Photo © Getty/OcusFocus

Data Security for Craft Brewers

BY
MARC SORINI AND LYNETTE ARCE

Over the past few years, news headlines have been filled with reports of large data security breaches impacting major brand names and affecting millions of people. It seems like with each new day comes a new breach. The reports are alarming for businesses and consumers alike.

No industry is immune from the soaring increase in data security breaches—not even craft brewing. Many small business owners erroneously believe they are too small to attract a hacker or fall victim to a breach. Scotty's Brewhouse, the Indiana-based brewery and restaurant chain, experienced a data breach in early January 2017 when an employee emailed 4,000 employee W-2 tax forms to an unknown scammer posing as the brewery's CEO.[1]

A data breach can devastate a business. Aside from a tarnished reputation and resulting decreased sales, a business that has suffered a data breach opens itself up to class action lawsuits and regulatory scrutiny from state, federal, and possibly international authorities. The Federal Trade Commission (FTC) has positioned itself as a strong enforcer of data security laws. It possesses the authority to impose costly punishments that include annual audits for 20 years and mandatory adoption of a cybersecurity program that includes a full suite of regularly tested, maintained, and monitored policies, procedures, and security measures.

Data security threats lurk around every corner and a business must prepare for and mitigate these threats. Here are practical steps to better protect yourself and your business from a large-scale breach.

1. Know what data you have and how it flows.

An important first step in securing your data is knowing what you possess and where it resides. Breweries collect and use data in a number of ways—payment card information from buyers, social security numbers and banking information from employees, birthdates from patrons, etc. A business should be able to explain in detail the type of data it collects, creates, uses, and maintains, and what happens with that data during its lifespan at the business. Creating a data map allows a business to identify the types of sensitive information in its possession and track its use.

Once the business locates and identifies its data, it can then fully assess the risks associated with the type and location of the data. It can further work to minimize those risks with appropriate security measures. Additionally, a well-documented data map permits a business to quickly assess whether an exposed server or database contains sensitive information that could require legal notice to individuals and regulators. This could save the business time and money in the event that notification is required.

2. Purge unnecessary data.

According to a 2017 study conducted by the Ponemon Institute[2], data breaches cost a company an average of $225 per record exposed. The cost is even greater for breaches involving the service industry—$274 per record exposed—which includes patron-friendly breweries and brewpubs. The more records maintained by the business and exposed during the breach, the more financially devastating the breach will be to that business. Businesses can minimize their potential for massive exposure by limiting the amount of sensitive information in their possession. A company can achieve this goal by purging or storing offline any sensitive information that is no longer pertinent to the business or in regular, active use.

3. Limit access to employees on a need-to-know basis.

Businesses should minimize access to sensitive information to only those employees with an absolute need specific to their particular job requirements. When a business minimizes access to its data, it minimizes risk. For example, an employee should not receive access to full social security numbers if the last four digits will suffice. A person engaging in payroll activities does not need access to any employee's health information.

If an employee falls victim to a phishing scheme and that employee has full administrative access to all of a business' information, the business could be in danger of the ultimate exposure. The fewer people with full keys to the castle, the safer the business is from cyber threats.

4. Develop a practical incident response plan.

The first 24 hours of an incident are critical. A company can make many missteps during this time period that could set the tone for its ongoing response efforts. An effective, tested incident response plan that outlines precisely how to respond when a breach hits can help minimize subsequent missteps.

In crafting a plan, companies should first identify the key individuals to include on the incident response team. Depending on the size of the business, the team may consist of just two or three people, but ideally would include individuals to handle issues related to legal, IT, finance, human resources, and marketing or public relations. These individuals should be strong leaders who understand the day-to-day operations of the business unit they represent. The incident response plan should clearly identify the names and contact information for the individuals included on the team. It should also outline each individual's responsibilities in responding to the breach—from the moment of discovery through notification and beyond.

The incident response plan should inform the business about initial steps to take from the minute an actual or potential incident is identified. It should provide a road map for the incident response team to follow when handling a live situation, including when and how to engage certain vendors. The incident response plan should be a living, breathing document that is tested at least annually. Lessons learned from annual testing should be considered and used to update the plan.

5. Vet your vendors.

Third-party vendors play a necessary role for any small business that outsources many of its day-to-day activities. Craft brewers typically outsource their payment card processing to a point of sale vendor, or their website operation to a hosting provider. But third-party vendors have been responsible for some of the most high-profile data breaches in recent memory (e.g., Target, Home Depot, Lowe's). Vendor management is one of the most crucial components of a business' cybersecurity plan.

As a start, a business should create a vendor management program that assesses the risks posed to the security of its data by each vendor. This risk assessment should occur before selecting a vendor or signing a contract. A risk assessment program is not one-size-fits-all. A smaller business with limited resources should perform due diligence on its vendors and work to understand how the vendor will access, use, and protect the data. Larger businesses with more resources should perform a deeper evaluation of a vendor's general cybersecurity practices. The business should document the identified risks and its reason for moving forward with the vendor in light of those risks.

Businesses should also create general cybersecurity provisions to incorporate into their contracts with vendors. These provisions should outline who owns the data, what should happen when an incident is discovered, how to protect data, and how to treat data at the end of the relationship. A business should attempt to negotiate strong cybersecurity terms into its contracts with all vendors that will have access to its data.

No company can completely shield itself from every threat. Even the most technologically sophisticated and secure company cannot fully protect itself when it comes to a data breach. However, following these simple steps can put your small business in a stronger position to handle potential threats.

REFERENCES

1. usatoday.com/story/news/crime/2017/01/31/all-scottys-brewhouse-employees-affected-data-breach/97300986/
2. Ponemon Institute. "2017 Cost of Data Breach Study," June 2017. https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN&

Marc E. Sorini is a partner in the law firm of McDermott Will & Emery LLP, based in the firm's Washington, D.C. office. He leads the firm's Alcohol Regulatory & Distribution Group, where he concentrates his practice on regulatory and litigation issues faced by supplier-tier industry members. Lynette Arce is an associate in the law firm of McDermott Will & Emery LLP, based in the firm's Chicago office. She is part of the Global Privacy and Cybersecurity Group.

YOUR BREWERY HERE
The art of brewing meets the
technology of control.
Remote access from your mobile device