Cyber Risks & Liabilities

10 Cybersecurity Resolutions

Cybersecurity risks and trends can change year over year as technology continues to advance at alarming speeds. As such, it's critical for organizations to reassess their data protection practices at the start of each new year and make achievable cybersecurity resolutions to help protect themselves from costly breaches. Here are 10 resolutions your company can implement to ensure you don't become the victim of a cybercrime:

1. **Provide security training.** Employees are your first line of defense when it comes to cyberthreats. Even the most robust and expensive data protection solutions can be compromised should an employee click a malicious link or download fraudulent software. That's why it's critical to thoroughly train personnel on common cyberthreats and proper response methods. Employees should be aware of the dangers of visiting harmful websites, leaving their devices unattended and oversharing personal information on social media. Your staff should also understand your company's cybersecurity policies and know how to report suspicious activities.
2. **Install strong antivirus software and keep it updated.** Outside of training employees on the dangers of poor cybersecurity practices, strong antivirus software is one of the best ways to protect your company's data. Be sure to conduct thorough research to choose software that's best for your company's needs. Once installed, antivirus programs should also be kept up to date.
3. **Instill safe web browsing practices.** Deceptive and malicious websites can easily infect your company's network, often leading to more serious cyberattacks. To protect your organization, employees should be trained on proper web usage and instructed to only interact with secure websites. For further protection, consider blocking known threats and potentially malicious web pages outright.
4. **Create strong password policies.** Ongoing password management can help prevent unauthorized attackers from compromising your organization's password-protected information. Effective password management protects the integrity, availability and confidentiality of your organization's passwords. Above all, you'll want to create a password policy that specifies all of your organization's requirements related to password management. This policy should require employees to change their passwords on a regular basis, avoid leveraging the same password for multiple accounts and use a variety of special characters in their passwords.
5. **Use multifactor authentication (MFA).** While complex passwords can help deter cybercriminals, they can still be cracked. To further prevent cybercriminals from gaining access to employee accounts, MFA is key. MFA adds a layer of security that can allow your company to protect against compromised credentials. Through this method, users must confirm their identities by providing extra information (e.g., a phone number or unique security code) when attempting to access corporate applications, networks and servers.
6. **Conduct vulnerability assessments.** The best way to evaluate your company's data exposures is through vulnerability assessments. Using simulated attacks and stress tests, vulnerability assessments can help you uncover entry points into your IT infrastructure. Following these assessments, cybersecurity experts will compile their findings and provide your company with recommendations for improving network and data safeguards.
7. **Patch systems regularly and keep them updated.** A common way cybercriminals can gain entry into your company's systems is by exploiting software vulnerabilities. To prevent this, it's critical that you update applications, operating systems, security software and firmware on a regular basis.
8. **Back up your data.** In the event that your company's systems are compromised, it's important to keep backup files. Failing to do so can result in the loss of critical business or proprietary data.
9. **Understand phishing threats and how to respond.** In broad terms, phishing is a method cybercriminals use to gather personal information. In these scams, phishers send emails or direct users to fraudulent websites and ask victims to provide sensitive information. These emails and websites are designed to look legitimate and trick individuals into sharing credit card numbers, account numbers, passwords, usernames or other confidential details. Phishing is becoming more sophisticated by the day, and it's more important than ever to understand the different types of attacks, how to identify them and preventive measures you can implement to keep your organization safe. As a result, it's best to train employees on common phishing scams and provide real-world examples to help them better understand what to look for.

10. **Create an incident response plan.** Most organizations have some form of data protection in place. While these protections are critical for minimizing the damages caused by a breach, they don't provide clear action steps following an attack. That's where cyber incident response plans can help. While cybersecurity programs can help secure digital assets, cyber incident response plans provide clear steps for companies to follow when a cyber event occurs. An effective response plan can help your company notify impacted customers and partners quickly and efficiently, limiting financial and reputational damages.

For additional cyber risk management guidance and insurance solutions, contact us today.