The Personal Data of Your Employees Was Hacked… **What's Next?**

Your company has experienced a cyber security incident. In addition to dealing with potential public, media, and regulatory scrutiny, you must take into account your most pertinent audience – your employees. Employees are the ones on the front lines during a breach, answering questions about what happened to their friends, neighbors, and each other. In the instance employee data has been compromised, there are a few basic steps to consider. The below checklist covers the basics for communicating openly and directly with your most important stakeholder group while reassuring them that the situation is under control.

Communicate Early, Transparently & Empathetically

When a cybersecurity investigation determines that employee data has been affected, it is crucial that they be informed – as appropriate – as soon as possible. Any leaks or rumors that a company did not disclose this information in a timely manner may not only run amiss of disclosure requirements but may also negatively impact trust in the company. Even if not all the information is known, transparent and sincere communication will instill confidence among employees. Communications can also be creative; leverage new technologies to share video messages or hold virtual town halls.

Establish Open Lines of Communication

Following an initial employee communication, companies should create internal channels for employees to reach out to a designated taskforce if they have specific questions about the data breach. While FAQs should be used for standard questions, having an easily accessed "hotline" allows employees to have more specific concerns addressed – especially as many companies continue to work remotely. The hotline should also be used for more than just questions; going through a data breach can be an emotional experience, especially when their data has been impacted. Make sure HR is involved in these communications to address employees' concerns.

Launch Training Programs & Awareness Initiatives

Instituting a new internal training program in response to the cybersecurity incident will serve to both educate employees on best practices and emphasize to employees that the company is doing everything it can to protect their data. In addition to these trainings, the company should outline the other steps it is taking as well.

Develop Talking Points & FAQs Specific to Each Internal Stakeholder Group

Employees will have plenty of questions when their company is going through a crisis – particularly when that crisis involves their own information. A set of talking points and responses to Frequently Asked Questions should be drafted as soon as possible – and then regularly updated – to ensure that employees receive accurate and consistent information.

Follow Up with Regular Communications

As developments occur, employees should be among the first to know. Setting up regular communications with employees during the investigation – as appropriate – will help reassure employees that the company is addressing the incident and is answering their questions proactively. Updates should explain what the company is going to do to make things right for its employees, including credit monitoring, identity theft protection, dark web monitoring, or other protective measures.

Check the Pulse

Checking in with employees regularly makes sure that their concerns are heard and that the company is effectively addressing those concerns. While informal surveys present the best opportunity for unfiltered feedback, these check-ins can also take place in staff meetings (virtual or in-person) or individual meetings.

FTI CONSULTING™