Are you secure?

How well is your company protected against cyber attacks?
Check it out with this quick-check, and start improving your cybersecurity!

Imagine that a cyber attack happens on your company today...

Yes　No　I don't know

1. Tasks & responsibilities

Has your company defined who is responsible for cybersecurity?

Does that person have the necessary knowledge, skills, and empowerment, to deal with the situation?

Do you know how you will minimise the economic impact if the attack is successful?

2. Awareness

Do your employees know how to work securely, and not to expose your business to cyber threats?

Do your clients know how to work securely?

Do your vendors know how to work securely?

3. Data protection

Do you store your sensitive and critical data encrypted in all devices (including mobile devices)?

Does your company handle personal and sensitive data compliant with the EU General Data Protection Regulation (GDPR)?

Have you protected the physical access to computers, servers, and the network of your company?

4. Backups

Do you have a recent backup of your data and your systems?

Is a backup available offline, or at least at a different place and completely disconnected from your systems?

Have you tried to restore a data and or system backup and seen that it is working?

5. Password and user administration

Are your employee's passwords strong and specific for each user account and system?

Can each employee (including former employees) only access the systems they are supposed to?

If any employee has experienced a cyber attack, have that employee's passwords been changed?

6. Malware protection

Does your IT network have a firewall that protects your systems from outside attacks?

Are your devices, systems, and applications protected against malware (e.g. antivirus, ransomware protection, spam filter)?

Is your malware protection configured to scan mail attachments, downloads, and connected storage media?

7. Updates

Is all software (applications, operating systems) on your employees' devices regularly updated?

Is your malware protection (antivirus program, spam filter) regularly updated?

Is all software of your servers and devices, including the firewall, regularly updated?

8. Secure communication

Are the passwords and data sent encrypted between the clients and the servers?

Is your wireless network (WLAN) encrypted and protected?

Do you require your employees at home to use a Virtual Private Network (VPN) to access your systems?

Is your WLAN for employees separated from the WLAN for guests?

9. If you develop software or devices

Did you define who is responsible for the security of each of your software products and services?

Did you perform code inspection, especially to detect vulnerabilities and security loopholes?

Have you done black-box testing against the common security threats?

10. Emergency response

Is the person responsible for cybersecurity able to end the cyber attack and limit its effects?

If your clients or vendors are attacked, and you were affected, would they inform you?

Count the number of 👍 answers! ➡ **Your result:**

0-9 Alarm level RED!!! Get started NOW: Turn the easiest 🧑 and 👎 answers into a 👍 !

10-23 Hmm, think about how it would feel to be secure – get GEIGER on www.cyber-geiger.eu !

24-29 You do quite a lot of cybersecurity already – stay updated about new treats and better protection with GEIGER!

30 Wow, you are a reference for small businesses – we want to work together with you for helping other businesses! Meet us in an event www.cyber-geiger.eu/events.html or send us a message at www.cyber-geiger.eu/contact.html !

Install the app, enroll in the GEIGER beta trial, give feedback, and benefit from the discount for beta testers for the future versions of the GEIGER solution!

www.cyber-geiger.eu

Check the availability for