HR Insights

Brought to you by: The Medical Society of Virginia Insurance Agency

MSV℠ INSURANCE AGENCY

HR's Role in Preventing Cyberattacks

Cyberattacks are a growing concern for employers across the globe but especially for those in the United States. According to the Identity Theft Resource Center, the number of reported U.S. data breaches rose 68% between 2020 and 2021, increasing to a record-setting 1,862 incidents. Of these breaches, 83% involved sensitive information, such as Social Security numbers.

These breaches targeted various organizations and industries, including those in manufacturing, utility services and finance. Essentially, any business that retains potentially valuable information could be a target; cybercriminals are frequently looking for the personal information of everyday citizens to sell or use to gain access to other systems.

Oftentimes, cybercriminals breach organizations via their own employees; all it takes is one employee clicking into a phishing email (i.e., a fraudulent message intended to trick recipients into compromising important data).

This is where HR comes in. HR teams are often tasked with communicating policy updates and workplace expectations. When it comes to cybersecurity, HR is naturally suited to partner with IT and provide basic educational resources.

This article offers tips to help HR teams protect employees and their organizations from cyberattacks.

Understand the Risks; Have a Backup Plan

While it's true that cybercriminals frequently target individuals' personal information, that's not their only goal. Sometimes, malicious actors will then take that personal information and use it to gain access to other secure points—potentially affecting other systems beyond the breached organization itself. For instance, a cybercriminal may steal an employee's login and password, then use those details to access customer databases or even critical infrastructure.

A recent example of this came in 2021 when cybercriminals took down Kronos, the ubiquitous timekeeping software. With the cloud-based system down globally, employees couldn't clock in or out—time punches were simply inaccessible. Obviously, this proved very disruptive for payroll and time tracking. Yet, the larger takeaway is that even if an employer does everything right, they can still be impacted if a vendor experiences a cybersecurity breach.

That's why it's important for HR teams to think about the vendors and systems they rely upon. These may include timekeeping software, case management software or learning management systems. Consider what would happen if any one of those tools stopped working or became inaccessible. How would that impact operations?

Considering these potential scenarios can help HR teams better strategize their responses. For instance, if timekeeping software were to break down, perhaps employees would be required to use an HR-provided paper form to track their time.

Additionally, with the vulnerability of cloud-based systems, HR teams can think about regularly backing up and archiving critical information, including customer details, time-tracking data or transaction receipts. Essentially, if a vendor system breaks down, HR still needs to ensure day-to-day operations can run smoothly.

Develop Cyber Training and Contingency Plans

Preparation is key for protecting an organization from cyberattacks. This primarily entails ensuring monitoring and security measures are in place to prevent breaches and detect when they occur. While this preparation is a responsibility for IT, HR teams can partner with them to help contribute to cybersecurity in their own way: employee training and contingency planning.

Every employee in an organization should be trained on proper cybersecurity protocols and best practices. This includes knowing how to spot a phishing scam, maintaining strong passwords, using unique passwords for different logins and reporting suspicious database activity. While HR teams likely aren't comprised of IT experts, they can still help disseminate these and other cybersecurity best practices to employees. Even basic precautions can make a huge difference in protecting against breaches of critical data.

However, not every breach is preventable, nor are all breaches the same. It's one thing for a cybercriminal to get a list of first names; it's another thing for them to steal both names and Social Security numbers. Moreover, employers can still have their data compromised even if they take all the right steps. After all, a breach may occur at a third-party vendor, a situation over which employers have no control. This means it's also vital for HR teams to strategize about cyberattack contingency plans.

Essentially, these plans can help employers make sense of a data breach once it occurs and kick off the recovery process. Generally, a cyberattack contingency (or response) plan should cover the following aspects:

- **What data has been impacted?**
- **How sensitive was the data** (i.e., does the breached data include addresses, Social Security numbers or banking information)?
- **What is the employer's obligation to report the data breach** (i.e., sometimes customers, employees, the government or all the above need to be notified)?
- **Based on the type of data breach, how quickly must the incident be reported to applicable parties?**

Depending on an employer's state and industry, the answers to these questions will vary. That's why it's essential to address these issues in a cyberattack contingency plan before a breach occurs. Employers should speak with legal counsel for help understanding their coverage risks.

Assess a Breach and Be Responsive to Employees

If and when a data breach occurs, HR teams must stay calm, as employees will be looking to them for messaging and next steps. HR will need to respond to employee concerns about the compromised data; other teams will likely address external messaging while HR focuses internally.

More specifically, a data breach that affects an organization almost certainly will affect its employees, even if the compromised data seems unrelated to staff. That's because employee credentials are often stolen to access larger databases. While employee credentials may not be the intended target of a breach, they can still get swept up during the cyberattack along with other pieces of personal data.

In other words, regardless of the type of data breach or its scope, employees may have concerns about their own information when one occurs. Therefore, HR teams should be ready to field employee questions related to a breach and have meaningful response measures in place. For instance, if employee data is compromised (potentially or actually), employers may provide free identity theft protection or credit activity monitoring services to their staff.

Conclusion

Cyberattacks aren't going away any time soon. In fact, they're likely to increase. According to the Identity Theft Resource Center, ransomware-related cyberattacks have doubled during each of the last two-year periods. This means now is the time for employers and HR teams to prepare for eventual cyberattacks by training employees and solidifying contingency plans.