4 WAYS Your Employees Could Be Putting You At Risk

Questions to assess the cyber readiness of you and your employees

With the ability for hackers to establish a beachhead in your business with little to no effort, here are 4 simple questions to help inform your cyber risk and readiness. Data is based on the results of 1,000+ security risk assessments for Small and Medium-Sized Businesses. How do you stack up?

01

Do you programmatically train and test your employees about current security threats, company security policies, and the personal role each employee plays in keeping the business safe from cyber threats?

- **57%** have not informed and trained their users on cybersecurity.
- **Security Awareness.** Train your employees often! Teach them about data security, email attacks and your policies and procedures.

02

Do you maintain awareness of the latest tools, tactics and procedures (TTP) of cyber criminals and regularly assess your environment for vulnerabilities and potential defensive blind spots?

- **48%** have not analysed cybersecurity attack targets and methods.
- **Security Awareness.** Establish a defensive baseline and close existing vulnerabilities. Look for tactics that target users, e.g. how much SPAM is reaching employees? Are strong passwords enforced? Do you deny or limit USB access?

03

If, for example, you discovered a phishing campaign targeted at your finance team or potential exposure of confidential information due to a system misconfiguration, do you have cyber incident response policies and plans in place for remediation?

- **42%** do not have a response plan for a cybersecurity incident.
- **Incident Response Plan.** The National Institute of Standards and Technology (NIST) outlines four phases of an incident response plan: Preparation; detection and analysis; containment, eradication, and recovery; and post-incident activity. Planning can feel overwhelming. Reach out and discuss first steps.

04

In the aftermath of an attack, do you have plans and policies in place to examine root cause analysis, test and return to secure production, and how to respond to new threats in the future?

- **75%** do not have a recovery plan for a cybersecurity incident.
- **Incident Response Plan.** Understand the root cause of an incident and what you can do to prevent it happening again. Cybersecurity is everyone's job—instil cyber diligence as part of every employee's mindset.

We can help you better protect your business through a simple and easy risk assessment designed to identify security blind spots. Armed with a risk score in hand and vulnerabilities prioritized by category, we'll help you develop a plan to course correct.

Let's talk and explore your security needs!

www.trustsystems.co.uk

marketing@trustsystems.co.uk