CYBER HYGIENE
BEST PRACTICES

INSURANCE BOARD
Partners in Protection

THE CINCINNATI
INSURANCE COMPANIES

As cyberattacks become more frequent and severe, it's increasingly important for organizations to practice good cyber hygiene — habitual practices ensuring critical data and connected devices are handled safely — to minimize their exposure to risk. Some consequences of poor cyber hygiene include:

Security breaches

Data loss

Software vulnerabilities

Antivirus weaknesses

The following are essential parts of cyber hygiene:

Passwords—Users should create strong and complex passwords, and avoid sharing passwords or using the same password across different accounts (change passwords routinely).

Security software—A high-quality antivirus software can perform automatic device scans to detect and remove malicious software and provide protection from various online threats and security breaches.

Data backups—Essential files should be backed up in a separate location, such as an external hard drive or in the cloud or at a secured off-site location.

Firewalls—Organizations should have a network firewall to prevent unauthorized users from accessing company websites, email servers and other sources of information.

Multi-factor authentication—Important accounts should require multi-factor authentication/user verification to limit the opportunity for criminals to steal data.

Employee education—Workforce cyber security education is essential to teach employees to identify phishing attacks, social engineering and other cyberthreats.

Daily routines, good behaviors and occasional checkups can make all the difference in ensuring that an organization's cyber health is in optimal condition. If additional risk management guidance is needed, contact us today. www.InsuranceBoard.org