As a small business, you may be more exposed to cyber risk than you think. That's why you need cyber insurance to protect your business.

**Common small business cyber vulnerabilities**

- **POS system**
  - Cash register, tablet, smart phone
  - If you’re taking payment from customers, you have access to their credit card numbers and other personal information – and so does a cybercriminal, if your system is hacked.

- **Landline phone**
  - Cybercriminals can tie up your business line by making numerous robo calls to your number. Or they can call and ask for personal information, posing as someone you know.

- **IoT items**
  - Thermostat, networked copy machine, security systems
  - When you connect devices to your network, you can introduce new vulnerabilities if they are not properly secured.

- **Employee cell phone**
  - If your employees use their smart phones to conduct business in any way, those devices are risks too. If their phone is hacked, it can be an entry point for a cybercriminal.

- **Files/papers**
  - Data breaches are not limited to electronic data. Physical papers and files that are stolen may contain confidential or personal information that may trigger data breach reporting requirements and leave affected individuals vulnerable to identity theft.

- **Computer**
  - Cyber criminals often try to get into your computer system by way of an employee, by emailing a malicious link or posing as an executive and asking them to transfer funds or goods.

- **Server**
  - If your server is hacked, cyber criminals may gain access to confidential business information, personal and health information of employees or clients.

- **Company vehicles**
  - Today's company vehicles are often outfitted with logistics software and GPS tracking systems. Both can be affected if your business suffers a cyber attack.

© 2020 The HSB Inspection and Insurance Company. All rights reserved. 2020-025 (New 10/2020)