Trends and developments in cyber security and data protection: Why pharma and life sciences companies should take action

Life Sciences Spotlight

2 DEC 2015

Why should the pharmaceutical and life sciences sector place an increased emphasis on cyber security?

Pharmaceutical and life sciences companies are increasingly the target of cyber-attacks and cyber-espionage. Two key factors behind the increasing level of threat facing the pharmaceutical and life sciences sector are:

- The intellectual property – including drug formulas and manufacturing processes – held by organisations in the sector is incredibly valuable. Not only does a new drug or medical device have the potential to generate billions of dollars of revenue, but it is also expensive and time consuming to undertake the research and development required to generate that intellectual property.
- Organisations in the pharmaceutical and life sciences sector appear to lag behind those in the financial and utility sectors in implementing measures to protect against and mitigate the effects of cyber-attacks and cyber-espionage. Pharmaceutical and life sciences companies may therefore be perceived to be and targeted as the 'low hanging fruit'.

It is perhaps the case that organisations in the pharmaceutical and life sciences sector have seen themselves as holding relative limited amounts of personal information compared to banks, insurers, retailers, telecommunications service providers and utilities, and therefore considered that they face a lower risk of suffering 'privacy' and 'data protection'
breaches. However, the potential operational, financial and legal impact of there organisations’ intellectual property should cause the boards and management of organisations in the pharmaceutical and life sciences to come to grips with cyber security issues and invest in their systems, processes and procedures to manage these risks.

**What is the nature of the threat?**

The threat environment is not only increasing in terms of the volume of attacks, but it is also evolving and continues to encompass both external threats and internal vulnerabilities and actors.

For organisations that hold large amounts of valuable intellectual property and trade secrets, it is insiders rather than external hackers that pose the biggest threat — although nobody knows the true impact of insider theft, the general consensus is that company insiders are the biggest thieves of proprietary information. In 2012, a (former) trusted employee of DuPont pleaded guilty to stealing trade secrets concerning DuPont’s proprietary manufacturing process for titanium dioxide, the white pigment used in paint and plastics, which must by any measure be very valuable to DuPont.

**What about clinical trial data and monitoring data?**

While we noted above that organisations in the pharmaceutical and life sciences sector may hold lower volumes of personal information than some organisations in other industry sectors, it is nevertheless the case that they generally are still holding personal information are both trial participants and end users of products. In holding this type of information, organisations in the pharmaceutical and life sciences sector may be subject to legislative and regulatory requirements around the collection, storage, handling and disclosure of such information, which also raises the potential for regulatory and/ or civil actions in the event of breaches.

The level of regulatory attention on organisations’ cyber security measures and compliance with relevant data protection regimes is, in general terms, increasing globally – for example, new and enhanced privacy regimes in a number of Asian jurisdictions include the potential for significant fines and/or imprisonment as part of the mix of available sanctions for non-compliance. Coupled with this, increased media attention for large-scale data breaches has had an impact on individuals’ own level of concern as to how personal information is treated.

**Current trends and developments of relevance to the sector**

With that background in mind, we will explore below a handful of the current trends and developments in cyber security and data protection that are relevant to organisations in the life sciences sector with their valuable intellectual property assets and personal information.

1. **Mandatory breach notifications and worldwide complications**

Mandatory reporting regimes for incidents in which there is unauthorised access to and/or disclosure of personal information (data breaches) have been implemented in a number of jurisdictions and have increased the attention given to data breach incidents. It is arguable that without mandatory breach notifications, the massive data breaches experienced by Sony, Adobe, Target, Anthem and many others would not have become widely known until long after the breach occurred, if ever.

However, there is a growing perception that mandatory breach notifications may not be the panacea for the exposure of cyber-attacks and data breach incidents that it first appears to be.

There are concerns, primarily originating from the United States where mandatory breach notifications were first introduced, that the volume of breach notifications may desensitise society to the impact of all but the largest breach incidents. Smaller notifications may also get lost as background noise in the face of larger breach notifications.

Of far greater concern is the increasingly complex and differing notification regimes being implemented worldwide. In our experience, breach incidents often involve the data of entities from multiple jurisdictions. Identifying the jurisdictions and breach notification laws of each relevant jurisdiction as soon as possible after a breach incident is critical given the diversity of requirements imposed by notification laws across the world.

