Liste de contrôle pour la cybersécurité

1. Exigez-vous une authentification multifacteur pour les comptes assortis à des privilèges d'administration?	
2. Exigez-vous une authentification multifacteur pour l'accès à distance?	
3. Avez-vous en place une politique en matière de cybersécurité?	
4. Avez-vous établi une longueur minimale pour les mots de passe et une limite maximale de tentatives de connexion ou d'accès infructueuses?	
5. À quelle fréquence, ou sous quelles conditions, les personnes sont-elles tenues de modifier leur mot de passe?	
6. Avez-vous en place un plan d'intervention en cas d'incident de cybersécurité?	
7. Avez-vous une norme qui définit le moment où les incidents de cybersécurité doivent être signalés aux clients, aux fournisseurs et/ou aux partenaires, et dans quels délais? Dans l'affirmative, veuillez préciser.	
8. Au cours des cinq dernières années, avez-vous eu une atteinte à la protection des données qui a nécessité une notification à l'extérieur de votre organisation?	
9. Avez-vous eu un incident de sécurité qui a eu un impact sur votre entreprise au cours des cinq dernières années? Dans l'affirmative, veuillez le décrire.	
10. Adhérez-vous à des normes de sécurité largement adoptées (par exemple, NIST 800-171, IS27001, etc.)?	
11. Procédez-vous à un audit formel et à une certification qui sont prévus par ces normes?	
12. Chiffrez-vous les données en transit?	
13. Chiffrez-vous les données inactives?	
14. Disposez-vous d'un logiciel de protection des points terminaux?	
15. Effectuez-vous régulièrement des correctifs de sécurité sur tous les ordinateurs de bureau et les serveurs?	
16. Effectuez-vous régulièrement des correctifs de sécurité sur les dispositifs non-utilisateurs (pare-feu, commutateurs, WAP, etc.)?	
17. À quelle fréquence procédez-vous à des tests d'intrusion?	
18. Disposez-vous d'un système de prévention des intrusions?	
19. Disposez-vous d'un système de détection des intrusions?	
20. Vos systèmes de sauvegarde sont-ils séparés de votre réseau et gérés avec des comptes d'administration distincts?	
21. Une formation de sensibilisation à la cybersécurité est-elle obligatoire et fait-elle partie du processus d'intégration/orientation des nouveaux employés?	
22. Procédez-vous à des simulations d'hameçonnage et/ou à d'autres exercices réguliers de formation et d'évaluation en matière de cybersécurité?	