TalkTalk of the Town:

As cyber attacks increase in prevalence, what should we be doing to protect against them?

The recent TalkTalk hacking was the third time in 2015 that the telecoms firm has suffered a cyber-attack, leaving the data held on millions of their customers at risk.

Following several arrests, the investigation continues and it will take some time before the full details of what occurred are revealed. The direct cost of responding to the incident to date is in excess of £35,000,000 and this is anticipated to increase substantially.

As the incident exposed personal data, the Data Protection Act requires this to be reported. The reality is that cyber breaches are more common than believed but, where there is no legal requirement to disclose, they typically go unreported. This may soon change however, as the new EU Data Protection laws come into effect.

When it comes to implementing measures to protect yourself against having to explain to your own clients why their private and confidential information has been leaked, a quick Google search reveals dozens of 'top 10' lists and all have their merits. The picture that begins to form is that, short of unplugging your computer network from the internet, there is not much you can do to prevent hacking.

The most common security advice is:

- Use strong passwords: a combination of uppercase, lowercase, numbers and punctuation. Each account must have a unique password – do not use the same password for multiple accounts.
- Install security software: software such as antivirus helps protect your device from viruses and hackers.
- Download software updates: updates contain vital security upgrades which help keep your devices secure.

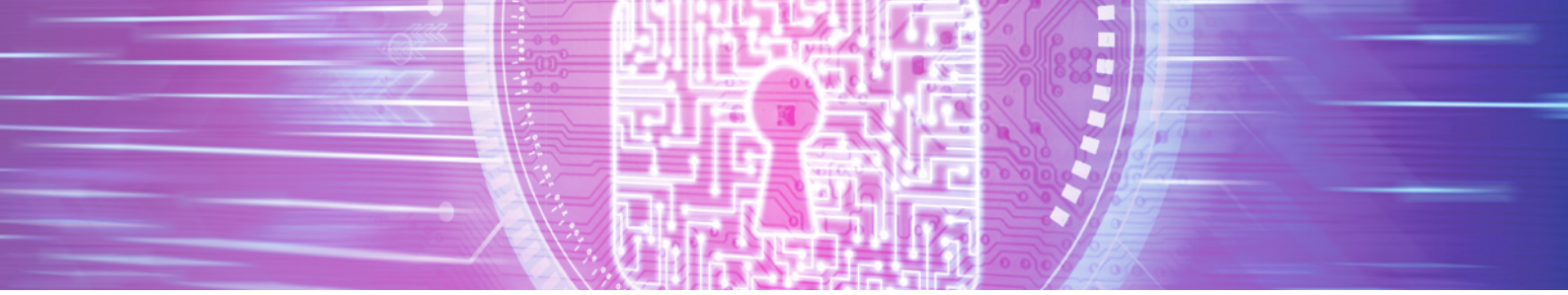
The Cabinet Office and the National Archives run a free e-learning course 'Responsible for Information' which helps business owners and employees to understand information security and associated risks. For a quick guide to safe surfing, passwords and patch management check Sophos' 'Checklist of Technology, Tools and Tactics for Effective Web Protection'.

Although the measures mentioned above are a sensible way to reduce the risks to your business, how should you deal with the outcome of an instance when your firm has been hacked?

An option offered by the insurance market is a Cyber Risks Insurance Policy which offers a cost effective and practical risk transfer mechanism to deal with such situations. The policy protects your business against many of the cyber-related dangers such as damage caused by viruses, hackers and electronic ID theft. Buyers of insurance will also gain access to a panel of expert information security, legal and PR consultants to restore IT infrastructure to operational capacity and to guide them through the process. Most people are in agreement that the most damaging and long-lasting effect of a hack is a tarnished business reputation therefore the main focus of an E-Risk policy is to minimise, rather than pay, for damages.

"A pound invested today on 'prevention' could be worth a thousand pounds spent tomorrow on 'cure' following an attack"

PROTEAN RISK



Possible claim scenarios include:

Data breach following employee theft

A financial advisor was targeted by an identity fraud ring. This group recruited one of the advisor's employees and paid them on a per-record basis for providing documents that contained names, addresses, and other personal information. Eventually the firm was contacted by the authorities; a raid had been conducted which resulted in the discovery of documents containing personal data, a number of which had obviously originated from them. The costs in resolving the situation were significant, including staffing a call centre, offering credit monitoring services to affected individuals, physically posting notifications to affected individuals and an IT investigation to assess the extent of the data breach. In this situation, the insurer would work closely with the financial advisor throughout, covering the costs incurred in meeting their legal obligations and paying for PR support to help mitigate further reputational damage.

Cyber business interruption

An online retail business was affected by a hack suffered by the hosting company which they used. In this scenario, the insurer would cover the retailer for the income lost in the time the website was offline, as well as any further loss of income (including where due to reputational damage) for a period of three months following the hack.

Denial of service attack

An international real estate client experienced a denial of service attack on their IT systems which was not only operationally damaging for the company, but had the potential to severely impact its brand and market standing. In this situation the insurer would not only assist the company by covering the loss of income but would also pay for expert PR support to mitigate any reputational damage.

Data breach following hacking

The IT systems of a large crowdfunding platform were hacked and a copy taken of a database which contained the names and contact details of more than 100,000 customers. In this case the insurer would assist the platform in notifying both their clients and the Information Commissioner's Office, supporting them throughout the investigation which followed.

Data breach following loss of a memory stick

In this scenario an unencrypted memory stick was lost. It had been provided to a potential buyer as part of the due diligence process during a corporate acquisition transaction when it was stolen along with the owner's handbag from a public place. It contained personal and sensitive data of over 500 employees including home addresses and bank details. A fine was levied by the Information Commissioner's Office (ICO) and significant costs were incurred. In this scenario, the insurer would have helped the firm to engage expert data risks or protection lawyers, liaise with the ICO and inform affected employees.

In conclusion, the advice on the street appears to be that a pound invested today in 'prevention' could be worth a thousand pounds spent tomorrow on 'cure' following an attack. However, as prevention is no guarantee, some consideration should be given to how an E-Risk policy can help protect the value, and reduce the ultimate damage, to the business.

For more information regarding Cyber Insurance please contact:

Nicolae Muturniuc
Account Manager

T: +44 (0)203 763 5343
E: nicolaemuturniuc@proteanrisk.com

www.proteanrisk.com

About Protean Risk

Protean Risk is a specialist insurance broker advising firms in the investment industry, financial services and technology sectors. Our clients range from start-ups to companies with revenues in excess of £100m and beyond. We advise clients across a full range of insurance products with a particular focus on professional and executive risks, specifically professional indemnity and directors' and officers' liability insurance.

PROTEAN RISK

One Gracechurch Street, London, EC3V 0DD