Arendt Governance Alert

Cybersecurity in an era of digitalization, remote work and GDPR

What do I need to know?

Since the beginning of the Covid 19 pandemic, the digitalization of businesses has accelerated considerably and employees continue to work remotely. With this context in mind, the GDPR has strict requirements in terms of technical and organisational measures to protect personal data. Many businesses hold trade secrets or a valuable know-how which they need to protect at all costs. Such changes and constraints imply greater security risks and threats for IT systems. Notification obligations may arise from a cyberattack and businesses must improve their information security in order to be prepared to act quickly and in a coordinated way. It is not a question of if, but when they will be hacked. We are all vulnerable to cyberattacks, there are no exceptions.

Why is this important for me?

While it is impossible to completely eliminate the risks, the Board must take appropriate action to limit these risks as much as possible. The Board is potentially liable if it has not taken all reasonable measures that a normally prudent and diligent Board would take. Boards need to protect their business against cyberattacks by having an emergency and business continuity plan.

Normally, organisations have contractual, legal and/or regulatory obligations to protect the data they are processing and which can be potentially violated in case of a cyberattack. In case of violation of those obligations, the risk of regulatory or administrative fines is high and third parties (employees, clients, investors, suppliers) suffering a direct damage from a cyberattack, could potentially start lawsuits.

What should I do?

In this context, the Board cannot remain passive but must ensure (i) that the company has taken the necessary measures to be prepared and protect its IT systems, (ii) that its staff at all levels are aware of the risks and what needs be done to minimize them and (iii) that a response plan is readily available in case of an incident. To summarize:

- Is cybersecurity and security a standing item on Board meetings' agenda?
- Are regular and mandatory cybersecurity awareness trainings in place?
- Do I need to consider appointing a CISO?
- Are my business' security maturity and risk assessed on a regular basis?
- Are the necessary strategies, policies, procedures and tests in place to limit the likelihood of an incident?
- Is the necessary action plan in place? Is the plan regularly tested and is my staff prepared to manage an incident or an attack?
- Do I have a panel of specialists (legal, technical and communication) in place to assist in case of a cyberattack?
- What about contracting a cybersecurity insurance policy?
- Did I consider cybersecurity as an integral part of the due diligence process on my service providers?

Arendt Corporate Governance Centre - How can we help you ?

A sound corporate governance framework is a key element for efficient management and control and the long-term success of companies. Optimise your activity with a comprehensive set of solutions to deal with every aspect facing a board, be it legal, tax, regulatory or compliance.

Contact us: corpgov@arendt.com