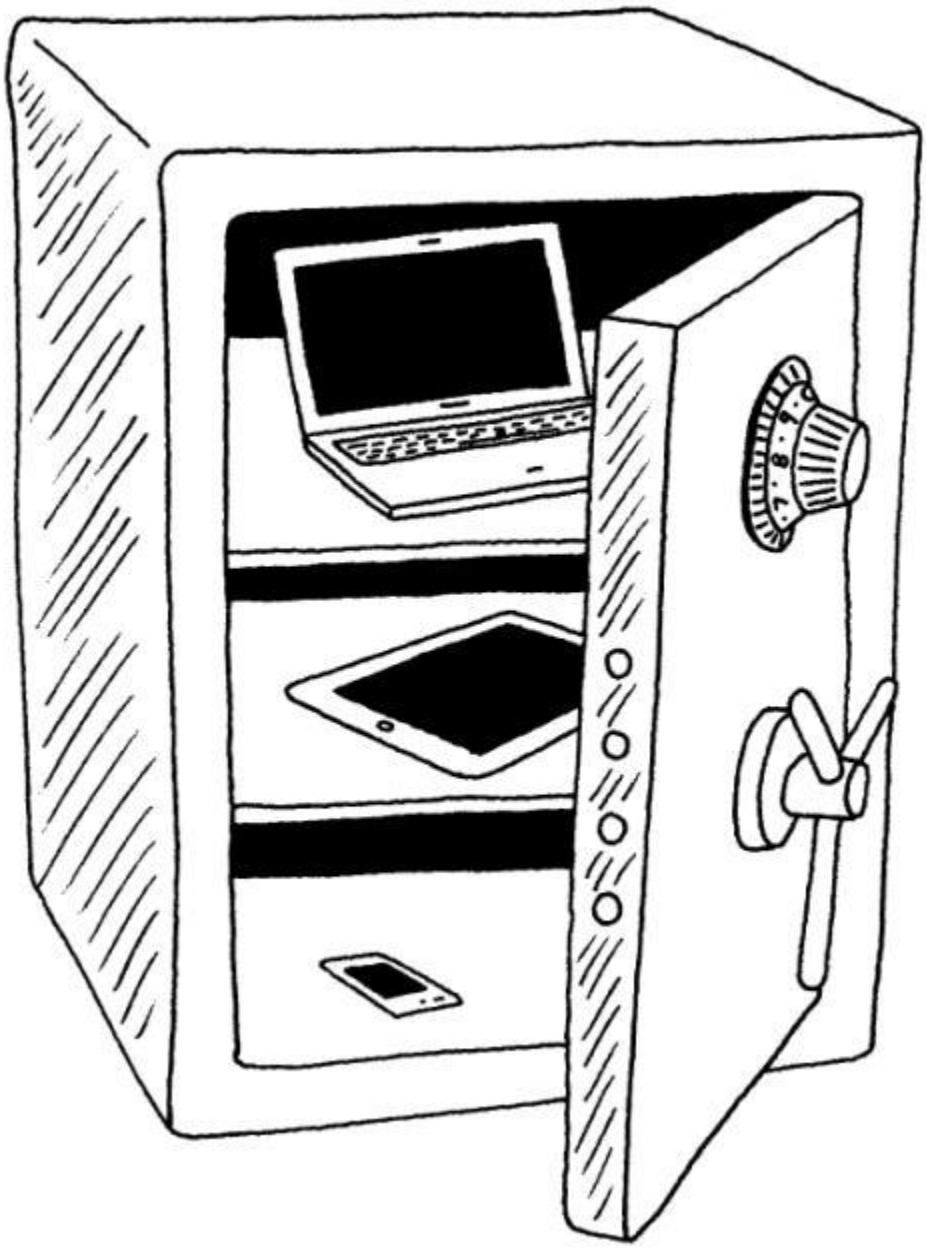
Insurance Coverage for Data Storage in the Pharmaceutical Industry

Jillian Raw, Partner, Kennedys Law LLP



Pharmaceutical Industry a top cyber attack target

Cyber risks are an ever present and ever increasing risk. There is no absolute protection model that can keep pace with the evolution and sophistication of cyber attacks. Every industry is at risk; although some are more at risk than others. One industry that remains a top target for cyber attacks is the pharmaceutical sector. A 2015 survey by Crown Records Management, a global consulting service, revealed that nearly two-thirds of pharmaceutical companies have suffered serious data breaches while a quarter have been hacked. The fact that pharmaceutical and life science companies are increasingly a top-target of cyber attacks is unsurprising. This sector holds highly valuable intellectual property and data from the research and development of new drugs and medicines. Cyber attackers are targeting drug discovery programs, drug registration applications, molecular formulae, patient records and clinical developments programs. The loss of intellectual property trial data can lead to significant losses to a company. The compromise of clinical trial data can also affect consumer confidence and expose confidential data about the subjects leading to costly litigation. Indeed, the 2015 Ponemon global study on the costs of cyber crime revealed that the pharmaceutical sector had one of the highest levels of data breach costs.

