

# CYBER RISKS

Cybercrime has risen up the ranks over the last year to become the second most commonly reported economic crime after asset misappropriation according to a PwC survey of global economic crime. As companies rely more and more on technology to conduct and grow their business, they are becoming aware of the potential consequences of cyber crime or technological disruption. A cyber incident is likely to be expensive and damaging.

Cybercrime accounted for 38% of economic crime incidents in a survey which in total analysed 3,877 responses spanning 78 countries, with 23% of those (878 respondents) coming from the financial services sector.

Some 45% of financial services respondents suffered frauds in the last 12 months, a much higher figure than the 30% reported by other industries. This is an indicator that the sector remains very attractive to criminals due to the significant amount of cash, assets and sensitive client data that is available to them as well as the nature of the industry.



*“Norton Cybercrime Report” estimated that the global cost of cyber crime is around \$110 billion per annum*

*The UK Government estimated the cost of cyber crime to the UK to be £27 billion per annum*

## *But what exactly are some of the key cyber risks?*

Theft or manipulation of sensitive information and the threat to disclose valuable information, trade secrets and intellectual property and extortion, loss of data resulting in financial loss, loss of revenue, disruption to supply chain management leading to loss of orders, personal information, downloading of viruses infecting computers that can destroy and cripple systems and business operations.

## CYBER INSURANCE



Studies made by top insurance companies highlight risks such as cyber crime, IT failures and espionage as those generating a growing concern, although behind risks such as business interruption, supply chain and natural catastrophes in a ranking of the top global business risks. Traditional business insurance policies will not cover all the exposure a business will face from a security breach. In fact, some insurers are now specifically **excluding** cyber liability in standard liability policies.

### *So how can companies protect themselves?*

Businesses seeking protection from cyber crime must consider their exposure carefully, choosing an insurance cover that meets their needs.

Ad hoc **Cyber policies** are now available for smaller and medium-sized businesses that will cover the gaps in their existing property and third party insurance programmes. The coverage offered by these dedicated policies normally includes:

**First party damage to data**

**Privacy and security liability**

**Cyber extortion**

**Business Interruption**

**Brand reputation**

**Cyber terrorism**

There are options to extend insurance covers for:

### **A) First Party cyber risks:**

Restoration costs  
Technical/legal/investigative support  
Replacement costs  
Intellectual property theft  
Business income and extra expenses

### **B) Third Party cyber risks:**

Disparagement, infringement and plagiarism  
Rights to privacy or breach of confidence  
Transmission of virus or denial of service  
Loss of customer data and data protection

*Did you know that new laws coming into force in the EU are set to introduce new cyber security standard regulations which will press corporations to tighten their cyber security or face harsh financial penalties?*

The European Commission proposes to ensure all Member States meet certain minimum security standards by implementing a Cyber Security Directive. The Directive will require notification of **potential** security risks. It will also require actual incidents to be reported to cyber security authorities that will be established across Europe.

### *Who will be affected?*

Organisations that will be effected by the new Cyber Security Directive are:

- ⇒ **public authorities;**
- ⇒ **information society service providers**, such as providers of e-commerce platforms, social networks, cloud computing services, application stores, internet payment gateways and search engines;
- ⇒ entities that operate **critical infrastructure**, including **energy** suppliers and **transport** carriers (such as air carriers, rail transport operators and logistics service providers);
- ⇒ **health sector** organisations (including private clinics); and
- ⇒ **banking** and **credit** institutions and **stock exchanges**.

The exemption for micro enterprises will provide limited relief as micro enterprises are defined as organisations which employ fewer than ten people **and** whose annual turnover does not exceed €2 million. Other SMEs are not exempted and will be required to comply with the Cyber Security Directive in full.

*Did you know that on the 12th August the Directive 2013/40/EU of the European Parliament and of the Council was issued inviting the Member States to introduce sanctions in the area of attacks against information systems?*

The threat of cyber attack is very real. It is a constant battle to keep up with the fast paced evolution of hacking and cyber crime as the people responsible continue to find new and innovative ways to break through security. Although, it seems, we will never reach a point where we are one step ahead, prevention is better than a cure, so adequate protection of your systems, together with tailored insurance, is key to avoid falling foul of cyber crime.

*If you want to learn more please contact us, PRS Ltd, where we can discuss or review your existing policies to see where cyber cover is included or could be included.*



## BUT WHO IS PAGNANELLI RISK SOLUTIONS LTD?

*PRS Ltd provides primarily risk management and consultancy services and looks to corporate and medium-sized industrial and commercial entities, as well as to private and public institutions. It can also provide insurance solutions, including protection against catastrophic events, terrorism and similar risks.*



*PRS is proud to be considered highly specialised in the space and aviation fields, but also possesses a high level of expertise and skills in many other fields of commercial and industrial activities. Since its initial years of activity, it has achieved important targets with the acquisition of a number of medium-sized to large clients and the assignment of qualified roles in complex insurance projects. Any kind of Property, Business Interruption, Cargo, D&O, Third Party Liability risks are our appetite for solutions. This success is due to its management's international experience which spans over more than 45 years.*

*PRS Ltd also supports professional and academic initiatives. Through the organisation of qualified international Conferences and Seminars, it provides forums for open discussions on how insurance can facilitate human progress and improve the quality of life.*

[www.pagnanellirs.com](http://www.pagnanellirs.com)

**Representative Office:**  
Via Luigi Carlo Farini, 3  
40124 Bologna (BO)  
Tel +39 051 0545543/0545516  
Fax +39 051 0545402

**Registered Office:**  
801 Dryden Building  
37 Commercial Road  
London E1 1LF  
[prs@pagnanellirs.com](mailto:prs@pagnanellirs.com)