



cyber
defense

Assessment

General Network Questions (Yes = 2pts / No = 0pts)	Yes	No	Unsure / Notes
1. Does your organization have a wireless network, or do employees or customers access your internal systems from remote locations?	2	0	
2. Does anyone in your organization take company-owned mobile devices (e.g., laptops, smartphones and USB drives) with them, either home or when travelling?	2	0	
3. Does your organization use Cloud-based software or storage?	2	0	
4. Does your organization have a “bring your own device” (BYOD) policy that allows employees to use personal devices for business use or on a company network?	2	0	
5. Are any employees allowed access to administrative privileges on your network or computers?	2	0	
6. Does your organization have critical operational systems connected to a public network?	2	0	
7. Does your organization store sensitive information (e.g., financial reports, trade secrets, intellectual property and product designs) that could potentially compromise your organization if stolen?	2	0	
8. Does your organization digitally store the personally identifiable information (PII) of employees or customers? This can include government-issued ID numbers and financial information.	2	0	
9. Is your organization part of a supply chain, or do you have supply chain partners?	2	0	
10. Does your organization conduct business in foreign countries, either physically or online?	2	0	
11. Has your organization ever failed to enforce policies around the acceptable use of computers, email, the Internet, etc.?	2	0	
12. Can the general public access your organization’s building without the use of an ID card?	2	0	
13. Is network security training for employees optional at your organization?	2	0	
14. Can employees use their computers or company-issued devices indefinitely without updating passwords?	2	0	
Page One Total			

ESCALATED RISK: 96-120

MODERATE RISK: 25-60

HIGH RISK: 61-95

LOW RISK: 10-24





cyber
defense

Assessment

15. Has your IT department ever failed to install antivirus software or perform regular vulnerability checks?	2	0	
16. Can employees dispose of sensitive information in unsecured bins?	2	0	
17. Would your organization lose critical information in the event of a system failure or other network disaster?	2	0	
18. Can employees easily see what co-workers are doing on their computers?	2	0	
19. Has your organization neglected to review its data security or cyber security policies and procedures within the last year?	2	0	

Policies & Procedure Questions (Yes = 0pts / No = 2pts)	Yes	No	Unsure / Notes
20. Do you have a written Privacy Policy?	0	2	
21. Do you have a written Network Security Policy?	0	2	
22. Do you have a written Identity Theft Prevention Program?	0	2	
23. Do you have a written Breach Incident Response Plan?	0	2	
24. Do you have a written Business Continuity/Disaster Recovery Plan?	0	2	
25. Do you have a written Laptop/Computer use Policy?	0	2	
26. Do you have a written Employee Training regarding Confidential Information?	0	2	
27. Does your organization use Firewall Protection?	0	2	
Page Two Total			

ESCALATED RISK: 96-120

MODERATE RISK: 25-60

HIGH RISK: 61-95

LOW RISK: 10-24





cyber
defense

Assessment

28. Does your organization use Anti-Virus Protection?	0	2	
29. Does your organization use Intrusion Detection Software?	0	2	
30. Does your organization perform System/Info. Backup tapes?	0	2	
31. Does your organization employ Username/Password Management?	0	2	
32. Are your organizations' Wireless Access Points Secured?	0	2	
33. Does your organization Encrypt Sensitive Data in transit?	0	2	
34. Does your organization Encrypt Data at Rest on Servers?	0	2	
35. Have you implemented Pre-Test Software Patches?	0	2	
36. Have you performed 3rd Party Network Intrusion Tests?	0	2	
37. Does your organization encrypt confidential information stored on Portable Devices, such as, laptops, flash drives, back-up tapes, smart phones, tablets, etc.?	0	2	
38. Does your organization use any 3rd party or outsourced vendors to service or store their customer and/or employee data?	0	2	
39. Do you have procedures in place to comply with HIPAA?	0	2	
40. Do you have procedures in place to comply with State Notification Laws?	0	2	
41. Do you have procedures in place to comply with HITECH Act?	0	2	
Page Three Total			

ESCALATED RISK: 96-120

MODERATE RISK: 25-60

HIGH RISK: 61-95

LOW RISK: 10-24





cyber
defense

Assessment

42. Do you have procedures in place to comply with State/Federal Privacy Laws?	0	2	
43. Do you have procedures in place to comply with Graham-Leach-Bliley Act?	0	2	
44. Do you have procedures in place to comply with Sarbanes-Oxley?	0	2	
45. Do you have procedures in place to comply with FACTA/Red Flags Rules?	0	2	
46. Do you have a procedure to monitor material displayed on your website for copyright, trademark, libel, slander or Invasion of privacy?	0	2	
47. Do you have a procedure to remove or deleted offensive/controversial material?	0	2	
48. Do you publish a bulletin board, chat room, or social networking on your site?	0	2	
49. Do you backup data on real time continuous basis?	0	2	
50. Do you do full backups of all operating systems?	0	2	
51. Do you employ a secure connection to access your data remotely?	0	2	
52. Do you require two-factor authentication to access your network externally?	0	2	
53. Is backup data kept fully isolated from the enterprise network and inaccessible from servers and endpoints that are joined to the network?	0	2	
54. Do you use email scanners and filters?	0	2	
55. Are wire transfer authorizations limited to specific employees?	0	2	
Page Four Total			

ESCALATED RISK: 96-120

MODERATE RISK: 25-60

HIGH RISK: 61-95

LOW RISK: 10-24





cyber
defense

Assessment

56. Do you have a maximum single amount that can be transferred from your accounts?	0	2	
57. Do you have a cap on foreign transactions?	0	2	
58. Do you have a procedure in place to verify transfer requests from vendors and/or customers?	0	2	
59. Do you employ an out-of-band authentication on all transfer requests?	0	2	
60. Do you carry a Commercial Crime/Fidelity policy?	0	2	
Total			

ESCALATED RISK: 96-120

MODERATE RISK: 25-60

HIGH RISK: 61-95

LOW RISK: 10-24

