Secure the management's commitment to cybersecurity

How do you go about securing management's commitment so that cybersecurity is prioritised? Here are a few things you should think about!

1. Analyse the risks

In order to make the right priorities in security work, a risk analysis is needed - a security protection analysis. It defines the most valuable assets of the business, the consequences that can arise if these assets are attacked, what the actual threat is and what vulnerabilities that exist. Based on this, appropriate security actions can be proposed.

2. Explain the consequences

Obviously, you must inform about the consequences that can happen if you do not work with information security. There are several known cases of ransomeware attacks, such as the Maersk case and Baltimore in the United States that may be mentioned. But it is even better to give examples based on your analysis. If, for example, you found out that you have shortcomings in the software updates, it is more communicative and convincing to say that "a hacker can copy the entire payroll and post it on the internet" than talking about having to do a number of security updates.

3. The investment is less than the opportunity cost

One possible argument is, "But doesn't it cost a lot to introduce a structured approach to information security?" This is something you can quickly respond to by explaining that the opportunity cost, caused by an attack, usually is so much higher than the investment needed. With a constantly increasing number of attacks, the risk of being hit is relatively high. Therefore, not investing in information security really means that, as a company, and management, you take an extremely large financial risk. Does management really want to take that risk?

4. Highlight the benefits

It is better if management associates information security with something positive and understands that it is not so complicated. Therefore, it is important that you end your argumentation by explaining that a systematic information security work means that you can avoid negative publicity, information leakage, possible downtime - simply avoid several risks of losing business.

ISO 9001 CERTIFIED
ISO 14001 CERTIFIED