New European Union General Data Protection Regulation ("GDPR") and Brexit

Pharmaceutical companies store vast amounts of personal data, and so data regulatory laws are particularly relevant to their business operations. After almost four years of negotiations, GDPR was published as Regulation 2016/679 on 27 April 2016, and will apply for all member states from the 25 May 2018.

Following the referendum result of Brexit, the Information Commissioner's Office (ICO) has been keen to confirm that *'the Data Protection Act remains the law of the land'* until it is repealed or amended but in the event that the UK is not part of the European Union, given the referendum result, the *'upcoming EU reforms to data protection law would not apply to the UK'*. However, the ICO has gone on to say that "*if the UK wants to trade with the Single Market on equal terms we would have to prove 'adequacy' [in respect of data protection legislation] -in other words, the UK data protection*

standards would 'have to be equivalent to the EU's General Data Protection Regulation framework".

It thus appears that the ICO considers it necessary to push forward with reforms of UK data protection legislation, which will mirror the provisions of the GDPR. Consequently companies, and in particular UK pharmaceutical companies who store personal data will need to continue to plan for the implementation of legislation similar to the GDPR.

Cyber Insurance- a vital pill for the Pharmaceutical Industry

For pharmaceutical companies the security and integrity of data storage is thus a key concern. No matter how advanced or sophisticated a company's IT security systems are, or how thorough the vetting of a company's vendors may be there will still be data breaches or network security failures as cyber attackers become ever more advanced. Cyber is a risk that cannot be eliminated. It can result in significant losses not only by reason of the loss of IP assets and claims arising from data breaches but with the changes being brought into effect by the new data protection regulation the amount of the fines for data breaches that can be levied are significant.

Insurance has long been a means by which an entity's exposure to a risk is transferred or mitigated. Given the prevalence of cyber attacks and the significant potential losses that can arise from an attack one would expect there to have been a surge in in the number of organisations who are purchasing bespoke cyber insurance cover. Not so. A 2015 report by the Corporate Executive Programme found that only 13 % of large and mid-sized companies in the United Kingdom have bespoke cyber insurance policies. The reason for this is that many organisations are of the view that their existing insurance polices will cover their costs arising from a security breach or network failure.

However, many traditional lines of insurance might not respond or fully address the types of loss or circumstances of the loss that arise from a data security breach or a cyber attack. For instance, data breach notification and regulatory costs would not be covered. A traditional policy might not extend to cover loss of data that is stored by a

third party vendor in a Cloud. There is also considerable uncertainty and debate whether data constitutes tangible property to trigger cover under a traditional property or liability policy. In the United States this has given rise to a body of case law that is not uniform on the issue.

Many insurers are also excluding cyber risks from traditional forms of cover and, in particular, are excluding claims arising out of the loss of software, data or other electronically stored information. Such exclusions are usually comprehensive; for instance, cover is often excluded for *"loss, damage, destruction, distortion, erasure, corruption or alteration of electronic data from any cause whatsoever (including but not limited to computer virus) or the loss of use, reduction in functionality, cost, expense of whatsoever nature resulting therefrom."*

As a result of these developments and uncertainties the need for companies, in particular pharmaceutical companies, to purchase bespoke cyber insurance policies is essential.

What does Cyber Insurance Cover?

Cyber policies have developed generally to offer both first-party and third party coverage.

First party policies generally provide coverage for:

Crisis Management. This covers the costs that are typically incurred following a breach incident being regulatory costs, the costs of credit monitoring services, forensic investigation and public relations costs.

Digital assets. This covers the costs associated with the recreation, restoration and repair of damaged or destroyed electronic data and software.

Cyber Extortion. This covers expenses associated with cyber extortion or the threat of cyber extortion such as payment of the ransom to prevent a data security breach or to restore access to data.

Network Interruption. This covers the loss of business income caused by the failure of the insured's computer systems.

The extent of first party cyber cover continues to evolve to match emerging technologies. For instance, and particularly relevant to the pharmaceutical industry (with their increasing use of the Cloud for data storage) is the creation of Cloud Failure extensions to respond to the migration to the Cloud and the exposure of contingent business interruption. Many cyber policies also include in the definition of the insured's computer system a third party computer or system used to access the insured computer system or data.

Third party cyber policies provide coverage for losses related to the policyholder's liability to third parties caused by a cyber event. These policies typically provide cover for:

Privacy liability. This covers liability (including defence costs) arising from data breaches and other failures to protect confidential or personal information. Most cyber polices provide cover for fines or penalties imposed by regulatory bodies to the extent insurable by law.

Network Security Liability. This covers third party liability arising from a security threat to a network. For instance, if the insured transmitted malware to a third-party network.

Media Liability. This covers third party liability arising from the infringement of copyright or intellectual property rights as well as defamation or other tort disparagement of character or reputation arising from multi-media activities.

