P&C Pro-File

Workplace and safety tips brought to you by: Montgomery & Graham

DID YOU KNOW?

As many as 110 million customers may be affected by the massive data breach that hit Target during the holiday shopping season. In early January, the retail giant announced that the personal information of an additional 70 million customers—including their names, addresses and phone numbers—may have been stolen. This is much worse than its initial estimate that 40 million customers' payment data was stolen.

As more details of the breach emerge, find out how cyber insurance is helping Target get through every company's worst nightmare.

Cyber Insurance Helps Target Cover Some of Its Breach-related Costs

On Jan. 10, Target announced it would offer one year of free credit monitoring, identity theft protection and zero liability for the cost of fraudulent charges to all its customers. Offering this is a smart move on Target's part to protect its credibility and to maintain good customer relationships. But offering all of this isn't cheap.

According to the Ponemon Institute's 2013 Cost of a Data Breach study, the average cost of a breached record is $188, which includes both direct and indirect expenses incurred by the organization. Even just the indirect expense of communication—sending customers notification of the incident and setting up a call center for customer inquiries—can cost a lot.

Target has at least $100 million of cyber insurance coverage. If you multiply the number of customers affected by the breach by the average cost of a breached record, the total cost of this massive breach exceeds the limits of its policy. But the insurance will help cover a big chunk of the customer notification and credit monitoring costs, as well as expenses related to hiring a computer forensics investigator, fines and more.

If a data breach happens to your company, how would you pay for the damages? Contact Montgomery & Graham to learn more about cyber insurance.

MONTGOMERY AND GRAHAM
Bringing you tomorrow's insurance planning strategies today.

Let OSHA Know What You Think

Given the "polar vortex" and other nasty weather this winter, protecting your workers from heat stress may not exactly be at the front of your mind right now. But in preparation for the weather warming up, the National Institute of Occupational Safety and Health (NIOSH) is asking for your input on how to revise its standard on occupational exposure to heat.

Questions have been raised regarding the current occupational heat standard—which was published in 1986—and whether it needs to be updated with new research and findings regarding measuring techniques, the effects of heat, and recommendations for occupational standards, prevention and control.

(Continued on next page.)

Contingency Plans Key in Data Breach Response

In what's turning out to be the largest retail data breach in U.S. history, cyber criminals left Target's website alone and targeted its brick-and-mortar locations instead. Perpetrators tampered with the point-of-sale (POS) systems at the checkout registers that connect to networks, proving that "cyber risks" encompass more than just a company's website.

As technology evolves, cyber criminals adapt by developing even more sophisticated and targeted attacks. Devoting resources to cyber risk management is no longer just "a good thing to have"—it is critical for businesses of all sizes to prevent a breach, or at least be prepared to respond and recover as quickly as possible if one occurs.

An essential part of cyber risk management is having a data breach contingency plan in place. A contingency plan involves identifying what could go wrong with your data security and all the different results that might occur from the worst-case scenario.

To develop a contingency plan, companies must look internally at their data security to ensure that access to critical systems and data is protected from the inside through intricate access controls. These controls include encrypting sensitive data, using role-based monitoring to detect suspicious insider activity and adopting the National Security Administration's new "two-person rule," in which a second person must approve any attempt to access a company's sensitive information.

As you prepare your contingency plan, it's important to know what your insurance covers. For incidents like Target's, cyber insurance can help a company swiftly establish a call center to respond specifically to customers' breach-related calls. Among other things, it can also cover damage or loss to your data system. Talk to your representative at Montgomery & Graham to make sure you have appropriate cyber coverage to put key components of your plan in place in case a breach occurs.

Input on OSHA Rules

(Continued from previous page.)

NIOSH is holding a public meeting on Feb. 13 for review and discussion of its draft document "Criteria for a Recommended Standard: Occupational Exposure to Heat and Hot Environments." You may also submit written comments on this draft through Feb. 25.

OSHA is also seeking additional input on another standard: its proposed rule to improve workplace safety and health through better tracking of workplace injuries and illnesses. In response to a request from the National Association of Home Builders, OSHA is extending the comment period on this rule to March 8, giving the public an additional 30 days from its original deadline.

The proposed rule would amend recordkeeping regulations to add requirements for the electronic submission of injury and illness information that employers are already required to keep under OSHA's regulations for recording and reporting occupational injuries and illnesses.

If you're interested in submitting comments electronically for either standard, visit www.regulations.gov.

P&C Pro-File

Workplace and safety tips brought to you by the insurance professionals at:
Montgomery & Graham