Making a List, Checking it Twice: Avoiding Cyber Attacks During the Holidays

December 24, 2025 Natalie DuBose, Reese Letourneau

PRACTICES Privacy and Cybersecurity, Insurance Recovery

What's the Concern?

During the holiday season—specifically, Christmas Eve, Christmas, New Year's Eve and New Year's Day—there tends to be a spike in cyber attacks on companies. Cyber attackers target this time of year due to staffing and information technology (IT) shortages, slower response times and increased online activity, especially in retail and banking industries. Together, these circumstances lead to scenarios where attackers exploit the distractions and year-end pressure that many companies face as the holidays approach.

No Industry is Immune

While any industry can be a target of a cyber-attack, often retailers, financial institutions, logistics companies and travel companies find themselves the targets of cyberattacks during the December to January months. For example, in December of 2023, VF Corporation, a company that owns and operates various apparel and footwear brands, experienced a data breach as a result of a ransomware cyber-attack. This attack disrupted the company's holiday sales and e-commerce for weeks leading into the holiday season. The attack on VF Corporation is not unique—many companies, including Staples, British Telecom, Change Healthcare and Blue Yonder, have experienced cyberattacks during the holiday season over the past few years.

How Can I Prevent Cyber-Attacks?

Lists aren't only for Santa! The best way to prevent cyber-attacks leading into the holiday season (or really any time of year) is by making a list of best practices and plans to follow in the event of a cyber incident.

- **Step 1:** Follow good cyber hygiene practices, including using strong passwords, enabling multi-factor authentication and keeping software up to date. Review your cyber policies and understand what they require and then implement those systems. Many companies find themselves without coverage because the policy required a practice that the company did not implement, for example, independent verification of payment requests through an alternative method.
- **Step 2:** Prepare for the unexpected by creating and maintaining an incident response playbook, which should include your risk management team. Be sure to consider particularly sensitive times when a cyber-attack may occur, including on the eve of bonuses, last day of the year, etc. If you don't have a playbook prepared yet, work with your risk managers, insurers and outside counsel to develop a plan.
- **Step 3:** Consider the team you will need to have in place in the event of a breach (forensics experts, outside counsel, breach coach, coverage counsel, etc.). Work to get those individuals approved beforehand through your internal systems and with your cyber or other insurer, if applicable.

- **Step 4:** Institute regular training and simulated phishing exercises for employees and conduct desktop exercises for your incident response team to practice how your company would respond in the event of an attack. Your cyber insurer may offer these trainings.

What Happens in the Event of a Cyber-Attack?

If you find yourself the victim of a cyber-attack, time is of the essence. Promptly notify your insurer, giving careful consideration to the facts known and the language of insurance policy when preparing your notice of claim, with the assistance of your coverage counsel, if possible. The response will likely involve a coordinated effort between coverage counsel, your risk manager, insurer, breach coach and outside counsel to address the insurance claim, any potential ransom payment, government notifications and required disclosures. Make sure you have the right team in place and bring them in as early as possible.

With the right security, planning and team in place, you can take some of the stress out of the holiday season!