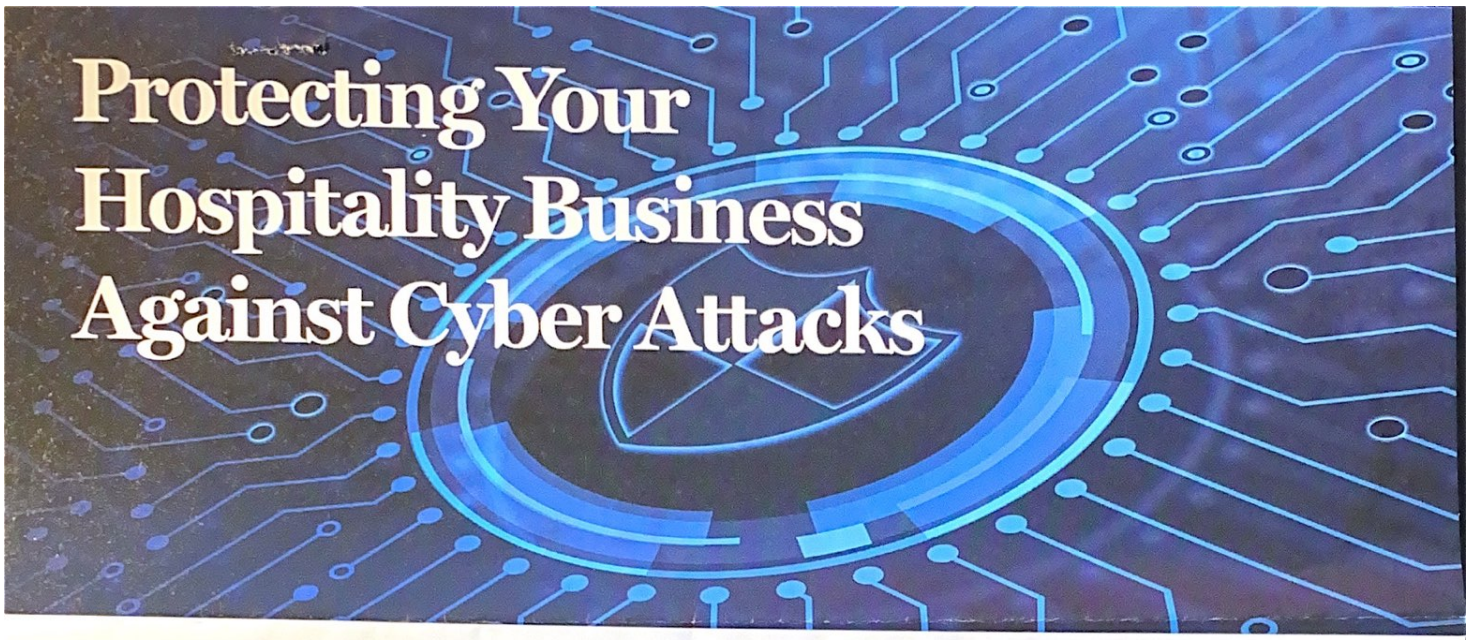

Protecting Your Hospitality Business Against Cyber Attacks

We all remember the time period when Chipotle repeatedly had one monumental security breach after another. However, data breaches can happen to big chains and small f&b businesses alike. Nearly half of cyber-attacks target small businesses and 60% of small companies who experience a significant attack go out of business.

We put together a brief guide to help you safeguard your hospitality business against cyber attacks and what to do if one happens to you.

What are common causes of data breach?

An overwhelming majority – a staggering 90% – of data breaches are due to human errors, such as a laptop or phone being accessible and stolen, employers or vendors having access to information they shouldn't, a statement being mailed to the wrong address or a WiFi account not being encrypted. However, this is actually "good" news. Since such a large percentage of cyber attacks are because of human error, there are steps you can take to mitigate the risk.

How can you prevent data breach?

The best offense is truly a good defense. Businesses can reduce the risk of cyber attacks by taking these proactive measures:

Make sure your business is Payment Card Industry (PCI) certified. The PCI Data Security Standard is an information security standard to protect credit card data.

Use secure passwords and properly secure your WiFi network. Make sure any passwords on mobile devices are encrypted and strong.

Be skeptical of emails. Question generic greetings (i.e. "Dear Customer") and threats regarding your financial accounts (i.e. "Please reply within five business days").

Stay aware of changing techniques for possible data theft. Bluetooth skimmers, RAM scrapers and malware programs are three common methods that thieves use to take advantage of businesses on a regular basis, but crooks are coming up with new methods constantly. During COVID-19, phishing scams increased 50%, according to Security Magazine. Knowledge of the enemy is important in any battle, and fighting to protect customer data is no different.

What to do if your business is the victim of a data breach?

Sooner is always better. Don't wait and don't try to "fix" the situation; you'll need professionals to step in right away.

Reach out to your financial institution.

Notify your insurance agent or carrier.

Consult local authorities.

Contact affected customers. Even though some states don't require you to inform impacted customers, honesty will serve you better in the long run. Incredible as the direct expenses from a data breach can be, reputational harm can also cause irreparable damage to a business.

Make sure services offered to customers fit the nature of the exposed data. If debit or credit card information was exposed, credit monitoring is a waste of money—without a Social Security number, a new credit line cannot be opened via an exposed credit card alone. Inform customers to keep an eye on their accounts and advise they speak to their bank about the breach. Most likely, the affected financial institution will issue a new card.

In 2021, 86 percent of customers were concerned about data breaches at restaurants with top worries cited as stolen payment information, account takeovers and hijacked loyalty rewards points. As businesses have integrated even more technology in their order systems in the past few years (QR codes, contactless ordering, etc.), these concerns are only going to grow. With the continually changing landscape, the last thing a business needs is a devastating data breach. Let's protect ourselves and give attackers something else to do.

This information is provided as a convenience for informational purposes only. It does not constitute legal or professional advice and does not establish compliance with any law, rule or regulation.

SPONSORED CONTENT

Paul Rosenquist, Security Architect at Society Insurance. Paul has been in the technology and information security industry for 20 years and is a Certified Information Systems Security Professional (CISSP).