NJORD Estonia: Cyber Risk Insurance - is it worth it?

The Information System Authority of the Republic of Estonia consistently points out that cyber-attacks happen every day. We hear more and more about cases where cybercriminals have been successful. The Information System Authority of the Republic of Estonia consistently points out that cyber-attacks happen every day. We hear more and more about cases where cybercriminals have been successful.

Cyber incidents cause property and reputational damage - both of which have a negative impact on the company. With regard to property damage, one possible solution is to conclude an insurance contract, which can also help mitigate cyber risks. The purpose of cyber risk insurance is to insure against damage, such as the cost of recovering data and systems, ransom claims, and damage caused by the cessation of activity.

As with many other insurance products (such as home insurance), insurers impose a number of requirements on policyholders (companies) when insuring against cyber risks, which the companies must comply with. Failure to comply with the requirements may lead to a situation where the insurance does not indemnify the damage or does so to a lesser extent.

Requirements set by the insurers include, for example, the obligation to inform and train the employees about cyber risks, to implement technical security measures (e.g., antivirus soft-ware), and also to back up data.

When setting requirements, insurers' aim is to ensure that policyholders implement measures that would prevent loss events and, thus, the need to pay insurance indemnity. At the same time, the conditions help businesses to meet the requirements that apply to them anyway. For example, if cyber risk insurance requires a company to implement technical protection measures, compliance with this requirement is a step towards meeting the requirements of the General Data Protection Regulation (GDPR). Namely, the GDPR stipulates that the data controller must implement up-to-date security measures.

Thus, concluding an insurance contract helps the company to take the necessary steps to-wards compliance. Complying with insurance conditions does not immediately mean compliance with all other applicable requirements (e.g., GDPR) but can help get closer to compliance and at the same time make one think more about cyber risks.

However, it must be borne in mind that if cyber risks are realised, the insurance will in no way exclude, avoid, or compensate possible fines. The concluding of insurance is not a measure that could be a mitigating circumstance in a supervisory proceeding in the event of an infringement, but at the same time, it helps to recover more easily from damage.

TRIINU HIOB
ATTORNEY AT LAW,
PARTNER

(+372) 66 76 440
TRIINU.HIOB@NJORDLAW.EE