S-Tech

Cyber Insurance

Cyber insurance covers the losses relating to damage to, or loss of information from, IT systems and networks.

Do I need it?

As a business of any size, it is likely you will rely on information technology (IT) infrastructure to some degree. If so, you will be exposed to the risks of business interruption, income loss, damage management and repair, and possibly reputational damage if IT equipment or systems fail or are interrupted.

A UK Government survey estimated that in 2014 81% of large corporations and 60% of small businesses suffered a cyber breach. The average cost of a cyber-security breach is £600k-£1.15m for large businesses and £65k-115k for SMEs.

While existing insurance policies such as commercial property, business interruption or professional indemnity insurance, may provide some elements of cover against cyber risks, businesses are increasingly buying specialised cyber insurance policies to supplement their existing insurance arrangements, particularly if they:

- hold sensitive customer details such as names and addresses or banking information;
- rely heavily on IT systems and websites to conduct their business;
- process payment card information as a matter of course.

What does it cover?

Cyber insurance covers the losses relating to damage to, or loss of information from, IT systems and networks. Policies generally include significant assistance with and management of the incident itself, which can be essential when faced with reputational damage or regulatory enforcement.

Generally cyber risks fall into first party and third party risks. Insurance products exist to cover either or both of these types of risk.

First-party insurance covers your business's own assets. This may include:

- Loss or damage to digital assets such as data or software programmes
- Business interruption from network downtime
- Cyber extortion where third parties threaten to damage or release data if money is not paid to them
- Customer notification expenses when there is a legal or regulatory requirement to notify them of a security or privacy breach
- Reputational damage arising from a breach of data that results in loss of intellectual property or customers
- Theft of money or digital assets through theft of equipment or electronic theft

Third-party insurance covers the assets of others, typically your customers. This may include:

- Security and privacy breaches, and the investigation, defence costs and civil damages associated with them
- Multi-media liability, to cover investigation, defence costs and civil damages arising from defamation, breach of privacy or negligence in publication in electronic or print media
- Loss of third party data, including payment of compensation to customers for denial of access, and failure of software or systems

Managing cyber risks

As well as putting adequate insurance in place, it is important for you to manage your own cyber risks as a business.

This includes:

- Evaluating first and third party risks associated with the IT systems and networks in your business
- Assessing the potential events that could cause first or third party risks to materialise
- Analysing the controls that are currently in place and whether they need further improvement

In 2014 the Government launched Cyber Essentials – a basic cyber security hygiene standard to help organisations protect themselves against common cyber attacks. Considering Cyber Essentials accreditation is a good first step in becoming cyber resilient.

If you suffer a cyber breach, having cyber insurance can make the recovery process as straightforward and rapid as possible (however it is still likely to take a number of days or weeks depending on the severity of the incident). Many insurers include technical assistance with managing a breach as part of the insurance policy – if so, get in touch with them as soon as possible after the breach is discovered.

UK and European action to tackle cyber risks

The UK Government views cyber attacks as a highest level risk to national security, alongside terrorism threats. As such it has introduced a number of changes to help prevent cyber attacks, including:

- Cyber Essentials – a basic cyber security hygiene standard to help organisations protect themselves against common cyber attacks
- a National Cyber Crime Unit within the National Crime Agency
- a 'Cyber Information Sharing Partnership' to allow Government and industry to exchange information on cyber threats
- a single reporting system for people to report financially motivated cyber crime through Action Fraud, a UK National Computer Emergency Response Team (CERT) to improve national co-ordination of cyber incidents
- a new Cyber Incident Response scheme in GCHQ to help organisations recover from a cyber security attack
- a network of Centres of Excellence for Cyber Security Research within UK universities in 2013, to help provide reliable and up to date research and academic prowess.

S-Tech

S-Tech Insurance Services Ltd
154-156 Victoria Road, Cambridge, CB4 3DZ
www.s-tech.co.uk
+44 (0) 1223 324233