Investment Planners, Inc.
FINRA/SIPC
IPI Wealth Management, Inc.

Concerned About Cyberattacks? The Threat Is Real

According to a 2024 survey, 60% of small businesses believe that cyberattacks are the biggest threat they currently face, and rightly so.[1]

When a data breach occurs, hackers gain access to the personally identifiable information of customers or other individuals, opening the door for identity theft and other financial crimes. Even small companies can be held legally responsible when their customers' personally identifiable information is disclosed. Moreover, the time and expense involved in recovering from any type of cyberattack could be insurmountable.

Does your company handle potentially sensitive information about customers, employees, or competitors? If so, you may want to be proactive about addressing this risk.

Methods of attack

Phishing often involves emails sent to employees. Clicking on a link provides access to the company's network, allowing the installation of malicious code (malware) designed to steal or hijack critical data.

A **watering hole attack** targets individuals or organizations by infecting websites that they frequently visit with malware.

Ransomware is a menacing virus that locks businesses out of their computer files and demands payment of a ransom in exchange for the return of company systems and data.

Fortify your defenses

The Federal Communications Commission has some cybersecurity tips for small businesses.

- Install and update antivirus software on every computer, and maintain firewalls between the internal network and the Internet. Lock up computers, laptops, and tablets to prevent them from falling into the wrong hands.
- If you have a Wi-Fi network, set it up so the network name is hidden and a secure password is required for access. Require passwords to be changed on a regular basis.
- Train employees in security practices, especially not to open emails from unknown senders. Set up a separate account for each user, and provide access only to the data needed for users to perform their jobs. Backup critical data regularly and delete data when it's no longer needed.
- Consider purchasing cyber insurance, which may offer some protection (up to policy limits) from the financial repercussions of a cyberattack, such as the cost of restoring lost or stolen data; liability stemming from a security failure; and in some cases, lost income due to business interruption.

The cost of cyber insurance depends on the types of coverage selected, and policies have exclusions, terms, and conditions for keeping them in force.

1) U.S. Chamber of Commerce, 2024

IMPORTANT DISCLOSURES

The information presented here is not specific to any individual's personal circumstances. To the extent that this material concerns tax matters, it is not intended or written to be used, and cannot be used, by a taxpayer for the purpose of avoiding penalties that may be imposed by law. Each taxpayer should seek independent advice from a tax professional based on his or her individual circumstances. These materials are provided for general information and educational purposes based upon publicly available information from sources believed to be reliable—we cannot assure the accuracy or completeness of these materials. The information in these materials may change at any time and without notice.

Securities and investment advice offered through Investment Planners, Inc. (Member FINRA/SIPC) and IPI Wealth Management, Inc., 226 W. Eldorado Street, Decatur, IL 62522. 217-425-6340.

.