bearing insurance®

Cyber Hygiene Best Practices

As cyberattacks become more frequent and severe it is increasingly important for organizations to practice good cyber hygiene to minimize their exposure to risk.

Importance of Cyber Hygiene

Cyber hygiene helps protect computers, networks, and data from threats such as malware, ransomware, and other cyberattacks. Maintaining strong cybersecurity practices reduces security gaps and helps prevent disruptions. Some consequences of poor cyber hygiene include:

- **Security breaches:** Cybercriminals take advantage of human error and poor security networks to access personal and business data.
- **Data loss:** Organizations can lose data when hard drives, online cloud storage and software-as-a-service apps aren't backed up or maintained.
- **Software vulnerabilities:** Software developers constantly update their programs with security patches to prevent known vulnerabilities. If software is out-of-date it is susceptible to cyberattacks.
- **Antivirus weaknesses:** Outdated security software will be less effective at protecting organizations against the latest cybersecurity threats.

Cyber Hygiene Best Practices

Daily routines, good behaviors and occasional checkups can make all the difference in ensuring an organization's cyber health is in optimal condition. The following are essential parts of cyber hygiene:

- **Passwords:** Strong, unique passwords with at least 12 characters, including upper and lowercase letters, numbers, and symbols, are essential for cyber security. Avoid sharing passwords or reusing them across accounts.
- **Multi-factor authentication:** Important accounts, including email, social media and banking apps, should require multi factor authentication to limit the opportunity for cybercriminals to steal data.
- **Data backups**: Essential files should be backed up in a separate location, such as on an external hard drive or in the cloud.
- **Firewalls**: A network firewall prevents unauthorized users from accessing company websites, email servers and other sources of information accessed through the internet.
- **Security software**: High-quality antivirus software helps detect and remove malware while protecting devices from online threats.
- **Employee education**: Employees are often the weakest link in cybersecurity. Regular training helps them recognize phishing, social engineering, and other cyber threats.

Organizations should develop a protective routine to secure all company, personal and financial information.