The role of Cyber Insurance (and why it's important)

Contact Details:
T: +44 (0)20 3763 5340
E: info@proteanrisk.com
www.proteanrisk.com
Protean Investment Risks Limited,
One Gracechurch Street, London, EC3V 0DD.
Authorised & Regulated by the Financial Services Authority.

PROTEAN RISK

Broker at LLOYD'S

Back in May 2017, The Financial Conduct Authority (FCA) called on Financial Services firms to do more to build their cyber resilience in order to protect customers, companies and data from malicious cyber-attacks. This call becomes all the more important as it was recently reported that 69 firms were hit by cyber-attacks in 2017, up from 38 in 2015 and 24 in 2016.

Indeed, the National Cyber Security Centre has recorded more than 1.9 million incidents of cyber related fraud and 1,100 cyber-attacks in the past 12 months, with 590 of these regarded as significant and 30 (many which included the Financial Sector) requiring action by Government bodies.

These startling numbers were delivered in a speech to the Personal Investment Management & Financial Advice Association (PIMFA) Financial Crime Conference by Robin Jones, Head of Technology, Resilience & Cyber at the Financial Conduct Authority in January 2018.

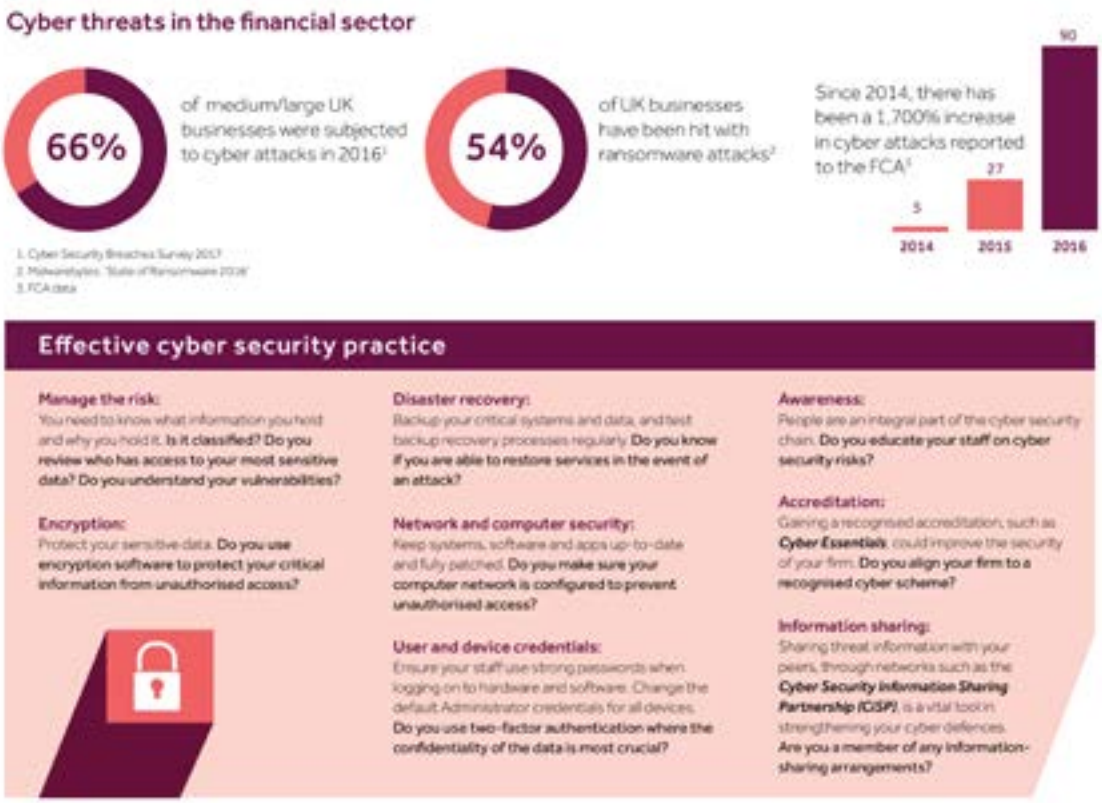
How can you prevent a cyber risk?

The threat of a cyber-attack is very real. In 2017, Wonga, Debenhams, Three and the NHS were all subject to cyber-attacks. These are well-known brands and such attacks therefore make the headlines.

This might unhelpfully create the impression that cyber-attacks are an issue for "large companies" but the reality is that cyber-attacks can be made against business of all sizes.

Small businesses should not presume that it "won't happen to me"; quite the opposite, since smaller businesses will have less investment in protective technology and are therefore more likely to be at risk from cyber criminals.

To help all businesses in the Financial Sector, last year the FCA published a useful infographic giving basic information about cyber hygiene, including how to use the National Cyber Security Centre's Cyber Essentials accreditation and connect to the Cyber Information Sharing Partnership.



With cyber threats becoming ever more frequent, you need to make sure that you have adequate IT protection in place against a cyber threat and if an event does occur, that you are sufficiently protected as one of your regulatory responsibilities.

One way to do this is to take out adequate Cyber insurance. However, you need to make sure that any policy you take out responds to your individual risk profile.

