November 26, 2014

InsideCounsel.com

BUSINESS INSIGHTS FOR LAW DEPARTMENT LEADERS

Ensuring the Right Insurance Coverage for Data Breach

BY BRUCE A. FRIEDMAN ESQ.

The Chief Information Officer (CIO) was at the CEO's office door when she arrived for work that Monday morning. Before the CEO could get through the door, the CIO informed her that over the weekend the company's computer system had been hacked. "We are investigating the scope of the breach and repair of the system which is down. We are trying to determine the scope of the loss of data, but we are afraid that the hackers obtained access to customer information, including customer credit card and other private financial information." The CEO called in all the C-level officers to discuss the data breach and all that would need to be addressed. The meeting produced a to-do list as follows:

1. Investigation of the cause of the breach, repair of the system, and the installation of new and better security software;
2. Restoration of the lost data or recreation of the data, if possible;
3. The duration of business interruption and the estimated time necessary to get the operating system functioning properly;
4. The retention of a public relations (crisis management) firm to assist in creating and communicating the breach to customers and the public;
5. The company's legal exposure to customers whose data was obtained, possible shareholders' claims and any claims the company may have against its outside consulting firm that designed the operating system;
6. The scope of insurance coverage for losses and expenses incurred in connection with the data breach and legal exposure to third parties.

The General Counsel was assigned Nos. 4 and 5 on the list. He left the meeting and immediately met with outside counsel to discuss the exposure to customers for invasion of privacy claims and potential class actions that could be filed. They also discussed potential claims against management if it was determined that the operating system did not have state of the art security against cyber-attacks.

The General Counsel also met with the company's risk manager and insurance broker. In that meeting, the General Counsel received some very disturbing information. The company was currently in discussions with a number of insurers to purchase a cyber insurance policy, but had not yet purchased a policy. After calming his nerves, the GC asked what a cyber insurance policy would cover. The broker told him the basic features of the policies under consideration:

1. Reimbursement of expenses and costs of investigation with respect to (a) the cause of the breach, (b) public relations professionals engaged to mitigate financial harm, (c) the restoration or recreation of the electronic data.
2. Losses resulting from business interruption as a result of the breach;
3. Defense, loss, damages, costs and expenses of third-party claims arising out of invasion of privacy or any theft of personal and confidential data;

The broker called his coverage counsel and together they informed the GC that there may be coverage for third-party claims by customers or shareholders under the company's current General Liability policy, Directors and Officers (D&O) policy and Crime coverages. First-party claims for losses to the company from the data breach may be covered under the Property policy and Business Interruption policy. They told the GC that they would immediately review the policies and provide him with a more definitive response.

Comprehensive General Liability (CGL) policies are the bedrock of commercial insurance and cover property damage and bodily injury claims. They also include coverage for various offenses, including invasion of privacy. Depending on the wording of the invasion of privacy offense, and absent an exclusion for losses resulting from cyber-attack or data beaches, (new policies may exclude claims arising out of data breach since insurers generally exclude claims covered under policies that are written for specific risks), a CGL policy should cover invasion of privacy claims arising out of data breach.

D&O policies provide coverage for the directors and officers of a corporation and possibly the corporation itself for wrongful acts defined broadly to include acts, errors or omissions. Obviously, a claim for invasion of privacy arising out of a data breach would be based upon a contention that the entity did not take adequate steps (an omission) to protect its system from hacking, which resulted in the data breach and the dissemination of customers' private information. Such a claim by shareholders, again, absent an exclusion for claims arising out of data breaches, would likely be covered under a D&O policy. As to claims

by customers for invasion of privacy, D&O policies exclude invasion of privacy claims.

Commercial crime policies may also provide coverage for losses resulting from data breaches. They often include computer fraud coverage for loss or damage to property resulting from the use of a computer to fraudulently transfer that property. This coverage is found in fidelity policies such as Banker's Blanket Bonds and other crime policies issued to financial institutions and businesses. Insurers construe this policy to provide coverage for losses resulting from computer hacking.

First-party losses for repair and replacement of the operating system and business interruption losses resulting from the system going down may be covered under the company's property and business interruption policies. Courts have found that damage to or corruption of data is property damage. Again, absent exclusions for damage to data or computer systems, these policies may provide coverage.

Many insurers now offer cyber insurance policies with the first and third-party features outlined above. Considering the prevalent risk of cyber-attacks, these policies will soon become a part of the insurance program of all major businesses. The likely inclusion of exclusions in traditional policies for losses resulting from cyber-attacks and data breaches will necessitate the purchase of cyber insurance.

All of the foregoing information was provided to the GC, who in turn informed the CEO and crisis management team. They braced themselves for the onslaught of claims arising out of the cyber-attack.

The GC recommended the consideration of establishing a fund to compensate their customers from losses resulting from the data breach. The GC was tasked with providing the team with the details of a plan and the identity of neutrals who could administer the claims process to determine the legitimacy of the claim and the extent of the loss. The GC consulted with the company's insurers in order to preserve the claim for coverage under the company's existing coverages. A meeting with the insurers and neutral to design the process was immediately scheduled. Following the meeting, the claim and settlement fund was established and announced to customers and the public.

Bruce A. Friedman, Esq. is a JAMS neutral, based in Southern California. He is an accomplished dispute resolution professional who has mediated a wide range of disputes including insurance, class action, professional liability, business, real estate and entertainment matters. He can be reached at bfriedman@jamsadr.com.