Do You CYBERSECURE?

	Yes	NO
Do you have multi-factors authentication (MFA) enabled and enforced across all your systems including email accounts?		
Do you use encrypted VPNs for all remote access to your business?		
Do you have Managed Detection and Response (MDR) or Endpoint Detection and Response (EDR) with a 24/7 Security Operations Center for all your assets?		
Do you follow the 3-2-1 backup rule, (3 copies of your data, 2 different storage types, with 1 stored offsite) and are backups tested monthly for restoration?		
Do you apply the principle of least privilege ensuring that users have access only to the resources necessary for their role?		
Do you have a data retention policy?		
Do you foster a cybersecurity inclined work environment that includes regular training and phishing simulations?		
Do you scan all emails exchanged within your business for known threats and suspicious email?		
Are all the patches for your environment deployed within one week (and faster if needed)?		
Do you have a documented incident response plan (should a cyber-incident occurred) that is regularly updated and practiced?		
Are all cybersecurity events from all devices reviewed and actioned 24/7?		
Are all identified critical and high vulnerabilities remediated within 30 days?		

Want to talk to one of our experts about your cybersecurity journey?
We offer 20 minutes meeting with an expert to talk about your needs. (no fees, no obligation). You can book at your convenience by visiting ALCiT.com/expert