In addition to these covers many cyber insurers are partnering with specialist IT security providers to assist companies in evaluating and augmenting their data security and cyber resilience. Such front end, pre-breach loss prevention services may include: (i) infrastructure vulnerability scanning, (ii) cyber security risk assessments, (iii) the generation of third-party vendor security ratings, (iv) the isolation and shinning of malicious IP addresses and (v) online employee education and training. These preventative tools can provide an additional line of defence in the prevention and mitigation of cyber attacks and data security breaches.

What is not covered

The vast majority of cyber polices exclude three key types of loss: (i) property damage, (ii) bodily injury (except for mental anguish and distress) and (iii) loss of the company funds, which is usually the domain of Commercial Crime policies.

A policy will also not cover betterment. For instance, following a data breach or security incident the policy will not cover costs to repair or replace or restore the insured's systems to a level beyond that which existed prior to the claim or loss. Given that technology is constantly changing, and it is often difficult to match pre-existing IT systems, this might be an issue that could give rise to disputes.

At present cyber policies respond to claims in relation to data that arise as a result of negligence, for instance, the loss of a laptop containing personal data. However, it is important to note that many insurers in the US are starting to include revised language in their policies that only covers losses from theft of data not negligence. Since negligence still accounts for close to one third of cyber data breaches policy wording that excludes cover for negligence could prove disastrous for a company that has suffered a data security breach.

An issue likely to give rise to disputes under bespoke cyber policies is the insured's compliance with maintenance of technology conditions. These conditions are common in many cyber polices. These clauses can take various forms. For instance, an insured

may be required to "*to take reasonable steps to use, design, maintain and upgrade your security.*" Other such clauses require an insured to take a number of listed reasonable steps at its own expense to prevent an insured event arising. Such type of clause is the subject of one of the first coverage disputes in the US involving a bespoke cyber insurance policy: Columbia Casualty Co v Cottage Health System USDC Case No 2:15 03432. In May 2015 Columbia Casualty commenced declaratory proceedings against its insured, Cottage Health Systems, seeking reimbursement of the settlement funds totaling $4.2m, which it had paid under a reservation of rights following a settlement of a data breach class action lawsuit. Columbia Casualty sought a declaration that coverage was barred by a failure to continuously implement its cyber security controls identified in the insurance application prior to the inception of the policy.

Cottage Health Systems had submitted a "Risk Control Assessment", which required it to respond to specific questions about *inter alia* security patches, threat assessments, audits of third party vendors and other cyber security patches. It had responded "Yes" to each of the application questions although it appears that it did not implement many if not all the security measures. A data breach of medical records occurred because it had failed to install encryption or take other cyber security measures to protect patient information. As a result, medical records were fully accessible to the public via Google searches.

The outcome of the case has not been determined, as the litigation has been moved to a compulsory ADR process. But the initiation of proceedings by insurers signals that cyber insurers may be willing to test an insured's compliance with the policy required cyber security systems and practices.

Some commentators argue that maintenance of technology conditions are open-ended, and that they can be overly broad. But against that is the argument that such conditions are essential to try keep pace with the evolving threat created by hackers and are an essential part of the bargain of underwriting a cyber risk. In the UK with the changes brought about by Section 11 of the Insurance Act 2015 such clauses might give rise to future disputes. Briefly put, Section 11 is intended to prevent an insurer from relying on

a breach of a term by the insured if that breach is not connected with the actual loss suffered. Thus, where there is non-compliance with a maintenance of technology condition an insurer will not be able to rely on that non-compliance as a defence if the insured can demonstrate that such non-compliance could not have increased the risk of loss that actually occurred in the circumstances in which it occurred. For example, where there is a requirement in the policy to change passwords every three months and that is not done insurers are unlikely to be able to refuse indemnity on that ground for a loss of data that arises from a software update. In the *Columbia Casualty* case, *supra*, the loss arose because the insured failed to follow a condition that required it to encrypt its servers. In that case there is a connection between the insured's breach and the loss and the circumstances in which the loss occurred.

Cyber Coverage disputes: the future

Common wisdom has been that as the cyber insurance market plateaus and claims arising from loss of data become more prevalent and costly, insurers might begin to resist coverage and push back more on claims. That appears to be the trend that is emerging in the US at present following a surge in data breach claims.

One of the reasons why we can expect cyber insurance coverage disputes to arise is that cyber policy wordings are still developing; there is at present no standard form wording. The wordings are untested. Coupled too with the ever changing nature of cyber threats we can expect that insurers and insureds will present, and will face a number of interesting arguments, that will help develop a body of cyber insurance coverage law.

How much Cyber insurance coverage is necessary?

While there is no simple answer to the amount of cyber insurance that a company should buy some important factors include the size of the insured entity, the amount of sensitive data stored, the extent to which the company is exposed to cyber threats and the value of the company's data to its business operations.

Pharmaceutical companies will score high on each of these factors. As these companies rely more and more on computer systems to store their valuable data they will need to constantly evaluate not only that they are purchasing the right type of cyber coverage to reflect their business operational needs and exposures but also that they are purchasing the right amount of cover.

Jillian Raw leads Kennedys Global Cyber Offering