10 Cyber-security Resolutions to Reduce Your Data Exposures

Cyber-security threats and trends can change year over year as technology continues to advance at alarming speeds. As such, it's critical for organisations to reassess their data protection practices at the start of each new year and make achievable cyber-security resolutions to help protect themselves from experiencing data breaches and paying costly fines under the GDPR.

Implement the following are resolutions to ensure you don't become the victim of a cyber-crime:

1. Provide security training—Employees are your first line of defence when it comes to cyber-threats. Even the most robust and expensive data protection solutions can be compromised should an employee click a malicious link or download fraudulent software. As such, it's critical for organisations to thoroughly train personnel on common cyber-threats and how to respond. Employees should understand the dangers of visiting harmful websites, leaving their devices unattended and oversharing personal information on social media. Your employees should also know your cyber-security policies and know how to report suspicious activity.
2. Install strong antivirus software and keep it updated—Outside of training your employees on the dangers of poor cyber-security practices, strong antivirus software is one of the best ways to protect your data. Organisations should conduct thorough research to choose software that's best for their needs. Once installed, antivirus programs should be kept up to date.
3. Instil safe web browsing practices—Deceptive and malicious websites can easily infect your network, often leading to more serious cyber-attacks. To protect your organisation, employees should be trained on proper web usage and instructed to only interact with secured websites. For further protection, companies should consider blocking known threats and potentially malicious webpages outright.
4. Create strong password policies—Ongoing password management can help prevent unauthorised attackers from compromising your organisation's password-protected information. Effective password management protects the integrity, availability and confidentiality of an organisation's passwords. Above all, you'll want to create a password policy that specifies all of the organisation's requirements related to password management. This policy should require employees to change their password on a regular basis, avoid using the same password for multiple accounts and use special characters in their password.
5. Use multi-factor authentication—While complex passwords can help deter cyber-criminals, they can still be cracked. To further prevent cyber-criminals from gaining access to employee accounts, multi-factor authentication is key. Multi-factor authentication adds a layer of security that allows companies to protect against compromised credentials. Through this method, users must confirm their identity by providing extra information (eg a phone number, unique security code) when attempting to access corporate applications, networks and servers.
6. Get vulnerability assessments—The best way to evaluate your company's data exposures is through a vulnerability assessment. Using a system of simulated attacks and stress tests, vulnerability assessments can help you uncover entry points into your system. Following these tests, security experts compile their findings and provide recommendations for improving network and data safety.
7. Patch systems regularly and keep them updated—A common way cyber-criminals gain entry into your system 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 system is 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 cyber-criminals use to gather personal information. In these scams, phishers send an email or direct users to fraudulent websites, asking victims to provide sensitive information. These emails and websites are designed to look legitimate and trick individuals into providing credit card numbers, account numbers, passwords, usernames or other sensitive information. 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 organisation safe. As such, it's critical to train employees on common phishing scams and other cyber-security concerns. Provide real-world examples during training to help them better understand what to look for.

10. **Create an incident response plan**—Most organisations have some form of data protection in place. While these protections are critical for minimising 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 cyber-security programmes help secure an organisation's digital assets, cyber-incident response plans provide clear steps for companies to follow when a cyber-event occurs. Response plans allow organisations to notify impacted customers and partners quickly and efficiently, limiting financial and reputational damages.