networkiq

10 things

YOUR IT COMPANY SHOULD BE DOING

MORE INFO :

0333 234 4288
info@networkiq.co.uk
https://networkiq.co.uk/contact/

Is your current IT company doing their job?

Here are 10 things they should be doing.

If your current IT company does not score a "Yes" on every point, they are NOT adequately protecting you. Don't let them "convince" you otherwise and DO NOT give them a free pass on any one of these critical points.

1. **Do they proactively monitor, patch and update your computer network's critical security settings?** If yes, do you know how frequently they are doing it? Is it daily? Weekly? Less frequently? Are they reviewing your firewall's event logs for suspicious activity? How do you know for sure? Are they providing ANY kind of verification to you or your team?

2. **Do THEY have adequate insurance to cover YOU if they make a mistake and your network is compromised?** Do you have a copy of their current policy? Does it specifically cover YOU for losses and damages?

3. **Have you been fully and frankly briefed on what to do IF you get compromised?** Have they provided you with a response plan? If not, WHY?

4. **Have they kept their technicians trained on new cyber security threats and technologies, rather than just winging it?** Do they have at least ONE person on staff with CISSP (Certified Information Systems Security Professional) or CISM (Certified Information Security Manager) certification? Do they have anyone on staff experienced in conducting security risk assessments?

5. **Do they have a ransomware-proof backup system in place?** One of the reasons the WannaCry virus was so devastating was because it was designed to find, corrupt and lock BACKUP files as well. **Ask them to verify this.**

6. **Have they recommended or conducted a comprehensive risk assessment every single year?** Many insurance policies require it to cover you in the event of a breach. If you handle "sensitive data" such as medical records, credit card and financial information, etc., you may be required by law to do this.

7. **Have they implemented web-filtering technology to prevent your employees from going to infected websites, or websites you DON'T want them accessing at work?** Porn and adult content is still the #1 thing searched for online. This can expose you to sexual harassment and child pornography lawsuits, not to mention the distraction and time wasted on YOUR payroll, with YOUR company-owned equipment.

8. **Have they given you and your employees ANY kind of cyber security awareness training?** Have they offered to help you create an AUP (acceptable use policy)? Employees accidentally clicking on a phishing e-mail, downloading an infected file or malicious application is still the #1 way cyber criminals hack into systems.

9. **Have they properly configured your email system to prevent the sending/receiving of confidential or protected data?** Properly configured e-mail systems can automatically prevent e-mails containing specified data from being sent or received.

10. **Do they offer, or have they at least talked to you about, Dark Web/Deep Web ID monitoring?** There are new tools available that monitor cyber crime websites and data for YOUR specific credentials being sold or traded. Once detected, it notifies you immediately so you can change your password and be on high alert.

Our free Cyber Security Risk Assessment will give you the answers you want, the certainty you need

If you want to be sure your network and systems are protected, you should get an independent Security Risk Assessment. For a limited time, we are offering to give away a Free Cyber Security Risk Assessment.

This is entirely FREE and without obligation. Everything we find and discuss will be **strictly confidential**.

When this Risk Assessment is complete, you will know:

- **If you and your employees' login credentials are being sold on the Dark Web.**
- If your IT systems and data are **truly secured** from hackers, cyber criminals, viruses, worms and even sabotage by rogue employees.
- If your **current backup would allow you to be back up and running again fast** if ransomware locked all your files.
- If employees truly know how to spot a phishing e-mail.
- If your IT systems and backups are in sync with **compliance requirements** for GDPR, Cyber Essentials, CQC, or PCI DSS and using best practices to ensure your business and customer data is protected from cyber threats.

If we DO find problems we will propose an Action Plan to remediate the situation that you can have us implement for you if you choose.

Get the facts and be certain you are protected.

Contact us and schedule your Free, CONFIDENTIAL Cyber Security Risk Assessment today: https://meetings.hubspot.com/ajani/free-assessment-niq . Feel free to also reach out to me direct at the phone number and e-mail address below.

Dedicated to serving you,

Ajani Bandele
Web: https://networkiq.co.uk/contact/
E-mail: a.bandele@networkiq.co.uk
Direct: 0333 234 4288