What can employers do to protect their companies against cyberattacks?

According to the data published by the Estonian Information System Authority last September, Estonian companies lose more than a million euros a year to cybercriminals. These numbers are just the tip of the iceberg - they cover only the data that has been communicated to this authority. Given the sad statistics of cybercrimes, it is clear that compliance with cyber hygiene by the employees should be considered as essential, as the obligation to wash hands.

A multi-layered approach is advisable to be implemented to mitigate cybersecurity risks. The defense against cyber threats broadly encompasses three components: people (stands for the awareness of the employees towards cyber threats and compliance with cybersecurity best practice), processes (routine procedures to prevent, detect and respond to cyber threats) and technology (implementation of the technological tools to mitigate cyber threats, i.e. firewalls, antivirus and malware software, multi-factor authentication systems, etc.). However, even if the organisation has established proper procedures and uses advanced cybersecurity technologies, the employees can still be a significant vulnerability. For example, if the employees are unaware of the cybersecurity best practices or do not follow them, they can easily fall a victim to phishing attacks. If successful, the cybercriminals will get access to the companies confidential data and assets.

The European Union legislation (General Data Protection Regulation) imposes an obligation to protect personal data processed by the data controller and implement appropriate technical and organisational measures in this regard. It requires organisations to protect their employees' and customers' data used in any internal procedure, system, service or product. However, apart from personal data protection, the laws do not oblige private companies that do not provide essential services or digital services to comply with specific cybersecurity rules. Thus, it is up to each company to assess the risks associated with its particular business activities and implement measures to reduce them. Considering that today the data on trade secrets, intellectual property, and other valuable business information is stored and managed in digital form, it is potentially exposed to cyberattacks. Unfortunately, in practice, the lack of security skills or negligence of the employees is one of the main factors, which causes data leaks and intrusion.

Cybersecurity policy

Compliance with cybersecurity rules can be made mandatory for the employees if these are documented correctly. The obligation to comply with cybersecurity rules can be established in the employment agreement or job description. If the cybersecurity policy is prepared separately from the employment agreement (as an annex to the employment agreement or the job description), then in order to be binding on the employees, it must be introduced to the employees and signed by both parties. It should be taken into account that once the policy is signed, the employer may change it only with the *employee's* consent (similar to the changes in other conditions of the employment agreement).

Cybersecurity policy usually specifies the rules of secure work with data and the mitigation of security risks, including the use of the Internet, the protection of personal and company devices, the security of e-mail communication, password management, specific risks associated with remote working, etc. The policy also contains guidelines for the employees on how to recognize different cyber threats and to act in case of security breaches.

Cybersecurity policy should consider the specific position and the level of risk associated with the nature of employment duties. The use of a standard policy for each employee is not a good idea, as the access rights to the employer's data and work objectives usually vary depending on the position. For example, it is reasonable to draft cybersecurity rules for an office worker and an IT specialist, taking into account the different levels of responsibilities and risks related to their positions. The wider the employee's rights to access and work with the employer's data are, the greater damage the employer may potentially suffer if the employee falls a victim to a cybercrime.

The obligations described in the cybersecurity policy should be reasonable and clear for both parties. The employer cannot rely on the breach of the obligation, which is vague and imprecise or anticipate fulfilment of the obligation requiring a specific skill for which the employer has not provided relevant training. Unreasonable conditions are harmful to the employer as well since they might not be enforceable in court.

Trainings for the employees

The policy alone is not enough to protect a company from cyber risks. The employees' awareness of cyber threats and their role in ensuring the company's cybersecurity is the key factor in avoiding damage. Therefore, the employer must provide employees with regular security training. Since ensuring data security is in the direct interest of the employer, the employer must provide training to the employees in this area at its own expense and pay average wages during the training, according to the Employment Contracts Act.