Insurance Coverage for Data Storage in the Pharmaceutical Industry

Richard Eveleigh*

The Main Concerns

The disclosure, loss or corruption of data kept by a pharmaceutical company gives rise to concerns of both the company's own first party loss and its liability to third parties. The same is true for most organisations, but types of data of particular worry to a pharmaceutical company are:

(i) sensitive and medical information about individuals compiled through clinical trials or through data legally harvested from medical bodies;

(ii) the company's own proprietary and confidential information, such as product formulas, manufacturing processes, product pricing, marketing plans and strategies;

(iii) proprietary and confidential information belonging to other organisations held by the company because it is in some collaboration with such other organisation (which may, for example, be another pharmaceutical company, a university or a research institution).

Concerns are now accentuated for the first of these by the coming into force of the European Union's General Data Protection Regulation in May 2018, in particular by its compulsory notification requirements for unauthorised disclosure of personal data and by its requirements relating to "special categories" of personal data including data about racial or ethnic origin, health, sex life or sexual orientation.

Growth of Cyber and Data Insurance

The most responsive type of insurance to the range of concerns raised by storing such data is "cyber insurance". Cyber insurance first appeared circa 2000 and was originally developed as a product for financial institutions. Over the next ten years very little of it was sold and towards 2010 insurers dusted off their old wordings and revamped them for marketing to all types of organisation. Since then sales have greatly increased, fuelled by the high profile data breaches of recent years and all the publicity that now surrounds the subject of "cyber".

Protection Provided

A typical cyber insurance policy covers a range of first party losses, third party liabilities and crisis expenses, some of which could only arise through the involvement of a computer system and some of which could arise in some other way but which in the particular event happen to involve a computer system. Cyber insurance is not just about data. It is about computer systems. Data storage is just one of the aspects about a computer system which a cyber policy deals with. This article is about data storage, but there are other losses and liabilities which a cyber policy can protect against:

* Richard Eveleigh, BILA Committee member.

- an organisation's liability for an attack on its system causing damage to a third party's system, eg the passing on of a virus;
- liability to customers for their inability to access the organisation's system due to a denial of service attack on that system, so particularly relevant to banks and retailers where customers are denied access to web services;
- liability for defamation committed via the organisation's computer (eg on its website) or for breach of privacy or rights to name or likeness committed via computer;
- an organisation's liability for intellectual property infringement through transmitting or displaying information via computer (eg a copyright breach on its website);
- business interruption: first party insurance for loss of profit and extra expenses arising from interruption caused by fraudulent access to the organisation's computer system;
- (usually for financial institutions only) first party insurance for an institution's losses through fund transfers caused by fraudulent inputs to computer systems or fraudulent modifications to electronic instructions).

Arguably the most important aspect of cyber policies and the one of most interest to potential customers (including pharmaceutical companies concerned about data storage) is the third party liability cover for wrongful data disclosure. Different insurers will give it different names, and for example, you might find it called "Data Disclosure Damage" or "Privacy Damage". This indemnifies an organisation for liability arising from someone obtaining unauthorised access to its data. Originally, cyber policies would only respond if this was access to data held on a computer, hence it was very much a "cyber" issue. But recent changes see insurers covering such access however obtained and wherever the data is stored. This could include the physical theft of a CD Rom or memory stick, or even the theft of good old-fashioned paper containing data. It means cover is no longer restricted to hacking or leak by computer, but now includes the clumsy loss of data by, for example, leaving something on a train.

There are many incidents involving clumsiness (see for example the enforcement pages of the UK Information Commissioner's Office website). It is a major risk for organisations, just as actual hacking is, and one for which insurance response was needed. Hence the removal of the computer restriction which has increased demand for the policies and is leading to an increased use of the term "data breach insurance" in place of "cyber insurance", as there is cover for data breaches of a non-cyber nature. To be pedantic, the full description of a policy should perhaps be "cyber and data breach insurance".

Data Disclosure Damage – The Data

Crucial to the cover for Privacy Damage / Data Disclosure Damage is the definition of the data, disclosure of which is covered. Until fairly recently, an insurer's definition of "Data", "Information" or "Records" (whichever expression it might use) would include two typical elements:

- two types of information about natural persons, being *identity information* (a name combined with a number such as a national insurance number (UK), social security number (USA), national health

number, driving licence or passport number) and *financial account information* (for example, bank details, medical insurance details, credit or debit card details);

- employee records and information.

Whilst a pharmaceutical company will have employee records and may also have identity information of natural persons outside the company (but less likely hold such persons' financial account information), these components are of greater help to banks and retailers and are not a strong solution to the dangers of holding clinical trial and medical information. However, insurers moved on to include a third element:

- sensitive personal data, non-public personal information, personally identifiable information, medical and health information.

