Why More Restaurants Should Purchase Cyberinsurance

Related People:
Jennifer Black Strutt
J. Wylie Donald

Law360

05.21.2015

Restaurants face a cybersecurity threat that is pervasive and alarming. P.F. Chang's China Bistro, the Dairy Queen and Jimmy John's are just a few of the more notable examples of restaurants that have fallen victim to hackers, with each security breach affecting customers in multiple locations throughout several states. Cybercriminals target businesses that have a high volume of credit and debit card transactions, as well as a system that is easily penetrable, such as a point-of-sale system or remote-access desktop service. Restaurants (and especially franchise units) typically fit this description and, therefore, may be particularly vulnerable to cyberattack.

The potential costs of a security breach may be significant. According to the Ponemon Institute, the hospitality sector has a per capita data breach cost of $93 for each lost or stolen record containing sensitive information. Moreover, a cyberevent may be a public relations nightmare because the public may lose confidence and trust in the company. There is another aspect of harm that is somewhat unique to merchants given their relationship with the payment card industry.

Unlike consumers who may not be liable for credit card data theft, merchants have a duty to protect that data. Entities that process, store or transmit cardholder data are required to comply with the Payment Card Industry Data Security Standards to protect cardholder data, and the failure to do so may result in fines. In the event of a breach, the contract between a credit card processing company and a merchant may permit the processing company to collect and hold back funds from the merchant's credit card transactions, thereby creating a cash flow deficiency. Given the unexpected cost associated with a security breach, the potential decline in business and a hold-back of funds, a single breach could threaten the future existence of a company.

What should be done to minimize the cyber risk? Merchants should, among other things, protect their data infrastructure by patching holes in firewalls and creating unique accounts and passwords for all users. Merchants also should protect the data itself, with encryption or tokenization.

One essential but often overlooked component is insurance. An insurer will not issue a cyber policy unless the applicant establishes a sufficient level of cybersecurity, so, if nothing else, the underwriting process may require a company to become better prepared. But there is something else: if an attack does happen, the insurance payment and the carrier's cyber incident response services will soften the blow. The utilization of cyberinsurance is not uniform. While some sectors, such as health care, are reported to widely purchase policies, other sectors, such as hospitality, are not so diligent. Marsh LLC, a global insurance broker, reports that only 26 percent of its clients in the hospitality and gaming sector purchased standalone cyberinsurance in 2014. One reason for this may be that cyberinsurance is one of the more confusing lines of coverage to navigate.

Why More Restaurants Should Purchase CyberinsuranceDownload