

NEWS FROM QUALITY INSURANCE SERVICE

QUALITYINSURANCESERVICE.COM

PRODUCTS WE OFFER

- Homeowners Insurance
- Auto/Car Insurance
- Umbrella & Liability Insurance
- Business Insurance
- Life Insurance
- Flood Insurance

Cyber-attacks on Small Business: The Risk is Real

Cyber-attacks are on the rise and we're shedding a light on an important matter many small business owners may not be aware of. Cybercriminals are targeting smaller businesses with 250 or less employees because many do not have the appropriate security measures in place to protect themselves against fraudulent activity.

A security breach can be detrimental to a small business; the average loss is \$38,000.¹ Because this loss is so significant, 60 percent of all small businesses will close within six months of a data breach.²

With these cyber-attacks happening at random and within minutes, can your business afford not to be prepared?

How are cyber-attacks happening?

Cybercriminals are sophisticated in their approach to steal a company's information, identity or customer data. Their tactics span from filing a fraudulent business registration to deploying phishing and malware schemes to gain access to confidential information.

What can I do to help minimize my risk for an attack?

Here are some actions small business owners can take to help minimize their risk for an attack.

- **Install firewalls, anti-virus, anti-malware/spyware on all computers** – refrain from using mobile devices when not connected to a secure network
- **Monitor financial accounts daily** – all banks have online account access with the option to receive call/text alerts on account activity. If possible, go paperless with statements
- **Use strong/unique passwords** – passwords should be at least

eight characters long, include capital letters, numbers and special characters. Don't repeat passwords or reuse them for personal accounts

Visit us at QualityInsuranceService.com

- **Review banking agreements** – understand how much time your bank allows you to report fraudulent activity
- **Watch for phishing schemes** – the IRS, government agencies, credit card companies and financial institutions will never ask you to verify information through an email. If you receive an email asking for this information, do not respond, click on any links or open any attachments

Importance of cyber coverage

No matter the size of a cyber-attack, consequences can be expensive. Plus, a business must respond quickly to help protect impacted individuals and the business's reputation. This is where the importance of having Cyber Liability coverage comes into play. Cyber insurance is not spyware — it does, however, help clean up the large mess after a data breach. If attacked without the proper insurance coverage, business owners are responsible for loss of income, restoration of computer hardware and data, computer and funds transfer fraud, notification expenses, credit monitoring services, damages to individual persons or companies, PR consultation and regulatory fines, penalties and expenses, etc.

Would your business survive if you had to cover these expenses? Costs for coverage can be less than you think and customized to fit your needs.

Start by implementing these safety precautions today and contact Quality Insurance Service to review your cyber liability coverage options.

Courtesy of [Integrity Insurance](#).