Cybersecurity Risk Management is Complex

By Lynda A. Bennett 4/13/2015

Hardly a week goes by without a new data breach being reported in the news. Companies of every size and industry are scrambling to manage their cybersecurity risks by implementing best practices for information management and creating disaster plans to anticipate and mitigate a breach. Through those processes, companies are coming to grips with the fact that one of the largest security risk factors they have is within their workforce: both negligent and disgruntled employees.

Although employers are managing workforce-related risks in a variety of ways, one area that is being overlooked by employers is the insurance coverage that may be available to manage security risks related to their workforce.

Variety of Tools

Companies typically have a written policy that informs employees that all information generated or accessed at work is property that belongs to the company and that most information should be kept strictly confidential. As such, employees should not expect privacy on electronic devices used for work.

Many companies have started to send regular e-mail blasts to all employees reminding them of privacy and security policies, which not only reinforce the policies but also let employees know that management is watching.

For higher-level employees, or those who have access to particularly sensitive business information, employers may require the execution of a nondisclosure and confidentiality agreement.

Some companies also have begun using data analytics to monitor employee conduct, for example, tracking keycard entry into work facilities at odd hours and tracking access to, and printing of, sensitive documents.

Finally, many companies require employees to use bitware technology to secure electronic devices used for work, such as encryption software, secure passwords and high-tech fingerprint scanners.

Insurance Coverage

However, most companies do not know that insurance coverage under their traditional insurance policies is incrementally disappearing.

There are steps they need to take right now to retain that coverage or receive appropriate premium reductions so that they may pursue dedicated cyber coverage to protect against cybersecurity risks.

There are three primary insurance policies that directly intersect with employment-related risks:

- Employment practices liability (EPL).
- Fidelity/crime.
- Directors and officers (D&O).

EPL coverage protects the company against lawsuits brought by employees that arise out of an existing (and sometimes prospective) employment relationship. A fidelity/crime policy protects the company when an employee engages in theft, embezzlement or other dishonest behavior. Finally, a D&O policy protects company directors, officers and sometimes all employees when they are sued for wrongful acts committed within the scope of their employment.

In the last couple of years, cyber-related exclusions have started to creep into each of these policies. For example, some insurers have placed an "employee privacy violation" endorsement on their EPL policies that eliminates indemnity coverage for a security breach that results in unauthorized access to confidential employee information such as Social Security numbers, medical records and credit/debit cards, and provides only a modest sublimit for defense costs associated with that kind of breach. Without the endorsement, companies have defense and indemnity coverage, up to the full limit of the policy, because EPL policies typically provide coverage for invasion of privacy claims brought by employees.

Similarly, many crime/fidelity policies are now being amended to include an incredibly broad and patently ambiguous "protected information" exclusion. The exclusion bars coverage for any loss that results from the theft, disappearance, destruction, unauthorized use or disclosure of, unauthorized access to, or failure to protect any confidential information or personally identifiable information that a party has a duty to protect. While that exclusion is sure to be subject to careful judicial scrutiny in the future, it nevertheless represents a substantial reduction in coverage when added to a crime policy. Companies must make efforts to avoid its inclusion in their policy or else should receive a premium reduction.

Finally, D&O policies also are seeing an incremental reduction of cyber-related coverage. For example, many D&O policies now "add" coverage for crisis management expenses associated with a security breach but the coverage is subject to a very low sublimit that, in most instances, will be insufficient to address all costs associated with the breach. Companies need to question why this coverage needs to be "added." Further, they must carefully consider how an insurer may try to use this coverage "enhancement" as a means to actually reduce available coverage under the D&O policy.

The bottom line is that managing employment-related cyber risks is complex and securing insurance coverage for them is even more complicated. Companies should work with experienced coverage counsel to audit their current insurance program to determine whether any cyber- or privacy-related exclusions have been added to their policies and, if so, whether a premium reduction has been provided that is commensurate with the coverage reduction. Companies also must give careful consideration to whether dedicated cyber coverage must be purchased to protect against their largest risk factors.

Lynda A. Bennett is the chair of Lowenstein Sandler LLP's Insurance Coverage Practice in New York City and Roseland, N.J., and can be reached at lbennett@lowenstein.com