How Vulnerable Is Your Firm?

Complete this quick risk assessment to identify where your cybersecurity measures are leaving you vulnerable.

SmartVault

SmartVault

Protect Your Data: Complete a Risk Assessment

A risk assessment is an appraisal of your practice's ability to keep itself from falling prey to cybercrime.

Risk Assessments Are Step One in Protecting Your Firm

Cybersecurity is about protecting electronic data from criminals or unauthorized use. There are many ways hackers and unauthorized users can access your information, and their technology and techniques are getting stronger every day. In fact, many cybercriminals are focusing on practices just like yours. They know you handle a lot of information and that you're less likely to have sophisticated cybersecurity programs that larger businesses have.

But there is good news is: There are ample ways you can protect your data, including simple measures that are fast to implement. Completing this brief risk assessment will help you identify, evaluate, and prioritize areas where your cybersecurity measures are leaving you vulnerable. That way you can create an action plan to address your weaknesses.

Answer Yes or No to the questions below to see how vulnerable your firm is today.

Policies	YES	NO
Are you operating without a designated employee responsible for your cybersecurity programs?	☐	☐
Are you operating without a mobile device security policy?	☐	☐
Are you operating without a remote working policy?	☐	☐
Are you operating without a plan of action for what to do in the event of a cybersecurity breach?	☐	☐
Are you operating without adequate cybersecurity insurance?	☐	☐

Hardware/Software	YES	NO
Does your office use hardware that's more than 5 years old (computers, routers, modems, firewalls)?	☐	☐
Is there a newer version available of your computer and mobile device operating systems and/or key software that has not yet been updated or is obsolete?	☐	☐

SmartVault

Answer Yes or No to the questions below to see how vulnerable your firm is today.

Password Management	YES	NO
Do staff members store login credentials on spreadsheets, written notes, or other unprotected methods?	☐	☐
Do your staff and/or clients share the same login credentials to access software or shared devices?	☐	☐
Do staff members use the same password for multiple logins?	☐	☐

Email	YES	NO
Does your firm request or share documents with clients and others using unencrypted email?	☐	☐
Do you think your staff would fail to recognize cybersecurity threats, including phishing emails?	☐	☐

File Sharing & Storage	YES	NO
Do staff or management ever use public Wi-Fi to access confidential information without additional security protection?	☐	☐
Does your firm store sensitive/confidential information on local hard drives, servers or removable storage (USB drives) without encryption?	☐	☐

Scoring

Count how many questions you answered 'Yes.'

1-3 Low Vulnerability	4-6 Moderate Vulnerability	7-14 High Vulnerability

Free Guide: How to Create a Robust Cybersecurity Program

Learn how to develop a strong cybersecurity program, meet legal requirements, and stay updated on the cybersecurity threats of tomorrow without having to become an IT expert.

Download the Guide