Risk Management tips for Cyber Crime Prevention

INSURANCE ADVISERNET
Advice you can trust

Encourage employees to use strong, unique passwords and regularly change them. Consider using a password manager to help employees keep track of passwords.

Enable two-factor authentication for all critical accounts, such as email and financial systems, to provide an extra layer of security.

Ensure that your business software, including operating systems, anti-virus software, and other applications are updated regularly with the latest security patches.

Implement firewalls to protect against unauthoriaed access to your network and to prevent the spread of malware and Use encryption technology to secure sensitive data and communications.

Educate employees on cyber security best practices, such as avoiding suspicious emails and links, and the importance of keeping software and security systems up-to-date.

Regularly backup important data to a secure location, such as an off-site cloud-based storage solution, to ensure that it can be recovered in the event of a cyber attack or data loss.

Regularly monitor network activity to detect any suspicious activity, such as unauthorised access attempts, and to identify potential security vulnerabilities.

Develop an incident response plan to be used in the event of a cyber attack, including procedures for reporting the incident, containing the attack, and restoring systems and data. Regularly review and update the plan to ensure it remains effective.

Limit access to sensitive data, such as financial information, to only those employees who need it to perform their job duties.

Important Information – These risk management tips are for information only and your personal circumstances have not been taken into account. This communication is not intended to constitute personal advice. If you are interested in discussing this information or acquiring an insurance product, you should contact your insurance adviser.