



SAFEGUARDING YOUR SUCCESS

10 STEPS TO PROTECT YOUR BUSINESS FROM CYBERATTACK



SENTINEL
RISK ADVISORS

Nearly half of U.S. businesses today have fallen victim to a cyberattack, with small and mid-sized firms most often the target. It's hard to know exactly how to protect your business from data breach and cybercrime when tech-savvy cybercriminals seem to stay a step ahead. But in fact, Sentinel's cybersecurity experts agree that the first step to protecting your business is to take a step back.

Look at the big picture. Ask: What is most important to my company? What exactly are we securing? By taking stock of what is at stake, you'll know better how to protect what you value most.

Next, take stock of your cyber inventory—the people, systems and processes that present an opportunity for a breach to occur. Record and document your company's cyber inventory and update it regularly, paying close attention to the people who have access to your company's data, resources and intellectual property, and the various ways in which they are able to access information.

Add depth wherever possible to cybersecurity protocols. Remember that cybercriminals want maximum gain for minimal effort. Often,

an additional layer of defense is enough to thwart a cyberattack in process. Yet, experts caution against being so afraid of a cyberattack that employees are prevented from doing the job they were hired to do. Keep a log of who has accessed certain systems and files, but don't restrict access to the extent that it leads to lost productivity and low morale.

Take care to manage the employee termination process. Change system passwords promptly, cut off access to all company systems and servers, and above all, insist on the return of all company-owned devices—laptops, mobile devices and USB drives.

The expert advice above offers a good place to start in protecting your small to mid-size company from cyber threats. Let's turn now to 10 tried-and-true tactics that will help protect your business from cyberattack.

Keep in mind that, no matter how vigilant your company is, when it comes to cyber threats, for every one thing we can successfully keep from losing, there are at least 10 other ways it can be taken.



10 Steps to Protect Your Business from Cyberattack

1. **Enable two-step authentication.** Wherever possible, turn on two-factor authentication to prevent system hacks. This requires each employee to know something (typically a password) and to show something that is a unique identifier (usually a special code).
2. **Establish strong passwords.** Typically, this means a password that is a minimum of eight characters and numbers (combination), including lower and uppercase, and at least one symbol. Don't use the same password for multiple accounts and do have employees update their passwords every 45 days.
3. **Invest in a password management program.** This will ensure that passwords are being stored safely and are not vulnerable to hacking and theft.
4. **Install anti-virus protection.** Update all anti-virus programs regularly on all company computers, laptops and certain mobile devices.
5. **Secure mobile phone data.** Add the four-to-six digit security code feature to prevent theft.
6. **Backup your data.** Conduct regular system backups to a local drive and to the cloud. This will prevent business interruptions due to encryption viruses.
7. **Educate employees.** Hold regular training sessions with employees to reinforce proper handling of data, systems, procedures, etc.
8. **Encrypt data.** Install encryption software for outbound (in transit) data, and data stored on mobile devices.
9. **Implement call-back procedures to prevent phishing scams.** When transferring funds, require call back procedures be complete before sending large amounts of money.
10. **Have a response plan in place.** In the event of a breach, having a carefully thought out response plan will help mitigate loss and control costs. If your company has a cyber insurance policy, the first call should be to your insurance carrier or risk management agent. If there is no cyber policy in place, your first call can either be to a cybersecurity analyst, legal representative, or law enforcement official.

Sentinel Risk Advisors is a premier insurance brokerage firm with a reputation for exceptional client experience in 36 states. Sentinel offers a broad scope of property, casualty, and risk management services for today's global marketplace. Clients depend on Sentinel Risk Advisors to protect their assets, preserve their wealth, and elevate their personal and professional position.

For more information, visit [sentinelra.com](https://www.sentinelra.com)



SENTINEL
RISK ADVISORS