Q&A

Information security is worth protecting

When cyber risks materialize, they can threaten the entire existence of the company. In this interview, Sami Kehusmaa Team Manager at OP Financial Group of Finland, explains how a cyber insurance policy aimed at small and medium enterprises (SMEs) provides coverage in the event of cyber damage.

1 WHAT ARE THE MOST TYPICAL CHALLENGES THAT COMPANIES FACE IN THIS AREA?

Smaller companies especially have challenges with recognizing cyber risks related to their business and operational network. It may also be difficult to understand how various digital solutions are linked to the company's business and how they affect its financial results. In addition, the new General Data Protection Regulation (GDPR) its requirements and implementation may be a challenge.

2 HOW SHOULD I PREPARE FOR INFORMATION SECURITY RISKS?

An information security policy or instructions describing the importance of information security and data protection to the business should be prepared, and all employees should receive compliance training. For information security, the minimum requirement is to protect the company's ICT devices and networks with up-to-date anti-virus software, firewalls, and backups.

3 WHY SHOULD I OBTAIN A CYBER INSURANCE POLICY?

In the worst case scenario, a cyber attack can interrupt the company's business for a long time and cause significant financial losses to the company, its partners and customers. Traditional insurance policies do not cover the cost of security breaches, data loss or the costs incurred as a result of similar cyber risks. Information owned by another party, such as customer data, is often at risk. Data may be lost or fall into the wrong hands.

A cyber insurance policy enables the company to partially prepare for the liabilities and obligations they would face after a cyber-attack or a security breach.

4 WHAT DOES THE CYBER INSURANCE POLICY COVER?

It covers direct crisis management costs up to the agreed insured amount, consequential losses incurred by the policy holder and financial damage incurred by the other party as a result of the security breach. Crisis management costs include the costs of expert services. It also compensates for the costs of restoring files and software and the costs incurred as a result of the communication obligations set out in the GDPR.

Cyber insurance will not compensate for personal injury, suffering, property damage or fines. In addition, the insurance will not cover damages incurred as a result of inadequate firewalls or anti-virus software or the failure to take daily backups.