MELAND | BUDWICK

10 Steps to Help Protect Customer Data

https://melandbudwick.com/2019/12/03/10-steps-to-help-protect-customer-data/

Julie Bawden-Davis

With cyber fraud events making headlines on a regular basis, you likely have protecting customer data on the top of your to-do list. And there's no better time than the present to check the effectiveness of your company's cybersecurity procedures.

"Protecting customer data is no longer a choice for businesses," says Stephen Hyduchak, CEO of Aver, an identity-verification service. "It's crucial businesses act responsibly and with transparency, or they'll lose customers."

Chris Nicholson, CEO of Skymind, an AI company associated with Pathmind, agrees.

"If you fail to make your customer data secure," Nicholson says, "you will lose the trust of those customers. And once you lose customer trust, your business tends to falter."

In some industries, safeguarding customer data is a mandate. Such is the case with healthcare providers.

"Our industry has HIPAA regulations, which is a U.S. sector of law that provides privacy standards to protect patient medical records," says Nerissa Aquino, a dentist and owner of Palm City Family Dentists. "As anyone in business knows, reputation and achieving good standing in your industry is paramount to your company's longevity and growth."

"Cyberattacks like phishing and ransomware often cause major business interruption, expensive incident response costs and identity theft," says Jason Pufahl, vice president of security services for cybersecurity company Vancord.

"In a world where electronic data is more valuable than tangible items, it's critical to follow protocols for protecting customer data," says Pufahl.

The following steps can help you protect your customer's data—and your company's reputation.

1. Perform routine backups and keep them offline and offsite.

"Data backups are the most important aid for successful recovery from a cyberattack or other unexpected disaster," says Pufahl.

"Create a simple data inventory of your data storage locations," he advises. "A backup strategy can be developed once the data is identified. Backup frequency should correspond to the criticality of the data."

2. Update software regularly and apply security patches.

"Hackers aren't as creative or sophisticated as movies and TV shows would lead you to believe," Pufahl continues. "Most cyberattackers walk through 'open doors' caused by out-of-date software. Routinely applying hardware, operating system and application updates is critical."

3. Practice vulnerability management and remediation.

"To infiltrate a business and steal data, cyberattackers search out and exploit unpatched security weaknesses," says Pufahl. "Stay ahead of them by proactively looking for vulnerabilities and making it a priority to fix them. Software tools are available to help businesses identify vulnerabilities and suggest improvements that will help with protecting customer data."

4. Use dual-factor authentication.

"Dual-factor authentication and similar security measures are useful and necessary to protect access to all content, structured and unstructured," says Vikas Dua, COO of Ocrolus, a fintech infrastructure company that transforms documents into actionable data. "Authentication requires confirmation from a second device, like a cellphone, before logging in, and works well when protecting customer data."

5. Avoid storing and sending unencrypted data.

“One common mistake organizations and individuals make is sending sensitive or confidential data over email, but email is not a secure way to share sensitive data,” says Pufahl. “Always ensure that any sensitive or confidential data is sent using transfer mechanisms such as HTTPS or SFTP that encrypt data while in transit.”

Nicholson of Skymind has this advice: “Store sensitive encrypted data on a separate server, and restrict access to the server.”

6. Install firewalls when protecting customer data.

“Firewalls have been and remain a centerpiece of network security,” says Pufahl. “These devices have evolved in sophistication, often including antivirus, intrusion protection and web filtering capabilities. A properly configured firewall, with a thoughtfully configured ruleset, can provide excellent protection against common threats.”

7. Limit WiFi access to customers.

“Limiting WiFi access to guests is a good way of protecting customer data,” says Aquino. “Change the login credentials for guests on a daily basis. Your clients will become accustomed to the process, and you don’t have to worry about someone nearby your office monitoring the publicly accessible traffic and activity.”

8. Provide security awareness and education.

Reliance on IT solutions when protecting customer data against cyberattacks such as spear phishing only goes so far, says trade secrets and IP attorney Eric Ostroff, a partner at Meland Budwick, P.A.

> “Building a culture of protection, from the C-suite down, can help to address this issue,” Ostroff says.

A security awareness program that discusses the threat of phishing

attacks, ransomware and credential management, at a minimum, is a core component of any successful security program, agrees Pufahl.

“The most effective asset against data loss can be a workforce that understands what data is important, how to handle it, its value to attackers, and common ways attackers will try steal it,” he says.

“The weakest link will always be the people who have authorization to access your data. They can be tricked,” says Nicholson. “Make sure you train your employees to know what suspicious emails and spear phishing look like.”

9. Collect and send only necessary sensitive information.

After use, removing nonessential information from your server is a good way of protecting customer data, suggests Hyduchak.

“Instead of storing customer IDs in your system, for instance,” he says, “look into apps that allow consumers to store their IDs on their phone or computer and make them available when needed.”

10. Consult with a cybersecurity expert.

A trained professional can spot weaknesses in your cybersecurity protocol. Have cybersecurity professionals examine how you store and access sensitive data.