Seven Steps to Improve Cybersecurity

Most businesses have a risk management plan in place to cover general physical risks. But what about electronic ones? No business is immune to cybercrime — do you have the necessary precautions in place to help prevent one wrong click from hurting your business?

The depth and breadth of cybercrime means that any business that is connected to the internet or stores information digitally is at risk. Understanding common types of cybercrime is the first step in protecting your business. Some of these include: card skimming, ransomware, wire fraud, false pretense and conversion, phishing/spoofing, and denial of service.

With so many ways criminals can attack your business, it makes sense to create and implement a cybersecurity risk management plan. Ask yourself: what is in the best interest of the overall well-being and safety of your company's electronic information? Here are seven potential action items to help bring your cybersecurity risk management plan to life.

1. **Conduct a risk assessment.** What are you trying to protect in terms of products, services, customers, vendors, communication, and information networks?

2. **Determine at least one way to mitigate the risk** of cybercriminals accessing the items identified above.

3. **Develop and include your company policies and procedures in your risk management plan**. These documents outline expected rules of conduct and everyone's responsibility to practice safe and savvy internet use.

4. **Communicate your plan and provide cyber security training** to employees. Explain how employees can help deter potential theft to help reduce vulnerability to these schemes.

5. **Monitor the effectiveness of your plan** and take any necessary action sooner rather than later.

6. **Revisit your risk assessment regularly** to be sure it is current, accurate, and complies with any new regulations. Consider re-ranking your risks as your company's organizational controls and systems evolve.

7. **Conduct regular audits** on your information security practices, including employee email phishing tests.

No single coverage protects from all types of theft, so review your cybersecurity policy with an insurance professional to make sure your policy accounts for your unique risks. Even if you have adequate insurance, the best way to protect your business is to stop cybercrime before it happens. Reach out to your local marketing representative to discuss Federated Insurance's risk management resources to help you prevent potential cybersecurity losses.