MEET YOUR CYBER SECURITY INSURANCE REQUIREMENTS

SwiftTech SOLUTIONS
INFORMATION TECHNOLOGY GROUP

#	MEASURES TO TAKE	✓
1	**Multi-Factor Authentication on Critical Systems** Implementing MFA on critical systems can ensure that only authorized users can access valuable data.	
2	**Advanced Endpoint Security** This involves the installation of endpoint protection software on all devices connected to your network	
3	**Secure Data Backups** Data backups are essential for restoring and recovering data in the event of a cyber-attack.	
4	**Keep Your Computers, Software, and Firmware Updated** Make sure you have the latest security patches installed on your systems and check for any new updates regularly.	
5	**Raise Cybersecurity Awareness Through Regular Employee Training** Organize regular training sessions and workshops to educate staff on cyber threats, ways to identify suspicious activity, and best practices for staying secure online.	
6	**Regular Security Audits** Cyber insurance providers may require organizations to have their systems audited by a third party on an annual basis or after any major changes to the system.	
7	**Develop and Test Your Incident Response Plan** Test your plan regularly to ensure it is up to date and that all team members are aware of their roles in the event of an attack.	
8	**Undergo Regular Penetration Testing** It involves simulating cyber-attacks on your environment to identify vulnerabilities that can be exploited in a real attack.	
9	**Monitor for Suspicious Activity** An intrusion detection system (IDS) or security information and event management (SIEM) solution can help detect unusual behavior on your network quickly.	
10	**Privileged Access Management (PAM)** PAM solutions help you control, monitor, and manage access to privileged accounts to reduce the risk of unauthorized access.	