the Management file

Data Breaches—A Growing D&O Concern

Insight for business owners and risk managers provided by Olson & Olson, Ltd

A data breach can be a devastating event, affecting a company financially and damaging its reputation with customers. But 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 will not be protected by your commercial general liability policy or 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 Social Security numbers or credit card information.

Losing sensitive information belonging to your customers or company can have a devastating effect on your reputation. If the credit card information of your customers is stolen, your customers would need to cancel their cards and get new ones—an inconvenient process and one that can damage your company's image in the eyes of customers.

Data Breach Response

Following a data breach, you may be legally required to notify certain people about it. For example, if your company is publicly traded, guidelines issued by the Securities and Exchange Commission (SEC) say you must report cyber security incidents to stockholders. The cost of notification after a breach is generally covered by a cyber liability policy. And depending on the number of people you need to notify, the cost can be quite high.

Notification should be taken very seriously, as the way a company responds to a data breach can lead to exposure and legal action beyond lawsuits from customers—the company could be subject to regulatory action from the Federal Trade Commission or the SEC.

Data Breaches and D&O Coverage

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. 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 the following:

OLSON & OLSON Ltd

- 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 would not offer the legal protection needed by directors and officers after a data breach, whereas a D&O policy can.

A D&O policy provides coverage 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

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

The following are some techniques to improve the cyber security of your company:

- 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 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 when, not if, you experience a data breach, you can act quickly and minimize your loss.

Data Breach Risks Without D&O Insurance

After a data breach, claims from shareholders and customers will most likely be made. 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 coverage, your personal assets are at stake and could be forfeited to cover legal costs. You can protect yourself with a D&O insurance policy. Talk to your insurer about this type of coverage and be sure your policy is tailored to cover any gaps.