation. If the external party's virtual identity is compromised, it is unlikely that a network firewall can

The increasing quality of technology is the top security challenge

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 and business partner misconduct	0%	50%	40%	7%
Cyber-terrorism (vicious code, malware, virus, etc)	0%	75%	22%	3%
Terrorism (not cyber)	17%	18%	45%	20%
Business continuity	2%	50%	40%	6%

prevent a potentially malicious user from gaining access to the organisation's assets. Perhaps in recognition of this risk, a third of the organisations surveyed plan to pilot single sign-on technologies (32 per cent) and/or access management systems (34 per cent) in the short term.

Few organisations 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 organisations that could measure their losses, damages ranged from less than \$1m to over \$20m.

Measuring the economic cost of security breaches is an area for improvement by life sciences organisations. 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 of reporting the breach to management and regulatory agencies, both from a personal and corporate perspective. Government regulations and industry standards are moving 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 organisations is mixed. Only 48 per cent report that all information assets in their organisation have identified owners, while another 28 per cent say that they are in the process of identifying such assets.

The weak link

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

a gap in their security programmes that makes conducting such analyses difficult.

Overall, relatively few organisations have effective processes to measure the return on security investments (ROSI) or other impact of their security programmes, 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 – for example, the tools and procedures in place that allow organisations 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 organisation – R&D, 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.

There is no one-stop or off-the-shelf security and privacy solution that fits all.

Future considerations

The competitive forces in the life sciences industry are compelling organisations to look at creative approaches to stay ahead of the competition, as well as to continue to produce strong shareholder returns. As such, organisations 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 a few bumps along the way.

'Information security is becoming recognised as a fundamental aspect of sound business practice and essential for safeguarding investment and intellectual property,' says Maddison. 'The protagonists are getting smarter, but the positive message is that many organisations in the sector are recognising the need to improve and are also stepping up their capability.' **END**