Subject to any debate about the precise words used by the insurer, this provides the important third party liability cover needed by a pharmaceutical company for wrongfully disclosing personal medical information obtained through clinical trials or data harvesting. The change also improves cyber/data insurance for hospitals, doctors' surgeries, health authorities and other healthcare organisations wanting the insurance.

A fourth, quite recent element is:

- another organisation's non-public information (including trade secrets, data, designs, forecasts, formulas, practices and processes) in the care, custody or control of the insured organisation or provided to the insured organisation under a written confidentiality obligation.

It was mentioned above that a pharmaceutical company may store proprietary and confidential information belonging to other organisations because it is collaborating with them (for example, another pharmaceutical company, a university or a research institution). This may include product formulas, manufacturing processes, product pricing, marketing plans and strategies. The insured company faces the danger of liability to its collaborator if such information is accessed by unauthorised persons who make illegal use of it. The recently added fourth element helps the insured in this regard.

Data Disclosure Damage – Covered Liability and Costs

As is typical for most third party liability insurance, the Privacy Damage / Data Disclosure Damage cover and the other third party liability covers of a cyber/data insurance policy should include cover for defence costs, damages and settlement sums. But, with regard to wrongful data disclosures, there will usually be additional covers:

(i) cover for fines imposed by regulators; and

(ii) cover for redress funds (money which a regulator requires the insured to pay into a fund for the payment of consumer claims arising from the disclosure)

to the extent that they are insurable. Whether regulator fines are insurable will vary from jurisdiction to jurisdiction and even from regulator to regulator.

Other covers relating to wrongful data disclosures are crisis management expenses and notification costs. Crisis management expenses should include legal and public relations advice and the costs of technical investigation into how the data breach occurred.

Notification costs (including the costs of setting up call centres) are now seen as a crucial feature of a cyber/data insurance policy. With many persons possibly affected, the cost of notification can be hugely expensive and the major part of the organisation's losses. Cover for the costs would typically include, beyond merely notifying the persons, the cost of changing their financial account numbers and security codes and the cost of providing them with credit monitoring to help against fraudulent use of their financial details.

Data Breach Response Services

Beyond the mere payment of notification and crisis management costs, a number of insurers provide a breach response service by having in place a range of professional advisers and the necessary physical infrastructure to mitigate damage when an insured organisation suffers a breach. Large pharmaceutical companies may already have their own crisis advisers and infrastructure in place. When buying a policy, there is much to be said for the insured to discuss with its insurer which services will be called upon and, if the organisation would wish to rely mainly on its existing infrastructure, to make sure that the costs of that are something that the insurer agrees are covered. In any event such conversation should lead to insurer and insured drawing on each other's knowledge and to both parties efficiently and swiftly acting together if and when there is a data breach.

Cyber Extortion and Cyber Vandalism

Cyber/data insurance policies typically contain two first party covers of relevance to data storage: extortion and vandalism. The former is cover for ransom paid in response to a threat to disclose, damage or destroy computer-held data or impair computer services. The latter is cover for the costs of reconstituting computer-held data which has been altered, damaged or destroyed by an attack on the system.

Data and Proprietary Information in Pharmaceutical Companies

So what protection does a cyber/data insurance policy provide for data of particular concern to pharmaceutical companies?

First, sensitive and medical information about individuals compiled through clinical trials or through data legally harvested from medical bodies. The company's risks include accidentally disclosing that information to the wrong person, accidentally making it available to the public at large or having unauthorised persons maliciously obtain access to it. Such events could lead to liability claims by the individuals, obligations (moral or legal, depending on jurisdiction) to notify individuals (perhaps many of them), fines by regulators or criminal proceedings. For such claims, proceedings and actions, cover for defence costs, civil liability and insurable regulator fines should come from the privacy damage / data disclosure damage cover of a quality policy. Such a policy should also pay the costs of notifying the individuals. Given the potentially huge liabilities and costs in the case of major breaches involving many individuals (perhaps more likely in the banking, retail and telecoms sectors than in pharmaceuticals), it will be difficult for any purchaser of cyber/data insurance to know that the insurance will always cover the entire loss. It is important for a pharmaceutical company to check that the policy's definition of covered data/records includes sensitive personal data, non-public personal information, personally identifiable information, and medical and health information.

A related risk for the company from unauthorised disclosure or access is damage to reputation, potentially of very large value but difficult to quantify. Whilst, via notification and crisis management costs, a cyber/data policy assists in minimising reputational damage, a policy does not typically include cover for the value of the damage. So a company might wish to find separate reputational damage insurance, but this is a slowly evolving product in the insurance market and not one which is easily available.

Secondly, the company's own proprietary and confidential information such as product formulas, manufacturing processes, product pricing, marketing plans and strategies. Unauthorised access to this information by those wishing to use it for themselves or destruction by malicious hackers will be a first party loss for the pharmaceutical company. To the extent that this information is the subject of a threat to access or destroy it by cyberattack or hack or that it is actually damaged by cyberattack or hack, the above-mentioned extortion and vandalism cover will be of some value. If the damage brings operations to a halt, the policy's business interruption cover may respond to the loss resulting from that.

