10 Cyber Security Questions to Consider

Yes	No	
_____	_____	1. Has your company defined and prioritized your most valuable information assets?
_____	_____	2. Has your company developed a cross-functional cybersecurity risk advisory committee?
_____	_____	3. Have you performed vulnerability and penetration tests on company network within the past year?
_____	_____	4. Does your company provide annual or more frequent cybersecurity education and training to your company senior executives, board of directors, and employees?
_____	_____	5. Does your company have an incident response (IR) plan in place? If you answered yes: • Does your IR plan contain the details for data breach notification guidelines for senior executives, company board of directors, and law enforcement? • Does your IR plan define your company policy for the payment of a cyber-ransom?
_____	_____	6. When employees access your company network, do you require multi-factor authentication?
_____	_____	7. Is your organization's network monitored 24 /7 / 365 via a Security Operations Center (SOC)?
_____	_____	8. Do your company Information Technology (IT) policies on the timeliness of performing security patches for operating systems and software applications require a patch be performed within 72 hours from the date the software security patch is released?
_____	_____	9. Is your current budget for information security hardware, software, and services less than 10 percent of your overall Information Technology (IT) budget?
_____	_____	10. Does your organization regularly evaluate its cybersecurity risk management program and the effectiveness of its controls?

If you answered NO to any of the questions above, we strongly advise you to contact an information security specialist who can help you draft a plan to protect your organizations valuable information assets, and who can help you take steps to safeguard your organization by mitigating your cyber risk exposure.

The ASA Group
11807 Hinson Road
Little Rock, AR 72212
https://www.theasagroup.com