Utica National
Insurance Group®

GENERAL BUSINESS

RISK MANAGEMENT ALERT

Five Steps for Securing Your Business's Information Systems and Networks

Protecting the employee, customer, proprietary, and tax information your business receives, creates, uses, or stores is called information security. Various threats could jeopardize that information. These threats can be accidental or intentional and include:

- **Environmental factors – fire, water, tornado, earthquake, etc.**
- **Business resources – equipment failure, supply chain disruption, employees, etc.**
- **Hostile actors – hackers, hacktivists, criminals, nation-state actors, etc.**

"Cyber risk framework" lays out a five-step process to managing cyber security risks.

1. IDENTIFY and control who has access to your business information.

- **List all of the information your business stores or uses.** Have employees list the information they use in their regular activities. Determine its value and what would happen to your business if you or your customers couldn't access it.
- **Be aware of who can access your business.** Unauthorized persons who have physical access to your computers can steal private or sensitive information. This includes computer or network repair personnel, cleaning crews, and maintenance personnel. No unrecognized person should be able to enter your office space without being questioned by an employee.
- **Physically lock up laptops and other mobile devices when not in use.** Use the session lock feature included with many operating systems, which locks the screen if the computer is not used for a specified time period. Use a privacy screen or position each computer's display so people walking by cannot see what's on the screen.
- **Conduct background checks on prospective employees.** Do a full, nationwide criminal background check, sexual offender check, and, if possible, a credit check, especially if the person will be handing your business funds. Request one directly from the FBI or an FBI-approved agency.
- **Require individual user accounts for each employee.** Set up a separate account for each user, including contractors needing network access, and require that strong, unique passwords be used. Ensure that all employees use computer accounts without administrative privileges to perform typical work functions.
- **Create information security policies and procedures.**
  - Policies should clearly describe your expectations for protecting your information and systems.
  - Employees should sign a statement noting that they have read the policies and relevant procedures and will follow them.
  - Policies and procedures should be reviewed and updated at least annually and whenever there are changes in the organization or technology.

The information provided in this article is intended for general informational purposes and should not be considered as all encompassing, suitable for all situations, in compliance with all laws and regulations or legal advice. Consult an attorney or other specialist to obtain advice with respect to any particular issue or problem.

2 PROTECT information to limit or contain the impact of a potential or actual cybersecurity event.

- Limit employee access to data and information.
- Install surge protectors and uninterruptible power supplies (UPS).
- Patch your operating systems and applications.
- Install and activate software and hardware firewalls on all of your business networks.
- Secure your wireless access point and networks.
- Set up web and email filters.
- Use encryption for sensitive business information.
- Dispose of old computers and other equipment containing important information properly.
- Train employees on:- what they are and are not allowed to use business computers and mobile devices for;
- how they are expected to treat customer or business information, such as whether they can take that information home with them;- what to do in case of an emergency or security incident; and
- basic practices as contained in the RESPOND section below.

3. DETECT

- Install and update anti-virus, spyware, and other malware programs.
- Maintain and monitor logs. Protection/detection hardware or software (e.g., firewalls, anti-virus) often has the capability of logging activity. Check the operating manual for instructions on enabling this functionality. Logs can be used to identify suspicious activity and will be valuable during investigations.
- Back up logs for at least one year. Some information will require longer backup.

4. RESPOND

- Develop a plan for disasters and information security incidents. These are actions you will take in case of a fire, medical emergency, burglary, or natural disaster.
- The plan should include the types of activities that constitute an information security incident, roles and responsibilities, what to do with your information and information systems in case of an incident, and who to call in case of an incident..

5. RECOVER

- Make full backups of important business data.
- Make incremental backups of important business data.
- Consider cyber insurance.
- Make improvements to processes, procedures, and technologies.

More information Many incidents can be prevented by practicing safe and secure business habits such as paying attention to the people you work with and around, being careful of email attachments and web links, and not clicking a link or opening an attachment that you were not expecting. In addition, use separate personal and business computers, mobile devices, nd accounts, and do not connect personal or untrusted storage devices or hardware to your computer, mobile device, or network. Finally, do not give out personal or business information, and use caution and follow company rules about downloading software.

- Information in this document is an adaptation of a U.S. Department of Commerce publication, Small Business Information Security: The Fundamentals, accessible at https://doi.org/10.6028/NIST.IR.7621r1.

The information provided in this article is intended for general informational purposes and should not be considered as all encompassing,
suitable for all situations, in compliance with all laws and regulations or legal advice.
Consult an attorney or other specialist to obtain advice with respect to any particular issue or problem.