Cyber Loss

The Non-Insurable Impact

Cyber losses can be classified into 2 basic categories: insurable and non-insurable. The first section considers the non-insurable; the following will consider the insurable losses.

In summary the non-insurable losses include:

1. Fines,
2. Reputational loss,
3. Impact on value of the company's share price,
4. Customer loss, and
5. Loss of employees.

Fines

Some losses are difficult to quantify, such as reputational loss where the true value may not be known for many months if not years, however, other losses are more obvious, such as fines levied by government agencies. In this respect, different international jurisdictions may impose fines for data protection violations and in this respect the United Kingdom may impose up to GB£500,000; Switzerland up to CH10,000; Mexico up to $1.5 million; Canada up to $100,000 and Hong Kong up to HK$1 million (based upon figure made available to the author).

Clearly, therefore, fines vary from country to country. Where there is a pre-determined level of fine such as shown above it is possible to assess this loss to a maximum level. However, some countries have yet to apply a predetermined level of fine where you may find yourself at the mercy of the court's leniency not bound by potential maximum fine.

In some countries the approach to fines is more sector specific rather than all-embracing and the USA has this approach.

Reputational Loss

Fines are only one loss area. As indicated above it may take time for an organisation to fully understand the loss suffered to its reputation as a consequence of a data breach.

Impact on the Value of a Company's Share Price

As to whether or not share prices are impacted over the long term would be difficult to assess and quantify, but it is thought and believed that the impact of cyber breach especially one attracting media attention will have at least a short term impact to some degree.

Customer Loss

To some extent, depending upon all the facts and size of the breach, some loss of customers would be a foreseeable loss. This loss would flow from the bad publicity attracted by the cyber breach. The real concern would flow from a substantial or meaningful loss which might hinder or even prevent an organisation from tendering for future contracts. This could be disastrous for some companies and its staff and their families.

Loss of Employees

It would be foreseeable for employees in professional organisations such as accountancy and law practices to lose their staff where professional people might not want to be associated with an organisation suffering from a major cyber breach. Professionals value highly their hard earned qualifications and such individuals would not want to suffer personal reputational damage by association. No-one wants to be collateral damage where it can be avoided.

Other Losses and Costs Flowing from Cyber Breach

Regulatory authorities may require an organization to take corrective action which could cost an organization dearly in terms of employee time in training costs and paying for the external trainers and courses.

The impact too, on intellectual property must not be understated, more so where companies rely heavily on their intellectual property. Ultimately for certain companies any diminishment to their intellectual property could end up with a closure of the company with all its consequences for investors, customers and staff.

Overall, the impact of a cyber breach to an organization could be catastrophic especially to areas of the business where no protection can be given by insurance cover. It is essential, therefore, for an organization to introduce controls to reduce its exposure to loss.

The Insurable Impact

In summary the insurable losses include, but are not restricted to:

1. Forensics,
2. Investigation,
3. Customer notification,
4. Business Interruption,
5. Legal and defence, and
6. Crisis Management.

Insurable Risk

Data breaches can be innocent or sinister, but either way, the consequences for an organisation sustaining a breach can be costly if not catastrophic.

Breaches may arise by losing documents, devices such as cell/mobile phones and laptops or consequential to more sinister and malicious attacks to your IT systems from a number of sources, such as former or even existing staff, criminals out to steal your data and market competitors.

As illustrated in the previous section, "The Non-Insurable Impact", many costs and losses associated with data breach fall outside of the scope of insurance policies. However, specific insurance products have been developed which may include cover for those costs listed above.

Each of the items of cost listed can be highly expensive to an organisation and immediately post discovery of a breach the best practice and advice would be to look into the seriousness of the breach which should be fully investigated together with all related issues using both forensic skills and lawyers, and if appropriate PR agencies too. At some point, normally sooner rather than later, there may well be the need to notify customers. All of these costs can be covered by insurance policies. Any one of these steps standing alone can be expensive as illustrated below.

Although the losses and insurance issues are far to lengthy in detail, it would be useful and insightful to consider more specifically some of the statistics and costs involved.

Examples of Costs Arising from Data Breaches and Statistics of Loss

A 2013 study undertaken in the USA by NetDiligence made a number of findings which it is thought were accurate at the date of their own research. Their report summarised their findings from a sample of 145 data breach insurance claims where 140 of them involved the exposure of sensitive data in a number of sectors. Some of their key findings are:

1. Personally identifiable information was the most frequently exposed data (28.7% of breaches) followed by Protected health information (27.2% of breaches).
2. Lost/stolen laptop/devices were the most frequent cause of loss (20.7%) followed by Hackers (18.6%).
3. Health care was the sector most frequently breached (29.3%) followed by financial services (15%).
4. Small-cap ($300m0$2b) and Nano-cap (<$50m) companies experienced the most incidents (22.9% and 22.1% respectively).
5. Claims submitted for this study ranged from $2,500 to $20 million, where typical claims ranged between $25,000 to $400,000.
6. The median cost for legal defence was $7,500 where the average cost for legal defence was $574,984.
7. The median cost for legal settlement was $22,500. The average cost for legal settlement was $258,099.

NetDiligence's 2013 study shows that the leading cause of loss were lost or stolen laptops and devices (27.7%) and hackers (18.6%). Following closely behind were rogue employees followed by malware/virus then paper record.

The impact of data breaches reflects the growing need for organisations to focus more on this risk and to use and develop tools of risk management to reach a balance of the risk which is acceptable to the organisation and insurers.

Controls to Reduce Loss Exposure

Some reliance has been made in this paper to a publication issued by CESG (the information security arm of GCHQ) entitled "10 Steps to Cyber Security". The areas where loss arises extend beyond the 10 steps highlighted by CESG, however, these steps do encompass and consider critical areas faced by most organizations.

Briefly,

Putting in Place a Risk Management Regime

This can be divided into a number of areas, such as establishing a suitable governance regime, determining your organization's own risk appetite, maintaining your organization's top level engagement with cyber risk, producing your own management policies and embedding them into the working practices of your business.

Maintaining a Safe and Effective IT System

This may be achieved by developing corporate policies to up-date and patch your IT systems, to lockdown your operating systems and software, and to scan regularly to check for weaknesses.

Security of the Network

Make it secure by building defenses, firewalls, by protecting the internal network, by monitoring and auditing and regularly conducting penetration tests.

Manage Users

This would require management and selection of individuals authorized to use the operating and software systems and monitoring user activity.

Education

Users and operators of your systems need to be educated into your user policies and trained to be responsible.

Management of Incidents

Leadership should come from the top of your organisation developing and maintaining incident management plans where those involved with this management should undergo specialised training.

Malware

Your organization needs policies to reduce the risk of malware penetration.

Monitoring

Devise and put in place a plan to monitor systems and network traffic based on your own risk assessments.

Removable Media

Scan all removable media for malware, take control over what media types can be introduced to your systems and implement appropriate policies.

External Working Policies

A careful risk assessment is needed to devise and implement a policy and to educate both home workers and those on-the-move accessing IT equipment and software.

The issues raised in this paper are in outline and in a non-specific form where specific consideration of your organisation's own risks should be fully considered to produce the best practice for your needs and protections against cyber loss.

Gary Marshall, Solicitor in England and a Member of the Institute of Risk Management.

This article is a publication of Jorgensen & Company. It not intended to represent the opinions of any insurer or provide legal or other professional advice.