COALITION CLAIMS SCENARIO

A Golden Ticket is all that's needed to access your restaurant's credit card transactions

The last thing you want is to have your business disrupted by a cybersecurity failure.

Nobody expects to be the victim of a ransomware attack, funds transfer loss, or data breach. But, once a cyber incident occurs, it's important to know you have a team of experts ready to help you figure out what happened — and what happens next. This series shares real stories from Coalition policyholders who navigated a cyber insurance claim. The organizations will remain anonymous to protect their privacy and security.

Like Charlie peeking into the Willy Wonka Chocolate Factory, cybercriminals can access a behind-the-scenes look into your business with what is known as the Golden Ticket attack. This type of attack starts with a deceptively simple phishing email. Once the perpetrators have access, they elevate their own credentials within your network to access other accounts. One Coalition policyholder — a restaurant chain — experienced the speed and scale at which a Golden Ticket attack can impact a business's integrated systems.

Incoming call from the FBI

During the holiday season — the busiest time of year for the hospitality industry — a restaurant group received a phone call from the FBI notifying them that data from four of their servers had been compromised by tenacious threat actors known as FIN8. This breach impacted three corporate servers and one restaurant server containing customer credit card information. As an organization that completes $8 to $9 million in credit card transactions annually, the restaurant group had to move quickly to ensure the least amount of damage possible.

VICTOR | Coalition®

They contacted Coalition within 24 hours, and remediation began immediately with the forensic discovery process, shutting down the VPN, and reaching out to the FBI for more information.

Securing the system and managing the fallout

Within two days of being notified, Coalition utilized Script Collectors to identify the intruder across all networks, determine how FIN8 was accessing the restaurant's networks, what they were viewing, and whether or not they could regain access to the victim's network. With all this information, the breach resolution team led by Coalition wrote a script to kick the threat actors out and reclaim control of the network.

Unfortunately, even with Coalition's quick action, the breach impacted more than 13,000 consumer credit cards. Coalition provided all notification services to the impacted consumers on behalf of the restaurant group and covered all litigations, depositions, and negotiations during the resulting two-year class action lawsuit, while also managing the regulatory fallout. In the end, the restaurant group only paid $21,000 out-of-pocket of the $3,000,000 claim.

Have a plan for data breach prevention and remediation

To protect the restaurant group from future cyber incidents, Coalition recommended the following best practices:

- Segregate networks. Network segregation can limit the impact of intrusion by making it significantly more difficult for a threat to locate and gain access to sensitive information and provide the organization and its partners more time to detect the intrusion. Unfortunately, the restaurant operated with a 'flat' environment that only required the threat actors to access a single network to reach their main network.
- Stay up to date. Another best practice involves performing frequent and thorough backups on important data to protect your business against a total loss after a ransomware or phishing attack. Coalition also suggests replacing all end-of-life software and training employees to identify and respond to phishing emails.
- Require two-factor authentication. To make their systems more secure against future attacks, Coalition recommended the restaurant group enforce a two-factor authentication process for administrative access to internal networks.

Coalition and Victor are here to help you manage risk

With a Coalition cyber policy, you gain access to Coalition Control, an integrated platform that lets you take a proactive approach to manage cyber risk, all for free. An Automated Scanning & Monitoring tool finds organizational risk and shows you how to fix it before the unthinkable happens. Sign up with just your email address and start controlling your risk right away. You can't afford not to.

Visit us at victorinsurance.com to learn more.

Each claims scenario is strictly documented for illustrative purposes only and provides an example of what a policy could cover. It is intended to provide a general overview of the program described. Please remember only the insurance policy can give actual terms, coverage, amounts, conditions and exclusions. Program availability and coverage are subject to individual underwriting criteria.

© 2024 Victor Insurance Managers LLC | 213600
Victor Insurance Services LLC in MN | DBA in CA and NY: Victor Insurance Services | CA Ins. Lic. # 0156109