Help protect your business against cyber attacks and data breaches.

Whether your business is a large corporation or a small operation with only a few employees, you could become the target of a cyber attack and the subsequent breach of your data. Cyber attacks can range from a stolen laptop to a hacked network, and the result can be anything from exposed personal data to viruses infecting your clients' systems. As the damages increase, so do your costs to recover.

In the wake of a data breach, the expense you incur for complying with state laws, notifying your customers and recovering lost data can significantly impact your bottom line. There's also the chance that lawsuits from your affected vendors and clients might arise, along with damage to your company's reputation.

The costs of recovering from a data breach can significantly impact your bottom line.

Types of breaches that can jeopardize your business.

- **Website tampering** — This can include defacing your website, hacking into your system, and compromising web pages to allow invisible code that tries to download spyware onto your devices.
- **Data theft** — This can occur when an offender gains access to files with sensitive information such as credit card numbers, bank account information, health records and social security numbers.
- **Denial of service attack** — By placing a lock on your devices and/or crashing your operational systems, this can prevent sales and communications, and impede your ability to conduct business.
- **Malicious code and viruses** — These can be sent over the Internet with the goal of: finding and sending your files, finding and deleting critical data, or locking your computer or system. They can hide in programs or documents and make copies of themselves without your knowledge.

Reducing your files can reduce your risk.

Minimizing data is a powerful way to guard against cyber attack. The less data you have available, the less damaging a compromise to your system can be. Here are some best practices for reducing your risk:

- Don't collect information you don't need
- Reduce the number of places where you retain data
- Grant employees access to sensitive data on an as needed basis, and keep current records of who has access to the data while it is in your company's possession
- Purge data responsibly once the need for it has expired

Nationwide® is on your side

Continued >>

Practical steps to help protect your business from attacks.

- **Don't rely on encryption as your only method of defense.** Encryption is a security best practice, but can give businesses a false sense of security. Use encryption as the first step to protecting your network.
- **Look beyond IT security when assessing your company's data breach risks.** Your company should evaluate employee exit strategies (HR), remote project protocol, on- and offsite data storage practices and more — then establish and enforce new policies, procedures and physical safeguards appropriate to the findings.
- **Retain a third-party breach and data security expert to analyze your level of risk and exposure.** An evaluation performed by an objective, neutral party leads to a clear and credible picture of what's at stake.
- **Establish a comprehensive breach preparedness plan** that will enable decisive action and prevent operational paralysis when a breach occurs. Disseminate this plan throughout the management structure to ensure everyone knows what to do in the event of a breach.
- **Educate employees on how to handle and protect sensitive data.** Your company can take extensive measures to prevent breaches, but your vulnerability increases when employees aren't properly trained.
- **Provide training and technical support to mobile workers.** Ensure that the same standards for data security are applied regardless of location, by providing mobile workers with straightforward policies and procedures, adequate training and technical support, and security and authentication software installed and updated on mobile devices.
- **Conduct a periodic risk assessment.** Business models and operations change and might alter risk levels and liabilities. Determining if you've acquired new areas or levels of risk can be accomplished through both internal audit and specialized external resources.
- **Keep current with security software updates/patches.** An unpatched system is, by definition, operating with a weak spot that hackers can exploit. However, applying patches takes time and resources, so senior management must agree on allocations and expectations.
- **Hold vendors and partners to the same standards.** It's important to define your security requirements upfront with vendors. Ensure that your organization maintains control of data at all times, especially with offshore data storage or services.

Another line of defense against cyber attacks.

Nationwide® provides CyberOne liability coverage through Hartford Steam Boiler Inspection and Insurance Company. Call your agent today to obtain a quote for this additional way to safeguard your business.

Providing solutions to help our members manage risk.℠

For your risk management and safety needs, contact Nationwide Loss Control Services: 1-866-808-2101 or LCS@nationwide.com.

Nationwide®