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. Cyber hygiene refers to habitual practices ensuring critical data and connected devices are handled safely.

This article discusses the importance of cyber hygiene for organizations and best practices.

Importance of Cyber Hygiene

Cyber hygiene helps keep computers, networks and data safe from threats, including malware, ransomware and other cyberattacks. Consistent cybersecurity practices keep systems running efficiently and reduce risks related to fragmentation, outdated programs and other security gaps. 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 If software is out-of-date it is susceptible to cyberattacks.
- **Antivirus weaknesses**—Outdated security software will be less effective at protecting organizations against the latest cybersecurity threats.

In addition to keeping machines and infrastructure protected, system users and clients also rely on organizations to keep their data safe.

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**—The use of strong and complex passwords—containing at least 12 characters and a mix of upper- and lower-case letters plus symbols and numbers—that are changed regularly is an essential cyber hygiene practice. Users should avoid sharing passwords or repeatedly using them across different 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**—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.
- **Employee education**—Employees are one of an organization's most significant cybersecurity vulnerabilities. Workforce cybersecurity education is essential to teach employees to identify phishing attacks, social engineering and other cyberthreats.

Conclusion

Organizations should develop a protective routine to secure all company, personal and financial information. For additional risk management guidance, contact us today.

This Cyber Risks & Liabilities document is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice. Readers should contact legal counsel or an insurance professional for appropriate advice.