Cybersecurity Checklist

1. Do you require multi-factor authentication (MFA) for privileged accounts?	
2. Do you require MFA for remote access?	
3. Do you have a cybersecurity policy?	
4. Do you have minimum password length and maximum failed attempt limits?	
5. In what intervals, or under what conditions, are people required to change their password?	
6. Do you have a cybersecurity incident response plan?	
7. Do you have a standard that defines when to report cybersecurity incidents to customers, vendors and/or partners, and in what timeline? If yes, please define.	
8. Have you had a data breach, which required reporting outside your organization, within the past five years?	
9. Have you had any security incident which impacted the business in any way within the past five years? If yes, please describe.	
10. Do you adhere to widely adopted security standards (e.g., NIST 800-171, IS27001, etc.)?	
11. Do you formally audit and certify to said standard?	
12. Do you encrypt data in transit?	
13. Do you encrypt data at rest?	
14. Do you have endpoint protection software?	
15. Do you perform regularly planned security patching on all desktops and servers?	
16. Do you perform regularly planned security patching on non-user devices (firewalls, switches, WAPs, etc.)?	
17. How often do you conduct penetration tests?	
18. Do you have an intrusion prevention system?	
19. Do you have an intrusion detection system?	
20. Are your backup systems separate from your network, and managed with separate administration accounts?	
21. Is cybersecurity awareness training mandatory and part of the onboarding process?	
22. Do you conduct phishing simulations and/or other regular cybersecurity training exercises and assessments?	