



HOW SECURE IS YOUR NETWORK FROM CYBER ATTACK?

Here are the 10 questions you need to ask to discover your network's readiness to fight off a cyber attack

SCORE YOURSELF HERE:

	YES	NO	NOT SURE
Does everyone in your organization know how to recognize a phishing attack? Is security awareness training provided to all employees in the organization? Are stringent policies for email, web browsing and personal mobile devices in place and enforced?	☐	☐	☐
Are your passwords sufficiently complex and frequently changed? Are password policies in place that are enforced regularly, with scheduled password updates mandated for all employees on a regular basis?	☐	☐	☐
Do you test your firewall regularly? Is regular testing of your firewall's security completed by your IT team? Does this testing include documented open/closed ports?	☐	☐	☐
Does your organization have a detailed Information Security Policy? Does this policy clearly outline anticipated IT security threats, and provide step-by-step strategies on how to mitigate and contain those threats?	☐	☐	☐
Is your data encrypted? Do you encrypt company data on all available machines and devices in order to prevent unauthorized access and theft of valuable data and information? Are your backups encrypted?	☐	☐	☐
How prepared is your incident response team if you come under attack? Has your organization's designated Incident Response team built and tested an in-depth Incident Response Plan? Does the plan address all breach scenarios, and outlined their specific response steps?	☐	☐	☐
Is someone monitoring your network 24/7? Does this network monitoring service provide security scanning, round the clock monitoring and reporting on all security vulnerabilities? Does it also provide on-going network performance analysis?	☐	☐	☐
How stringent is your removable media policy? Does your removable media policy outline the types of media that can be used, the types of information that can be transferred/shared?	☐	☐	☐
Is your mobile staff protected? Has a mobile security risk assessment been performed, and appropriate security policies put into place for off-site employees? Is security training provided for off-site employees, as well as VPN access (if applicable)?	☐	☐	☐
Are you testing your backups regularly? Is regular testing of backup restores being conducted? Does the testing include data recovery and restoration as well?	☐	☐	☐

NOT HAPPY WITH YOUR RISK LEVEL?

Talk to us about a risk assessment-we're waiving our regular fee for pre-qualified companies like yours, **for a limited time only.**

When we've completed your assessment, we'll review our findings with you. Contact us today.

RON DEANGELIS

Jump Start Technology President/CEO



HAVE QUESTIONS? WANT TO LEARN MORE?

CONTACT US TODAY FOR YOUR FREE RISK ASSESSMENT

Give us a call

650-949-0667

Visit us online

www.jumpstarttech.com