How Cyber Insurance is Building Resilience.

Insurance can play a key role in helping all companies in the Financial Sector build their cyber resilience.

The benefits are not just the valuable financial protection when an insured cyber event occurs, but also access to expert consultants and on-the-ground support, from IT specialists through to ransom, extortion and PR experts, that might otherwise be beyond reach.

Estimates suggest only 35-40% of UK businesses take up Cyber Insurance, but as threats increase and become more complex, unsurprisingly more and more firms are considering this protection.

What level of Cyber cover is right for my business?

Predictions that global Cyber Insurance premiums will more than double in the next three years has caused an explosion of choice for buyers. For example, just within the Lloyd's insurance market there are now 77 cyber risk insurers.

Despite the first Cyber Insurance policies appearing in the late 90s, the product is still in the juvenile stage of development and evolving all the time. Policy coverage can be grouped into common categories (see table below), but the scope and cover options can vary widely among different insurers:

First party loss or damage	Damage to your property as a result of a cyber-attack, including: •**Data & Software-** The cost to reconstitute data or software that has been deleted or corrupted. •**Intellectual Property-** IP loss of value based on a reduction in revenue and market share. •**Incident investigation and response costs-** Cost to investigate incidents and minimise the cost a cyber-attack.
Business Interruption and Increased costs	Lost profits or extra expenses incurred due to the unavailability of IT systems or data as a result of IT failures, including those resulting from cyber-attacks. Loss of revenues which can be directly attributed to a security breach event, for example, loss of specific contracts or customers, or reduced transaction volumes. Additional expenses incurred to restore data, the network or IT systems.
Third Party Liability	Cover for third party claims and defence costs arising from a data breach including: •The cost to investigate and respond to a data breach/cyber-attack •The costs of providing a service to help manage the incident, including the costs of notifying customers; forensic investigations; customer credit monitoring; and public relations expertise to help mitigate reputational harm to you •Defence costs associated with regulatory investigations •Liability for death and/or bodily injury.

Cyber extortion	The cost of an experts employed to help you manage an extortion incident, pay ransom demands and restore affected systems.
Cybercrime/ cyber fraud	Cover for losses suffered as a result of the use of computers to commit fraud or theft of money, securities or other property.
PCI DSS Assessments and Fines	Breaches involving payment card data could expose you to PCI related fines and PCI DSS assessments. Policies can provide cover for costs relating to stolen card data, reimbursements of card reissuing costs and forensic investigations to establish the misuse of card data.

To be able to properly consider different insurance options, firms need to understand their cyber risk exposures and how these match with the different policies being offered.

All sizes and types of firms benefit from involving different stakeholders in their business to pool knowledge and expertise. For example, CIO or IT experts could identify potential scenarios; those responsible for business continuity might quantify operational impacts and the finance department could help with calculating the likely costs and lost business.

The benefits of Cyber Insurance.

Business Interruption – One of the main benefits of having cyber insurance in place is that your insurer may cover you for loss of income or increased costs while your business deals with and recovers from a cyber-attack.

Privacy Infringement Claims – If any data is lost or compromised as a result of a cyber-attack, you may need to notify your customers and also deal with any privacy infringement claims. Your policy could cover the cost could cover legal costs in the event of a breach.

Extortion – If you are attacked with ransomware, you may be faced with having to pay hackers to release your data. Your policy could cover these demands. You may also face lost or corrupted digital assets and your policy could help with recovery or restoration costs.

Forensic support – Most cyber insurance policies will give you access to trained cyber specialists in the event of an attack. These specialists can work with you to assess the damage, help to recover any lost data and devise a recovery plan.

GDPR – Cyber Insurance could also prove to be a lifeline for GDPR when the new regulation comes into force in May 2018: Having adequate procedures and covers in place could protect you from data breaches and subsequent penalties from the ICO.

Media Liability & Reputational Damage – a policy may cover you in the event that a defamation or infringement of intellectual property claim is made against you, which could affect your reputation and impact your brand.

Limitations of Cyber Insurance.

Complex & Changing Environment – The nature of cyber-attacks is constantly changing, and cyber criminals are finding new and innovative ways to hack into businesses. This means that the cyber insurance landscape is constantly changing. Ensure that you speak to the right people who provide the right advice for your business and can make sure that your policy is adaptive to your needs.

Data protection – Even though cyber insurance will help you in the event of a cyber-attack or data breach, preventative measures should already be in place to stop this from happening. Prevention is always better than cure. You must ensure that you have employed adequate data protection measures to prove you've done all you can to prevent a cyber-attack and not left openings for cyber criminals.

Protean can help protect your Business.

Financial Services insurance and risk specialists, like Protean Risk, can feed information in this assessment by sharing peer knowledge and experience, including types and levels of cover similar firms purchase.

Without a doubt, insurance has a key role to play in building cyber resilience, but this is just one tool that forms part of a comprehensive strategy.

Small, medium and large Financial Services firms need to find their own balance between cyber risk management, security investments and securing insurance suitable to the unique needs of their sector and organisation.

Contact us today to find out how we can help your business with Cyber Insurance on +44 (0)20 3763 5340 or visit www.proteanrisk.com for more information.