Data Breaches: A Growing D&O Concern

Insight for business owners and risk managers—provided by **Crendon Insurance Brokers Ltd**

A data breach can be devastating—ruining a company financially and permanently damaging its reputation with customers. As a director or officer at your company, you face litigation risks based on the decisions you make following a breach and on how you influence cyber security policies, as these are often considered board-level issues.

If a suit is filed against you after a data breach occurs, based on your position as a board member, you may not be protected by your cyber liability policy. Your best source of protection is from your directors' and officers' (D&O) policy—as long as your policy is tailored to include protection after a data breach.

Data Breach Threats

The biggest threat from a data breach is loss of information, whether it is information regarding your company's finances or the personal identification information of your customers, such as National Insurance numbers or credit card data.

Losing sensitive information belonging to your customers or your company can ruin your reputation. If the credit card data of your customers is stolen, your customers would need to cancel their cards and get new ones—an inconvenient process that can damage your company's public image.

Data Breach Response

Following a data breach, you may be legally required to notify certain organisations about it. For example, depending on the type of company you run, you may need to notify the Information Commissioner's Office (ICO) of any personal data breaches within 24 hours of becoming aware of the breach. Failure to comply with the requirement to submit breach notifications can result in a £1,000 fine.

Notification should be taken very seriously, as the way a company responds to a data breach can lead to exposure and legal action from customers and regulatory authorities if it is done poorly—the ICO has the power to issue monetary penalty notices of up to £500,000.

Data Breaches and D&O Cover

Insufficient cyber security that leaves your company vulnerable to a data breach can be seen by your customers or shareholders as negligence or a breach of duty. Your customers and shareholders may seek to hold you responsible for the damage, as the board is responsible for making decisions on behalf of the company.

Crendon Insurance Brokers

Because of this, you need protection in the form of a D&O policy.

In past legal cases following a data breach, directors and officers have been accused of:

- Failing to take reasonable steps to protect customers' personal and financial information
- Failing to implement controls to detect and prevent a data breach
- Failing to report a breach in a timely manner

A cyber liability policy cannot offer the legal protection needed by directors and officers after a data breach, whereas a D&O policy can.

A D&O policy provides cover for a 'wrongful act', such as an actual or alleged error, omission, misleading statement, act of neglect or breach of duty.

Cyber Security Is Vital

Cyber security is rapidly becoming a vital aspect of responsible business management and customer service, and a company's directors and officers are expected to be involved in and knowledgeable about the company's cyber security.

Ensuring your company has suitable and trustworthy cyber security is paramount. If you determine your cyber security may not be sufficient, you should take steps to improve it. The following are some techniques to strengthen your company's cyber security:

- **Install a firewall**. Companies with five or more computers should consider buying a network firewall to protect the network from being hacked.
- **Install security software**. Anti-virus, anti-malware and anti-spyware should be installed on every computer in the network. All software should be up-to-date.
- **Encrypt your data**. All data, whether stored on a tablet, flash drive or laptop, should be encrypted.
- **Use a virtual private network (VPN)**. A VPN allows employees to connect to the company's network remotely without the need of a remote-access server. VPNs use advanced encryption and authentication protocols, providing a high level of security for your network.
- **Develop a data breach plan**. Have a plan in place so that when—not if—you experience a data breach, you can act quickly and minimise your loss.

Data Breach Risks Without D&O Insurance

After a data breach, shareholders and customers will most likely submit claims. Since you can be held personally responsible for the acts of the company as a board member, your plans and decisions need to be protected.

Without D&O cover, your personal assets are at stake and could be forfeited to cover legal costs. But you can protect yourself from such losses with a D&O insurance policy. Talk to the insurance professionals at **Crendon Insurance Brokers Ltd** today for more information about a bespoke D&O policy that protects you and your co-workers from data breach liability.

Crendon Insurance Brokers Limited
11 Greenfield Crescent
Edgbaston
Birmingham
B15 3AU

Tel: 0121 45 45 100
www.crendoninsurance.co.uk
enquiries@crendoninsurance.co.uk

Crendon Insurance Brokers