advenica

8 pieces of advice when starting information security work

The digital world places new and higher demands on information security. The ever increasing connectivity offers many advantages and opportunities but also opens new ways for attackers to get into our computers and/or systems.

New laws have been passed to increase preparedness. These require that organisations delivering services essential to society increase their information security. However, it is not always easy to know where to begin. Here are eight pieces of advice to get you on the right track.

1. Realize that information security means more than technology

Today, a great deal of information is managed in IT systems, often making information security equivalent to IT security. However, information security is not a novel concept – on the contrary, it has been around ever since the Stone Age man sat in his cave and whispered secrets to his friends. IT security, on the other hand, entered the scene with computers.

Information security is often mentioned in connection with technology. But it is crucial to understand that it is much, much more. People and processes have to be included, and all parts are equally important to succeed. Systematic and continuous work based on assets, threats and risks is vital for creating sustainable protection.

2. Information security work has to be linked to your organisation´s risk management

All security work has to be based on how risks are managed in the environment where you operate. Organisations may also face financial risks, natural disasters, sabotage, competing technologies, etc. Information security-related risks have to be treated the same way as other risks.

3. Ensure that management takes its responsibility

The responsibility for security work always lies with management, as only management can decide NOT to do something about security risks. Given how the rate of cyberattacks are accelerating, a decision NOT to invest in information security means that both the organisation and its management take a huge financial risk. Is your management prepared to put that on the line?

4. Review procedures and processes

Information security encompasses the entire organisation's operations and all information, regardless if it is in computers or on a piece of paper. With most information handled by IT systems, information security is, of course, a question of technology, but just as much about the routines that users need to make sure they correctly go about business. Are you aware of how your processes and routines work and what kind of security thinking is applied – or not applied? Start mapping out routines and processes, who has access to information and systems, and the state of your security thinking. With this analysis at hand, you can start discussions on how to ensure information security.

5. Ensure the right resources

Information security work must be conducted systematically and continuously to ensure an adequate level of information security in an organisation. Information security is not a technical solution that you purchase once and for all – it is an ongoing process (plan, do, check, act). Therefore, it is important that management always supports the work, and that the necessary financial and organisational resources are allocated. For successful information security work, you have to have management's commitment and the right resources.

6. Start with an analysis

Systematic information security work should always be adapted to the specific circumstances of an organisation. A recommendation is to start with an analysis of both the outside world and your operations. What are the most valuable assets and which threats are there? This analysis it the foundation for designing information security work and regulatory documents such as a security policy. Based on the results, it is also possible to decide which security measures have to be implemented.

7. Develop a security policy (– this helps you to maintain information security)

Regulatory documents such as a security policy are the formal framework for your information security work. In these, you have to specify what should be available, what should be done, as well as how it should be done. With the aid of these documents you can ensure that the level of information security is maintained, and making it easier to ensure that for instance, new employees get the right information on how to act.

8. Get help from those with in-depth information security knowledge

Getting started with systematic information security work on your own can feel a little overwhelming. If possible, get help from those with extensive knowledge about information security.

At Advenica, we have extensive experience with both general security analyses (risk and security analyses) as well as security protection analyses. We can advise you on how to get started with mapping processes and routines from a security perspective. We also provide expertise and unique, technologically advanced, sustainable and future-proof cybersecurity solutions with high assurance for critical data-in-motion up to Top Secret classification. Contact us at advenica.com/en/contact-us

advenica

ISO 9001 CERTIFIED
ISO 14001 CERTIFIED