CYBERSECURITY
TOP 10 BEST PRACTICES

Ensuring cybersecurity is crucial for any organisation to protect its sensitive data, intellectual property, and maintain the trust of its customers. Here are the top ten things a company can do to enhance its cybersecurity:

		Effort to Implement	Cost to implement
1	**Develop a comprehensive cybersecurity strategy:** Establish a clear plan that outlines the company's approach to cybersecurity, including risk assessment, incident response, employee training, and ongoing monitoring.	★★★★	★☆☆☆
2	**Regularly update software and systems:** Apply security patches, updates, and fixes to operating systems, applications, and firmware promptly. Outdated software can be vulnerable to known security flaws.	★★★☆	★★★☆
3	**Implement strong access controls:** Enforce strict user access controls, employing the principle of least privilege. Ensure that employees only have access to the systems and data necessary for their roles.	★★★☆	★★☆☆
4	**Conduct employee training and awareness programs:** Educate employees about common cyber threats, social engineering techniques, safe browsing habits, and the importance of strong passwords. Foster a cybersecurity-conscious culture.	★★☆☆	★☆☆☆
5	**Use multi-factor authentication (MFA):** Implement MFA wherever possible to add an extra layer of security. This requires users to provide additional verification, such as a unique code sent to their mobile device, in addition to their password.	★★☆☆	★★☆☆
6	**Regularly backup data:** Maintain regular backups of critical data and test the restoration process periodically. This helps mitigate the impact of data loss due to cyberattacks, hardware failures, or natural disasters.	★★☆☆	★★☆☆
7	**Employ strong and unique passwords:** Encourage employees to use complex passwords that are unique to each account or system. Consider using a password manager to generate and store passwords securely.	★☆☆☆	★☆☆☆
8	**Use encryption:** Encrypt sensitive data, both at rest and in transit. This ensures that even if the data is compromised, it remains unreadable and unusable without the encryption keys.	★★☆☆	★★☆☆
9	**Implement network segmentation:** Divide the company's network into separate segments to limit the potential impact of a security breach. This practice restricts lateral movement by attackers and helps contain any compromised systems.	★★★☆	★★☆☆
10	**Conduct regular security assessments and audits:** Perform internal and external security assessments, penetration testing, and vulnerability scanning. Regular audits help identify potential weaknesses and areas for improvement.	★★☆☆	★★☆☆

Remember: cybersecurity is an ongoing process that requires continuous monitoring, adaptation to evolving threats, and a proactive approach to protecting company assets.

Classification: Public

Disclaimer