From our experience, notification requirements across the globe can differ significantly for even a relatively minor breach, with regulations in some jurisdictions stipulating that a minor breach amounts to criminal conduct, whereas no action may be required in other jurisdictions. The deadlines by which a breach needs to be notified also tend to vary by jurisdiction.
Cyber security has an inherently global dimension and the jurisdictions in which a company may face exposure is an often overlooked risk that companies do not properly consider. In fact, a 2015 Cyber Impact Report revealed that only 24 percent of respondents are fully aware of the consequences that could result from a data breach or security exploit in countries other than those in which their company operates.

We expect that the complexity and diversity of breach notification requirements across the world will only increase in the next five years. Indeed, breach notification requirements in the United States itself will likely become more complex in the near future on account of the anticipated introduction of Federal notification laws in addition to pre-existing state laws. It is and will increasingly be a major cost for companies. We cannot see there being any unification of breach notification laws across many countries in the near or long term future.

2. Cyber insurance as a standalone product and rapid response

Insurers are taking steps to ensure that cyber related risk is excluded from policies never designed to cover these risks. For example, many insurers are refining management liability policies to exclude cyber related incidents they were not designed to cover. Claims relating to electronic records and data are also being excluded from general liability policies.

Coinciding with this is the growth in specific cyber cover extensions for these policies (as opposed to stand-alone cyber policies). These products fit a current market demographic of insureds who are not yet willing to purchase a stand-alone cyber insurance product.

However, cyber cover extensions generally have limitations as to cover as compared to stand-alone products. This can include limiting the range of potential attacks covered, providing low policy sub-limits, or often limiting the heads/classes of loss as compared to a standalone policy – and the types of losses arising from a cyber-attack are very broad.

In addition, many stand-alone cyber policies provide a rapid response cover. The protection afforded by rapid response comes into play as soon as a cyber-attack has been identified. Rapid response cover can play a pivotal role in controlling the fallout from an attack and also limit the financial and reputational damage by controlling what happens in the first 48 hours after a company has identified it is under a cyber-attack.

The decisions made during this period will affect all future decisions and measures relating to the attack. This includes the protection of sensitive communications, how best to address the attack itself from an IT perspective (a brute force approach is often not the best approach) and the extent of notifications that need to be made (including the number of jurisdictions involved). In this respect, not all cyber-attacks result in a data breach incident (a common misconception).

Since the benefits of having expert teams to handle cyber claims in a consistent manner for all clients are significant we expect that the offering of access to a rapid response team will become a standard component of policies.

3. Increased legislative and regulatory focus

There are increasing legislative and regulatory pressure on organisations to ensure that they take “reasonable steps” that their data and systems are secure. Given the generally accepted view that the pharmaceutical and life sciences sector has a low level of preparedness and performance in relation to cyber security, this increasing regulatory focus should be of concern to organisations in the sector.

Australia’s corporate regulator, ASIC, noted in Report 429 (Cyber resilience: Health check), issued in March 2015, that effective corporate governance should involve active engagement by directors and the board in managing any applicable cyber risk and that directors may need to take cyber risks into account when undertaking their duties. While boards and directors have been aware of these issues for some time, the fact that ASIC expressly identified these issues in its report highlights that cyber security and information security are very much “front of mind” issues for corporate regulators in Australia and the Asia-Pacific region.

Listed entities are also subject to continuous disclosure obligations in relation to market sensitive information. Given the potential financial and reputational impacts of data breach incidents, the occurrence of a cyber-attack or data breach incident is potentially market sensitive information that must be disclosed under these continuous disclosure obligations.

4. A change in the nature of attacks

The current threat environment stems from the lack of attention that cyber security has received prior to the last few years. This has led to a volume of wide and varied vulnerabilities across many systems as businesses struggle with
making their systems more resilient. The resultant nature of cyber-attacks have been wide and varied, including ransomware, distributed denial of service, watering hole, remote access, phishing and malware attacks.

We expect that as consolidation and standardisation of security tools and systems increases over the next six to eight years, cyber attackers will focus their attention on identifying and attacking vulnerabilities within these “standard” tools and systems so that they maximise the potential number of targets.

An example of this is the exploitation of the Heartbleed vulnerability (which affected systems that used OpenSSL, a secure networking protocol) that was identified in April 2014. The vulnerability was exploited en masse within hours of its release, before a fix had been developed or could be applied. The risks posed by these exploits in “standard” tools and systems are exacerbated by the slow responses of organisations to address them – in the case of Heartbleed, approximately 84 percent of Australian businesses had yet to fully address the vulnerability 12 months after its release.

There will always be targeted attacks on high profile businesses. However, it might be the case that cyber attackers move from attacking a range of different, high profile targets to attacking many organisations, large and small, based on a newly released vulnerability.