Should unauthorised access lead to others using the company's know-how with consequent damage to the company's growth and profits (possibly even its existence), this is unlikely to be something covered by a cyber/data policy. This suggests the need for a policy which generally protects against theft and infringement of intellectual property and proprietary information. Perhaps, surprisingly, this cover is not widely available or well developed, whether as an individual policy or as an add-on to other commercial policies. There are some products which provide the costs of pursuing infringers in cease and desist actions but there seems to be very little by way of insurance for loss of profit attributable to infringement. It also seems that, whatever first party intellectual property insurance can be found, the appetite of insurers does not stray far beyond insuring small research and development organisations.

Thirdly, proprietary and confidential information belonging to another organisation held by a pharmaceutical company because it is collaborating with that organisation (which may, for example, be another pharmaceutical company, a university or a research institution). The company's concern is one of third party liability to the collaborator and it is important for the insured to check that the definition of covered data/records contains the following language more recently introduced to cyber/data policies: another organisation's non-public information in the care, custody or control of the insured organisation or provided to the insured organisation under a written confidentiality obligation. If it does, then the policy should protect the company for claims by the collaborator arising out of a privacy/data disclosure wrongful act.

It is interesting that, whilst insurers do not rush to offer loss of profit insurance for intellectual property infringement, they are indirectly exposed to such loss where it forms part of a claim against an insured by a collaborator whose intellectual property has been infringed through access to it on the insured's systems.

Underwriting the Risk

In underwriting cyber/data insurance for pharmaceutical companies, insurers look closely at the safeguarding of corporate records (particularly records of know-how, intellectual property and pricing) and of clinical trial records. They are cautious about pharmaceuticals but generally expect to find good controls, good business continuity plans and good crisis response plans. Proposal forms and processes are detailed and searching and questions about such controls and plans will be raised. The pharmaceutical sector seems generally regarded as better

structured and lower risk than the healthcare sector, particularly the state funded (or insufficiently funded) healthcare sector such as the UK's National Health Service.

For pricing for cyber/data insurance, insurers tend to take an organisation's revenues as a starting point. But many other risk factors will come into play. Such as:

- types of information held, how sensitive and private;
- how many individual records held, and how many people potentially to notify in the event of a data breach;
- staff training, access restrictions, the "human firewall";
- outsourcing, where storing and who with, ability to impose own security conditions on the large storage companies;
- storage on mobile devices;
- likelihood of being targeted by protesters (eg animal rights activists);
- likelihood of being a victim of foreign state sponsored hacking;
- likelihood of being targeted for industrial espionage, the commercial value of proprietary information held;
- holding of third parties' information, whether collaborators or perhaps takeover targets during a due diligence process.

As stated, insurers hold pharmaceutical companies in good regard. Such companies are inherently quite high risk but they are generally regarded as being professional in their handling of data. This is contrary to public sector healthcare – see the enforcement pages of the UK's Information Commissioner's Office website which shows a good number of healthcare data breaches. It seems similarly in the USA that breaches in the healthcare sector are far more numerous than in the pharmaceuticals sector. Breaches amongst the pharmaceutical companies seem few. An example is the case of Akorn Inc of Illinois in 2015 where it was claimed that 50,000 individual records were compromised by a hacker who is boasting of it on Twitter under the name of Mustafa.

Directors and Officers Liability Insurance

This article has focused on cyber/data insurance, certainly the most relevant to insuring the concerns discussed even if, as mentioned, there can be overlap of some of the features of such insurance with other types of policy. A few words should be said about directors and officers liability insurance ("D&O"), generally applicable in the event of actual or alleged shortcomings of directors.

If a company suffers its own first party data or cyber-related losses or is sued for a "cybertort", the company or its shareholders might sue the directors or the IT manager for the consequent damage to the company's value. The directors or IT manager may also face regulatory investigation or possibly criminal proceedings. The company's D&O policy would normally be expected to provide these individuals with defence and representation costs and cover for any civil liability. Whilst a number of years ago the pharmaceuticals sector was regarded as one of the "sickly six" sectors to insure, this was because of the economic uncertainties of the sector, particularly the danger of disappointment to investors regarding failed products, rather than because of danger regarding data.

“Cyber”?

Finally, “cyber”, where does the word come from? Following his creation of a flight path predictor machine during the Second World War, Norbert Wiener wrote “Cybernetics or Control and Communication in the Animal and the Machine” in 1948. “Cybernetics” derived from the ancient Greek “cyber” meaning “steer”, “navigate” or “govern”. Wiener was a polymath interested in biology, philosophy and mathematics who, along with his colleagues at the Massachusetts Institute of Technology, Vannevar Bush and J.C.R. Licklider, is regarded as a key figure in the origins of the Net.