



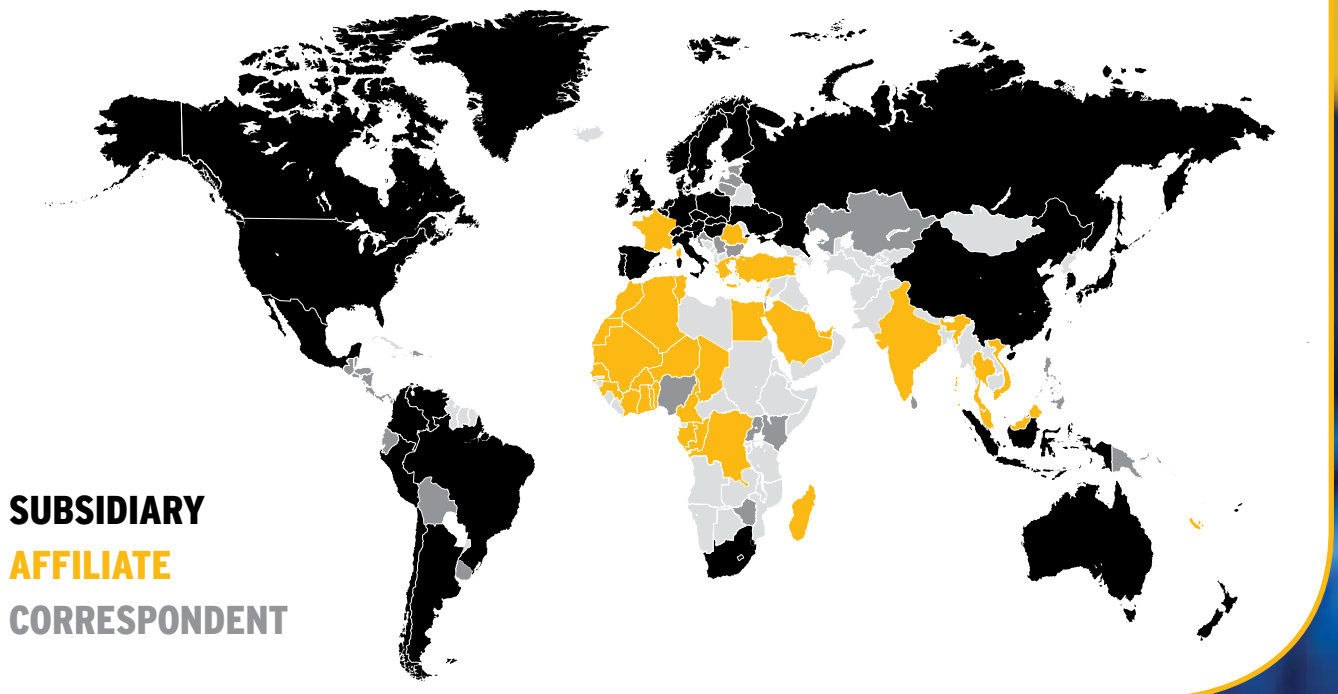
CYBER/ NETWORK SECURITY

FINEX GLOBAL

Willis

ABOUT US

- » We are one of the largest insurance brokers in the world
- » We have over 180 years of history and experience in insurance; we currently operate in over 400 offices in nearly 120 countries, with a global team of approximately 17,000 Associates serving clients in some 190 countries
- » USD 32.2 billion of global premiums placed through worldwide markets



ANY COMPANY THAT STORES PERSONAL DATA, ARE RELIANT ON COMPUTER OR TELEPHONE NETWORKS, DIGITAL INFORMATION OR THE INTERNET FACES CYBER EXPOSURES

WHAT ARE CYBER RISKS?

Today, using computers and logging on to public and private networks has become second nature in both our personal and business lives. We are all constantly producing and saving data, surfing the net, uploading content and sending and receiving email traffic. It is difficult to recall how we were ever able to manage without such technologies and the benefits they bring. However, in creating this new digital world we have also created a by-product – Cyber risks.

Cyber risks are faced not just by e-commerce companies and those undertaking transactions over the internet, but also by companies that store personal data, are reliant on computer or telephone networks, holds digital information or uses the internet can face these exposures. In short, just about every business in the world today is faced with Cyber risks, some of the core Cyber exposures include:

» PRIVACY BREACH

Anyone that stores Personal Identifiable Information (PII) is exposed to data breaches. Data breaches may occur from a hack, a disgruntled employee or even a lost laptop. In the UK the costs a company face as a result of one compromised record is approximately GBP 70 – large scale breaches can therefore be very costly indeed.

