BY BRAD KORKOW,
SOCIETY INSURANCE

A Recipe for Disaster

Five mistakes caterers make that put data at risk—and how to avoid them

In today's digital world, it's impossible to avoid handling electronic data while running your catering business. Credit card and mobile payment options are the norm, putting caterers increasingly at risk of a cyberattack. Considering 60 percent of small companies go out of business within six months of a cyberattack (according to the National Cyber Security Alliance), data security should be at the top of any caterer's to-do list.

While data can never be 100 percent protected, you can make it more difficult for cybercriminals to access sensitive information by avoiding these five common mistakes.

MISTAKE #1:

Reusing the same password. It's easy to use the same password across multiple sites, but that creates a major security risk. Once a criminal has the password for one account, it's easy for them to log into others and steal data. Tips to prevent this include:

- Avoiding default or common keyboard patterns for passwords (e.g., 123456, QWERTY).
- Creating strong passwords by using a mix of upper and lowercase letters, as well as numbers and symbols; and avoiding common words.
- Using different passwords for different sites—a password manager can keep track of them.

MISTAKE #2:

Opening "phishy" email attachments. Sifting through your inbox is part of doing business. Before clicking open a message, be sure the email is safe. One of the most common ways criminals breach security is by phishing, i.e., impersonating a trustworthy source to trick the recipient into revealing sensitive info. Tips for preventing phishing attempts include:

- Avoiding opening emails from strange email addresses, with questionable subject lines and with spelling errors in the message.
- Never sending or confirming sensitive information in a reply email.
- Never clicking on any suspicious or unsolicited email attachments.

Even when sending emails containing private data through a secure network, the messages need to be protected. Sensitive information is especially lucrative to cybercriminals, who may try to intercept messages to steal it.

MISTAKE #3:

Sending confidential information electronically. Even when sending emails containing private data through a secure network, the messages need to be protected. Sensitive information is especially lucrative to cybercriminals, who may try to intercept messages to steal it. Tips to protect confidential information include:

- Password-protecting documents, and providing the password to the recipient in a secure way.
- Encrypting emails containing social security numbers, financial data or passwords. Refer to your email provider for instructions.
- Using OTR (off-the-record) messaging to automatically encrypt sensitive info sent via instant messages. Some messaging services have this feature built in, or it can be added as a plug-in.

MISTAKE #4:

Connecting to unsecured Wi-Fi networks. Wireless networks allow multiple users to connect at once, making them a gold mine for criminals looking to access data. Networks that are unsecured, meaning they don't require a password to log on, are especially risky. Tips for avoiding unsecured networks include:

- Investing in a mobile hotspot and carrying your own private wireless network with you when on a catering location.
- Securing the network with a strong password that you only share with your employees.
- Hiding your business's private Wi-Fi network name—it won't show up when guests are looking to connect to a network and tempt them to tap into it.

MISTAKE #5:

Not educating employees on data security. Employees have a hand in the digital security of your business. Without a policy or training on cybersecurity, employees might not know what to do if they notice suspicious activity on company computers or accounts. Tips for educating staff members include:

- Training employees so they know what constitutes a cybersecurity threat.
- Encouraging employees to report any suspicious activity, no matter how small it seems.
- Emphasizing the dangers of weak passwords and the risk of online accounts being compromised.

The takeaway? It's better to be safe than sorry. Data breaches are costly and can be devastating to a caterer's reputation and bottom line. Take the necessary precautions to avoid making your business an easy target.

For an extra layer of protection, consider adding cyber liability coverage to your current insurance plan. A good cyber liability policy will include data security and privacy coverage, plus response services from the moment a breach is suspected until it has been resolved. At Society Insurance, for example, our cyber liability policy provides coverage for a variety of expenses that result from a security breach, including legal, public relations and IT forensic expenses. With some extra caution and a cyber liability policy as an added safeguard, you can feel confident that your business won't be toppled by a cyberattack.

ABOUT THE AUTHOR

Brad Korkow has been in the insurance industry since 1985 and has experience in claims, field underwriting, marketing and sales. He has spent the last 17 years of his career with Society Insurance and is currently a regional sales manager, working with agents in southwest Wisconsin and eastern Iowa. The author has earned his CIC, CPCU, AU and AIC designations. For more information on Society Insurance, visit societyinsurance.com.