NWBIB
Insurance Brokers

CYBER RISKS

Any business holding electronic data whether it's on a mobile device, computer, server or online faces a risk if the data is interfered with by a hacker, stolen by an employee or accidentally lost.

This risk could result in expensive costs to:

- Rectify the breach
- Notify affected customers that their data may have fallen into the wrong hands
- Rebuild your network to fix the breach and resolve any e-viruses
- Repair your reputation
- Defend any legal action arising out of the breach

The European Commission estimates that more than 1 million people worldwide are victims of cyber crime every day*

HOW CAN CLAIMS ARISE?

Rogue Employee

Employee stole and sold the personaL Information of its employer's customers.

Cover - Defence costs and reimbursement of customer notification and credit monitoring costs

Theft

Briefcase stolen containing a USB Memory stick holding personal data of customers. Action taken by Authority for the failure to have proper policies in place for the security of personal data.

Cover - Defence costs and reimbursement of customer notification and credit monitoring costs

Hackers

Hackers broke into a database and accessed customers ' personal data. Class action lawsuit determined lack of encrypted data and unsecure firewall.

Cover - Defence costs and ultimately damages awarded to customers

3rd Party Outsourcing

A printer wrongfully provides credit card information to a third party resulting in unauthorised transactions for its customers.

Cover - Significant legal defence costs

PREVENTION IS BETTER THAN CURE

Here are a few simple precautions that can reduce the risk of a breach:

- Understand your IT risks and exposures, by keeping close to your IT department
- Develop clear IT security policies for staff and ensure these are kept up to date and clearly communicated to all relevant staff
- Work with your HR and Marketing department to understand any new developments and how these could impact on data security
- Make cyber risk integral to your business recovery plan – so that you have a plan of action should a major breach occur

A Cyber insurance policy can provide the following protection for financial losses arising from data security breaches -

THIRD PARTY ACTIONS

Disclosure	Unauthorised release of personal records
Content	Intellectual cyber property infringements
Reputation	Privacy breaches, defamation when disseminating information
Conduit	Damage to a third party computer system caused by hacker/attacks on or access to your own computer system
Impaired Access	Where customer is impaired from using your computer system due to hackers/attack

YOUR OWN EXPENSES

Privacy Notification	The costs incurred notifying your customers / persons who have had their data hacked or wrongfully accessed – even when not required by law
Reward	To help induce an arrest and conviction following a cyber-attack
E-Business Interruption	Loss of business income and recovery expenses following a cyber-attack on your own system
E-Threat	Ransom payments met in response to a range of threats relating to your own computer system or data
E-Vandalism	Reproducing damaged computer data
Crisis Management	Managing the impact and costs of an insured event from third parties

A Cyber policy will meet these costs even if the loss was caused by an outsource data-handling firm.

For more information on Cyber Risks contact your Account Executive or email commercial.insurance@nwbib.co.uk

* European Commission Cyber Security survey report published July 2012