» NETWORK DOWNTIME

Most companies are reliant on networks, whether it's the network that interconnects various company sites, enterprise private networks or the critical backbone network that deals with network performance management and network congestion. Network downtime can be caused not just by malicious hacks such as a 'Denial of Service' (DoS) attack, but also by operational failures involving software and hardware failures, both of which can have a significant financial impact on a business.

» MULTIMEDIA RISKS

Social media is now a key marketing strategy utilised by companies. However 'User Generated Content' (UGC) and the posting of unlicensed content has caused a dramatic increase in online defamation claims and intellectual property infringement claims. The use of such sites requires additional infrastructure and maintenance resources, to ensure the appropriate defensive layers are in place to protect the company. Monitoring of chat rooms is not always possible and reliance on self regulation by the audience is a dangerous strategy. Also, pre-screening is not possible on Facebook and Twitter and the minimum fallback must be relevant staff training.

» CYBER EXTORTION

Cyber extortion is a crime involving an attack, or threat of attack, against a company, coupled with a demand for money to stop the attack. There are various types of Cyber extortion but originally DoS attacks were the most common method. More recently Cyber criminals have developed actual ransomware that can be used to encrypt the targets data. The attacker then demands money for the decryption key. The probability of prosecuting the criminals is low because criminal gangs usually operate from countries other than those of their target. Cyber extortion is big business and with criminals earning millions of pounds annually the majority of Cyber extortion episodes go unreported because victims do not want the publicity.

SOME OF THE LARGEST BREACHES THAT HAVE OCCURRED HAVE COST COMPANIES UPWARDS OF GBP 100M

THE DATA BREACH PHENOMENA

By far, the most well known Cyber risk and the most common cause of Cyber risk claims notified to Willis' FINEX Global practice group and the insurance market presently is a privacy/data breach. How the breach occurs can come in a variety of ways – from hacking to lost laptops. Common to all breaches is the significant quantum of the costs suffered by the breached company to deal with the data theft/loss.

Increasing data protection legislation, the growth of the underground digital economy and new technology such as cloud computing and social media has seen the number of data breaches significantly increase year on year. Some of the largest breaches that have occurred have cost companies upwards of GBP 100m. Costs as a result of a data breach can include:

» FORENSIC COSTS

Immediately after a breach it will be necessary to carry out forensic analysis and investigations to identify and contain the breach. It may also be necessary to undertake an official forensic audit by approved auditors of the relevant data protection authority.

» NOTIFICATION

In the event there is a data breach customers affected by the breach will need to be notified. This is mandatory in the US, Spain, Germany, Austria and Norway however it is considered good practice by the Information Commissioner's Office (ICO) here in the UK. Notifying customers will also ensure that consumer churn is kept to a minimum.

» CREDIT MONITORING

Another service provided by companies to their customers after a security breach is 'credit monitoring'. This is a service provided by a third party to monitor the affected individual's credit history for fraudulent activity. It may be offered for up to 5 years post breach.

» PR COSTS

In the event of a major security breach it is necessary to employ PR expertise in order to try and reduce the reputational impact to a company.

» CRISIS MANAGEMENT COSTS

Other miscellaneous costs including setting up of third party call centres for affected customers.

» FINES AND PENALTIES

Regulatory fines and penalties plus Payment Card Industry (PCI) fines where credit card information is involved.

» LIABILITIES

Companies may incur liability claims for damages from banks if financial data has been taken from the individuals themselves for any costs they have incurred as a result of the breach such as time off work, and from any other third parties that may have suffered a financial loss from the breach.

CYBER INCIDENTS/ CLAIMS SCENARIOS

The table below looks at some of the most common types of Cyber claims and highlights the associated costs that companies could face as a result:

INDUSTRY	SCENARIO	TYPE OF COSTS INCURRED	COVER
Retail	A hacker accessed the retailer's network and stole 15 million customers' PII.	The retailer incurred significant costs to deal with the breach including forensic costs, notification costs, PCI fines and credit monitoring costs. Liability claims followed.	Privacy/Network Security Liability/ Privacy event mitigation costs, PCI fines.
Hotel	A hotel group's point of sale network was hacked into and 6 million customer's credit card details were taken.	The hotel experienced high forensic costs to isolate the hack. Additional costs included mandatory notification costs and PCI fines. The hotel offered all of the individuals 2 years credit monitoring service. They also received liability claims for damages from the banks.	Privacy/Network Security Liability/ Privacy event mitigation costs, PCI fines.
Airline	An airline received a Distributed Denial of Service (DDoS) attack bringing down their online sales platform for 48 hours.	The airline experienced a significant loss of revenue during the network downtime plus increased costs of working.	Non-physical business interruption.
Media	The media company utilised content on their website without obtaining the appropriate licences.	They were successfully sued for over GBP 1m for copyright infringement.	Multimedia Liability.
Financial Services	An employee of a financial services company left a laptop in a public place containing the PII of its clients.	Costs included the hire of a PR firm, notification to all of the customers affected, setup of an ID theft/credit alert service call centre and credit monitoring services.	Privacy/Network Security Liability/ Privacy event mitigation costs.
Gaming	A hacker threatened to take down the private network of the gaming company unless they paid them GBP 5m.	Investigation costs to identify the threat plus the extortion demand amount.	Cyber Extortion.



