London Drugs Cyber Attack Lessons Learned

The cyberattack on London Drugs highlights the need for companies to have cyber-insurance and employee Internet Security training.

The recent cyberattack on London Drugs has underscored the critical need for comprehensive cybersecurity measures and insurance coverage for large corporations. After the cyber incident, London Drugs had to shut down all 79 of its Canadian outlets for over a week, only recently beginning to reopen about half of them.

During the closure, London Drugs presented its staff with various work options, including merchandising and store maintenance, or using vacation pay for those who opted not to work.

But an employer can't force an employee to accept going days or weeks on end without work.

Having employees use their vacation or banked overtime pay might have been a necessary "middle ground" in the sense that employees can continue paying their own expenses, but then they lose their vacation time later on. The alternative is laying off employees, but that can be a breach of an employment contract and the duty to provide work and compensation for it.

Companies, like London Drugs, that get hit by cyberattacks can face costs in the tens of millions of dollars to address the fallout of a technical issue, as well as lost sales. They may also face penalties for having to delay accepting merchandise from suppliers or not being able to pay invoices, which would also involve breaches of contract that could be contested in court.

In fact, in some instances, a cyberattack can result in needing more employees or hours, such as when self-checkout kiosks go down, which is what happened at national grocery retailer Empire Co. stores, including Safeway, Sobeys, IGA, FreshCo, and Thrifty Foods, among others, in Fall 2022.

For Managers, these incident are a potent reminder of the need for robust cyber insurance and employee training programs. Such measures not only mitigate financial risks but also ensure that staff are prepared to prevent data breaches, which are often facilitated through simple errors like unsafe email and internet practices. Over 80% of data breaches begin with employee actions, emphasizing the necessity for ongoing training in cybersecurity awareness.

Even though insurance for cyberattacks is worth having, companies have to protect against many other unforeseen events too.

Organizations like yours should have clear policies for handling closures due to various emergencies, including cyberattacks. These might include details on work-sharing, remote work arrangements, and utilizing backup systems.

Having a cyber insurance policy is increasingly vital, given the growing frequency of digital threats. To qualify for such insurance, companies must demonstrate effective cybersecurity strategies, including employee training and robust security policies.

As a member, you can access model policies, procedures and other tools to help get you where you need to be, but we also have the training your employees need to make sure they aren't letting cyber criminals in through the backdoor.

Click here to find out more about HR Insider and SafetyNow's cyber security training and let the experience of London Drugs serve as a cautionary tale, urging proactive measures rather than reactive responses.