SOCIUS

www.sociusinsurance.com

Restaurants Beware: Hackers are Hungry!

What you restaurant clients need to know.

By Laura Zaroski, J.D.

Restaurants, pubs and diners all over the country serve hungry and thirsty people everyday. From white tablecloth establishments to the local taco joint, almost all restaurants take credit/debit cards for the vast majority of their transactions, resulting in millions of daily transactions. One swipe and customers go on their way. But behind the scenes, restaurants nationwide are suffering at the hands of cyber thieves who target restaurants in an effort to steal their treasure trove of daily credit card information.

A recent VISA report indicates that restaurants now account for close to 73% of the data breaches in United States. Why restaurants? Low effort - high yield. The smaller the better! Cyber thieves know that the smaller the establishment, the more likely they are to have weak securities in place and will be the most vulnerable to an attack. With a single hack, a thief can reap a whole day's worth of stored credit card data, while a continual harvest can produce months and even years of data. How is this possible? Thieves can break through weak firewalls, taking advantage of the all too common use of default passwords, providing access to non-segmented networks where all web connected systems can talk to each other (i.e. security cameras, payment processor, computer, DVR, WiFi), unsecure remote access systems, and unaware employees. How easy can a hacker get into the system? A hacker can simply sit in the parking lot or even the dining room, and simply gain access to a network by hacking into one of the establishment's multitude of access points. Once in, they can steal current data or install Malicious Software ("malware") on the establishment's system, which then allows thieves to routinely access the credit card information that is collected each day. Failure by the establishment to detect and remedy this intrusion can lead to legal liability from customers alleging failure to adequately protect their credit card information.

Companies that have been breached often do not learn of the breach until they are notified by customers who have had their credit cards compromised, or even worse, when Visa/Master Card detects a pattern of compromised cards from one point of sale and contacts the establishment for reimbursement. Following a breach of customer credit card information, establishments will be required to notify affected customers of the breach. Notification is complicated and costly, and must be done in a timely manner. Often, the after-effects of a breach include significant IT costs to remedy the breach, determine what information was compromised, and to repair the system. Lawsuits by customers and a significant drop in business revenue is also common, so there's significant exposure to both first and third party loss.

Why are these types of breaches becoming so common? Because hackers and thieves can earn quick cash. The going rate on the black market for credit card information is about $20 per card. Not bad for a day's work! (or not having to do a day's work...)

Restaurant owners should take heed and take the security of their clients' information very seriously. Establishments that process credit card information should review their security systems, update virus software routinely, train employees on security and best practices, and consider a risk management plan which would include a network security and privacy policy ("Cyber Insurance").

As restaurants are a growing target for cyber crime, if you have restaurant clients (or other clients that take credit card data) you should consult with them about their risks and liabilities. Based on their risk tolerance, consider whether the risk of being a victim of cyber theft is a risk they want to self-insure, or whether they would prefer to outsource this risk via a Cyber/Network Security policy. In today's high tech world, a well thought out risk management plan to safeguard a system against cyber theft is invaluable- and should work in conjunction with Cyber/Network Security insurance, as no computer system- regardless of size or sophistication- is 100% hack-proof.

SOCIUS

www.sociusinsurance.com

Restaurants Beware: Hackers are Hungry!

What you restaurant clients need to know.

By Laura Zaroski, J.D.

A well drafted cyber policy that is tailored to restaurant exposures will aid response in the event an establishment is a victim of cyber crime. The proper cyber policy can provide a restaurant that experiences a breach with a forensic expert who will examine their systems to find out how and when the breach occurred, determine what information was compromised, and assist in notifying the affected individuals in accordance with applicable state breach notification laws. Depending on size and revenues, cyber policies can be as cheap as $1,000 and can provide $1M in coverage.

If your clients don't want to shoulder this risk alone, having a Network Security/Cyber policy can prevent what otherwise could be a devastating blow to a small eatery, franchise restaurant or family dining establishment.

Hackers are just like the rest of us: they like to eat! Take precautions so your restaurant clients are not the ones that feed them. In the event that hackers get hungry at one of your client's establishments, strong security controls and vigilance, combined with a well drafted cyber policy that provides coverage in the case of a breach, will certainly help your clients sleep at night.

This article was authored by:

Laura Zaroski, Esq., VP of Management and Professional Liability at Socius Insurance Services, a wholesale broker, located in the Chicago office. Laura can be reached at 312.382.5373 or lzaroski@sociusinsurance.com

Joseph Gagliardo, Esq., Managing Partner of Laner, Muchin, Ltd., Chicago, Illinois, a law firm specializing in employment practices, assisted by Sara Yager. Joe can be reached at 312.467.9800 or jgagliardo@lanermuchin.com