FINEX GLOBAL CYBER COVER

Willis FINEX Global, in conjunction with key Cyber markets has developed a market leading Cyber Insurance solution:

» **PRIVACY PROTECTION**

1. Third party and employee privacy liability for damages and claims expenses as a result of a privacy breach.
2. Privacy regulatory defence and penalties.
3. Notification expenses to notify victims of privacy breaches.
4. Forensic costs to contain a breach and carry out the necessary forensic audits following a breach.
5. PR expenses to help limit the reputation impact following a security breach.
6. Credit monitoring costs to monitor the victims credit history for fraudulent activity.
7. Payment Card Industry (PCI) fines.
8. Reputational risk extension as a result of a data breach (case by case basis).

PLUS other Cyber liability coverages including:

9. Network Security Liability for damages and claims expenses the insured is legally obligated to pay, arising out of computer attacks caused by failures of security.
10. Negligent transmission of a virus: for damages to customers' computer systems and/or data.
11. Multimedia Liability, Intellectual Property Infringement and libel and slander due to email or website content.

» **LOSS OF DIGITAL ASSETS INCLUDING NON-PHYSICAL BUSINESS INTERRUPTION**

1. Data/electronic information loss: The costs to restore data that has been lost or corrupted.
2. Indemnification for loss of revenue following unplanned system outage and increased cost of working.
3. Cyber extortion coverage: Covers both the costs of investigation and the extortion demand amount related to a threat to commit a computer attack.
4. Cyber terrorism coverage (case by case).

Typically this will act as the template coverage. After a period of consultation, our e-solution experts will further develop and tailor the coverages so that it is aligned with your business specific risk profile.

WHY FINEX GLOBAL CYBER PRACTICE?

» **SPECIALIST KNOWLEDGE**

With our specialised knowledge in the sector we are able to design innovative programmes that specifically reflect the needs of our Cyber clients. For our clients the benefits are simple – expert advice ensuring the ultimate in cost-effective programme design.

» **A CONSULTATIVE APPROACH**

We fully analyse your Cyber exposures before proposing the most appropriate Cyber risk transfer solutions for your business.

» **EXCLUSIVE WORDINGS**

Our Cyber Practice has its own exclusive wording that we have designed in conjunction with key Cyber insurers. The breadth of coverage goes way beyond the off the shelf products typically offered.

» **CLAIMS HANDLING**

We have been in the Cyber market for over 10 years and our claims team have developed insightful experience in how best to deal with your Cyber claim to ensure it gets paid.

» **CYBER RISK MANAGEMENT**

We can establish your Cyber risk profile utilising Cyber assessment tools. This will allow you to take the appropriate actions to better protect your company's computer network resource and information assets in order to mitigate potential network risks.

» **MARKET LEVERAGE**

Willis has excellent market leverage due to the significant amount of premium that our Cyber Practice places into the market.

» **MARKETING APPROACH**

The same team that analyses your risks and develops a protection strategy approaches markets on your behalf.

» **THE WILLIS "ONE FLAG" APPROACH**

Willis' expertise in all our offices around the world is available to you – essential for international companies who need to comply with the various international data protection laws.

» **CYBER RISKS INFORMATION UPDATES**

Our clients are kept up-to-date with the latest Cyber trends via the Cyber e-newsletter, seminars and workshops.

If you are concerned about your businesses Cyber risks contact us and arrange an initial consultation to start mapping out your risks:

Jeremy Smith

+44 (0)20 3124 6086

jeremy.smith@willis.com



Willis Limited

The Willis Building
51 Lime Street
London, EC3M 7DQ
United Kingdom
Tel: +44 (0)20 3124 6000

www.willis.com

Jeremy Smith

+44 (0)20 3124 6086
jeremy.smith@willis.com

Willis Limited, Registered number: 181116 England and Wales.
Registered address: 51 Lime Street, London, EC3M 7DQ.
A Lloyd's Broker. Authorised and regulated by the Financial Services Authority.

9895/09/11

