Cyber security check - where is your company?

Please mark:
1 = hardly applies
5 = fully applies

At our company, cyber security is **anchored throughout the organization** and is defined by clearly defined roles and responsibilities: from the executive floor to IT management through to the specialist departments. Staff are available to fill these roles. 1 2 3 4 5

We have **an inventory overview and therefore an overview** of our data and all assets data and all assets, e.g. software, systems, users, identities, infrastructure, vendors and environments. We classify data according to categories such as *public*, *confidential* and *internal*. 1 2 3 4 5

We have **fixed rules** on how employees and external parties should handle company IT resources and critical data. The rules are based at least on standards such as ISO or BSI standards. 1 2 3 4 5

Our IT staff continuously build up **cyber security knowledge** through training. We create a fundamental awareness of cyber security among all employees through training and a targeted communication strategy. 1 2 3 4 5

Through regular security tests and assessments, we minimize the risk of **cyber security incidents**. In the event of an incident, all those responsible know how to recognize it and how to react. 1 2 3 4 5

We use a **central Identity & Access Management (IAM) system** for all data, resources, applications and machines as well as standardized IAM processes for e.g. *joiners*, *movers*, *leavers*, *grants* and *revokes*. Security is provided by password policies, strong multi-factor authentication and dynamic access controls. 1 2 3 4 5

We ensure **data protection** through modern technologies and data governance. We encrypt data depending on its use, e.g. through secure mailing & messaging. We protect ourselves against data loss through data loss prevention (DLP) and backup & recovery measures.
We are also aware of the compliance requirements to be met in all our business processes. 1 2 3 4 5

We provide comprehensive protection against **cyber attacks** through endpoint security and firewalling, network segmentation, malware protection/antivirus programs, cloud security posture management, automatic security scanners, device management and patching. 1 2 3 4 5

We have a **security monitoring system**. 1 2 3 4 5

We are aware of the error-prone nature of manual processes and **automate** as many processes as possible, e.g. monitoring, risk detection, data classification and patching. 1 2 3 4 5

Take your cyber security to the next level!

Please add up the points you have ticked. Depending on this value, we will give you the following recommendations:

Sum 10 - 20: You are concerned with the topic, but also know that there is an acute need for action in some areas. We help you identify security gaps and initiate measures to implement solutions.

Total 21 - 40: You are already on the way to making cyber security an integral part of your company. Together we can work out where there is further potential for improvement, e.g. through concepts such as Zero Trust. In this way further minimize security risks.

Sum 41 - 50: You are already very well positioned in terms of cyber security. Now it's time to keep your security level up to date. Feel free to contact us and together we will find out how you can refine your strategy!

Your guide to more cyber security

Wherever you currently stand: Let us deepen the dialog. Together we will find out how you can position yourself even more securely and which measures will be helpful for your company in the short, medium and long term.

Dr. Jan Ciupka
Executive Manager Consulting
+49 228 9770-0

Write to me and we will arrange an exchange appointment!

GET IN TOUCH