Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Why More Restaurants Should Purchase Cyberinsurance

Law360, New York (May 21, 2015, 10:25 AM ET) --

J. Wylie Donald

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.

Cyberinsurance Basics

The decision to purchase cyber coverage (and include this investment in the risk management budget) is only the first step. The company must carefully analyze its specific risks to ensure the right coverage is purchased. Cyberinsurance may cover first-party loss and claims brought by third-parties (i.e., liability coverage).

There are many first-party cyber coverages available, which may include:

• *Privacy breach notifications* — The Ponemon Institute reported the average notification costs in 2014 were $510,000 per breach, but this amount may be higher or lower depending on the severity of the breach and the number of individuals affected.

• *Business interruption arising from computer disruptions* — In an Advisen Cyber Liability Journal article entitled "Uninvited Guests Help Themselves to Hotel Restaurant Data," Damien Magnuson reported: "With nearly 60 percent of reservations now being made online, even a short interruption in service may be costly. Additionally, if a company is not able to accept point-of-sale card payment for even a few hours, the loss may be extensive."

• *Cyber incident preparation and response* — A common coverage is for reimbursement and assistance with crisis management expenses. This includes pre-event identification of crisis response and forensic experts. Insurers also can provide cyber assessments to identify vulnerabilities before they are exploited.

• *Cyber extortion* — Although this sounds like a fictional movie plot, cyber extortion is a real risk. Domino's Pizza in France and Belgium was targeted by hackers who threatened to release stolen details on more than 600,000 customers if the company failed to pay a ransom.

First-party coverage also may include computer disruptions (introduction of viruses or malware that destroy hardware, software or data) and physical damage arising from computer disruption.

There are a variety of liability coverages, which typically include:

• *Privacy liability* — loss of personally identifiable information of customers. In litigation arising over the P.F. Chang data breach, plaintiffs alleged "P.F. Chang's security failures enabled hackers to steal financial data from within P.F. Chang's systems and ... subsequently make unauthorized purchases on customers' credit cards and otherwise put class members' financial information at serious and ongoing risk."

• *Security liability* — contribution to loss arising from malware, viruses, hacking, social engineering and employee malfeasance. For example, The New York Timesreported a case where a petroleum company was electronically infiltrated when its employees inadvertently downloaded malware from a Chinese restaurant's online menu. The article does not say whether the petroleum company pursued any claims against the restaurant.

• *Internet/social media liability* — libel, slander and trademark and copyright infringement in those media. Online reviewers can find themselves subject to suit — and found liable — for defamation.

Once a company identifies which coverages it needs, it must carefully analyze the coverage offered under a particular policy. Unfortunately, the typical format of the cyber policy usually makes this task difficult. Let's take a cyber policy issued by a nationally known insurer as an example. This policy includes ten separate insuring agreements, 59 defined terms, 15 pages of conditions and exclusions divided into four separate classes of application. This means that if a company has not purchased all 10 coverages, the policy includes numerous irrelevant provisions that add to the confusion of an already confusing document. Additionally, in many instances, the "definitions" narrowly describe the events that trigger coverage. A plain reading of the coverage grant without sufficient understanding of the defined terms may lead to the incorrect assumption that coverage for a particular risk is provided, when it is not. Further, not all definitions or exclusions apply to all coverages. Therefore, one must take each type of hypothetical loss and trace it through the policy to determine whether there is coverage and the outcome for one kind of cyber loss may differ from the outcome for another kind of cyber loss.

One also must consider the relevant time frame of the coverage it needs. Cyber coverage is typically written on a "claims-made" basis, meaning that if no claim is made during the policy year (or during an extended reporting period), there will not be coverage, even if the covered event occurred during that year. If a company is interested in purchasing coverage for an undiscovered event that occurred prior to the cyber policy's inception date, the policy must include a "retroactive date," which means that if an event occurs after the retroactive date and leads to a claim during the policy year, there will be coverage. However, any event occurring before the retroactive date will not be covered. Additionally, a series of related events occurring over an extended period may be determined under typical policy language to occur at the date of the first event; so if the first event precedes the retroactive date, the insurer likely will argue there is no coverage.

In view of the potential delay in discovering a security breach, having a retroactive date that does not go back far enough could be problematic. For example, in June 2014, P.F. Chang's reported a security breach involving the stolen credit and debit card data during an eight-month period from Oct. 19, 2013, to June 11, 2014. Using that scenario as an example, if the restaurant's cyber policy carelessly set its retroactive date for the beginning of the policy, say Jan. 1, 2014, then if the claim were made in 2014, an insurer may argue there is no coverage for the loss because the first of all related events occurred in 2013, prior to the retroactive date.

In conclusion, a company must be deliberate and careful in purchasing cyber coverage. Specific risks must be understood and the appropriate coverage identified. Because cyber coverages are so varied and the policy terms, conditions and exclusions often precise, a company that decides to buy cyberinsurance without competent and thorough analysis may discover at an inopportune time — i.e., in the midst of a cyber incident — that its cyber policy does not cover the loss.

—By J. Wylie Donald and Jennifer Black Strutt, McCarter & English LLP.

J. Wylie Donald is a partner in McCarter's Washington, D.C., office.

Jennifer Strutt is an associate in McCarter's Stamford, Connecticut, office.