Data Breaches: What You Need to Know to Protect Your Bar and Your Customers

by Brad Korkow

Data Breaches: The Case for Securing Sensitive Information

When it comes to data breaches, it would seem like the bigger the business, the bigger the bullseye for a potential threat. Shockingly, the opposite is true. Skimming and exposing credit card information from the small corner bar may not be as lucrative as hacking a big box retailer, but small businesses, like bars and taverns, are an opportunity for thieves to dip their toes in the water of cyber breaching. By "starting small," thieves test and perfect their methods before diving in to bigger opportunities. In fact, 90 percent of data breaches affect small businesses , putting almost every business at risk. That being said, it's more important than ever to protect your bar's—and your customers'—valuable data to ensure it doesn't end up in the wrong hands. A data breach can be especially devastating for small businesses, causing financial strain and irreparable harm. Fortunately, breaches can be mitigated. Below are common myths surrounding data breaches and tips to minimize the risk.

Data Breach Myths and Security Tips

Myth: It won't happen to my bar.

Fact: A data breach is a true threat to everyone. Most people associate a breach as the result of a hacked network or malware disruption. However, simple theft, such as stealing a laptop, zip drive or traditional file folder, are legitimate ways that information can be stolen and exposed. Consider these simple actions to keep data safe:

- Maintain payment card industry (PCI) compliance
- Shred all customer documents (e.g., receipts) that are not necessary to store
- Monitor internal systems on a regular basis for suspicious activity
- Update computer systems to eliminate known vulnerabilities
- Educate employees on data risk and exposure

Myth: If a breach happens, the bank will handle it.

Fact: In most cases, a business is responsible for paying damages associated with a data breach. Payment processors often have contracts with businesses that give them the right to recoup certain costs for a breach. For example, one major credit card merchant typically charges $2.50 per card that is exposed in a breach. That seems minimal at first, but if 5,000 cards were exposed, that costs a business $12,500 in bank fees alone. Other associated costs can include internal investigations, regulatory noncompliance, crisis management and class action lawsuits, amounting to tens of thousands of dollars in fines and expenses.

When that much money is on the line, it doesn't pay to take a half-hearted approach to data security. Investing in cyber liability insurance is a must.

Myth: A strong password is enough to keep data safe.

Fact: You know that going beyond a basic password is smart—think uppercase and lowercase letters, special characters and nonsensical letter combinations—but bars need to double down on their approach. Two-factor authentication and data monitoring are also needed for optimal data security. Two-factor authentication requires two out of a possible three options to verify a user: something you know (e.g., password), something you have (e.g., cell phone) and something you are (e.g., fingerprint). This security feature is available for a variety of programs and better secures the data that you're trying to access.

Myth: It's possible to be 100 percent secure.

Fact: Unfortunately, a business is never completely safe against a data breach. The best way to mitigate the risk is through ongoing threat education (including the latest ways cyber criminals are breaching data), security awareness training and routine system maintenance.

Cyber Liability Coverage: Small Details That Can Make a Big Difference

To keep your bar's reputation intact, going without cyber liability coverage is not an option. Unfortunately, many insurance policies do not adequately cover the various costs involved in a privacy breach. When evaluating policies, look for these important protections:

- IT forensic costs
- Regulatory fines and penalties
- Printing and mailing costs to notify customers/clients, whether or not it is required by law to do so
- Cyber extortion expenses and monies paid for a cyber extortion threat
- Legal liability—victims will seek to recover their costs, perhaps as part of a class action suit
- Electronic and non-electronic acts or accidents that result in the exposure of sensitive information

Ongoing diligence and preparation are priceless, but as more information is stored and shared online, there is greater risk of data theft. Society Insurance offers one of the most comprehensive cyber liability programs available, covering both first-party losses and third-party liability claims if the unthinkable happens. When it comes to the safety of your business, there's no time like the present to assess and upgrade your current data security measures and activate a policy with breach recovery services. Small changes will make a big difference—for both your bar and your customers.