SPECIAL SECTION
Cybersecurity

Prevention and Cybersecurity

We are frequently startled by international cyberattacks. Hackers steal confidential information and ransomware shuts down companies, hospitals and governments. Since company computer systems are increasingly connected to the Internet (online stores) and also rely on Information Communication Technology (ICT) for internal processes, they are not just more vulnerable to attacks, but the impact of such attacks is higher. Orders cannot be processed, documents cannot be accessed, (manufacturing) processes are interrupted, and client data is made public with the risk of high regulatory fines. Obviously, you can prevent that by taking IT measures. Less obvious, but still as important, is that you can take preventive legal measures to reduce the risk of an attack, limit the potential consequences of a hack and invest in your cybersecurity.

This article deals with concrete preventive legal measures you, as a director or supervisor, can take to guarantee the safety of the company to the greatest extent possible, and thereby comply with your duty of care. A breach of the duty of care may lead to directors' liability.

Management

Cybersecurity must be dealt with at the highest level. In addition, there has to be the required expertise. It has to be discussed at management level what kind of systems will be used and what the risks involved in using them are. This has consequences for the structure of the organization, the management and the company.

Chief Information Officer

Appointing a chief information officer (CIO) is a good way to acquire digital knowledge, centralize it and use it effectively. Many large and medium-sized companies have CIOs as the ICT has no longer only a supportive role but is leading in all company processes. The CIO is a member of the management and has the ultimate responsibility for the ICT policy of the entire organization. This is necessary for the company and will reduce the risk that the company and director are liable in the event of infringements relating to cybersecurity.

Maybe your company is too small to employ a CIO. This does not change anything regarding the distribution of responsibility. The management or board of directors will be ultimately responsible for cybersecurity and the application of privacy regulations and will therefore have to make sure to possess the competence required in this field.

Supervisors

In appointing supervisors and non-executive directors, make sure to consider people who are familiar with digital risks so that they will be able to exercise their supervisory and advisory role sufficiently. After all, it is their task to advise the management board on digital security and to control the processes within the company in this respect too. In addition, the supervisors can benefit from this knowledge as they could be liable in case of insufficient supervision.

Corporate Structure

Risks can be reduced by incorporating the development of a new product or service, such as a new app, in a separate legal entity, whether or not with a separate ICT network. If matters turn out to be undesirable, the consequences for the remaining company will be limited.

Personnel

Most problems in the area of ICT arise accidentally, by human errors. All people involved in the company, employees but also contractors and agency workers, therefore have to be aware of the importance of cybersecurity. This is called security awareness. Security

Reinier W.L. Russell

Reinier W.L. Russell is the managing partner of the Dutch law firm Russell Advocaten B.V. He is an experienced lawyer who serves as outside corporate counsel for both domestic and foreign businesses in the retail and IT sectors. He deals with business formation and reorganization, corporate governance, employment issues, real estate and all aspects of liability and contract law.

Russell Advocaten B.V.
Reimersbeek 2
1082 AG Amsterdam
Netherlands

+31 20 301 55 55 Phone

reinier.russell@russell.nl
russell.nl

awareness exceeds merely reacting to incidents: it has to be guaranteed via a continuous process in which an organization can reduce risks to an acceptable level. This could be, among other things, by drafting a personnel handbook including guidelines on internet usage, emails and passwords. Further, it should be clearly defined that employers have to report abuses, how they have to be reported and what the time limit is. Otherwise, companies would have to depend on the reasonable conduct of their employees instead of being able to require such conduct.

Contracts

When concluding all contracts, not just ICT contracts, it is important to distribute responsibility and limit liability. After all, your company is responsible for the ICT you use. This does not change if your ICT only has a supporting function or if you have not developed the ICT yourself.

Check for instance your General Terms and Conditions, where liability can be excluded, limited or transferred to a third party but also concrete arrangements such as Service Level Agreements (SLAs). The scope for agreements will be more limited if the counterparty is a "consumer." A provision in the General Terms and Conditions of an agreement has no legal consequences (it is "voidable") if it is extremely disadvantageous ("unreasonably onerous") for the consumer. A provision stipulating that your company has no or limited obligations in the area of cybersecurity will probably be unreasonably onerous. Besides, arrangements agreed upon only apply with regard to the party you concluded the agreement with.

It is crucial to phrase agreements clearly. Vague agreements bear the genuine risk that a court will interpret provisions, at least in the event of a conflict, to the detriment of the company. Suppose that your company determines in an agreement that it shall not be liable if a cyberattack causes its being too late in fulfilling its obligations. Without a more detailed description of this term, a conflict could arise on the question as to whether a certain kind of malware would constitute a cyberattack.

Your company can lastly not exclude all liability. Obviously, hardware and software, apps and web-based tools must comply with the latest requirements in the fields of security. Therefore, despite exoneration clauses the company remains liable regarding, for instance, if it uses, with the knowledge of the management, ICT whose cybersecurity falls short. A company using obsolete software to save costs and not taking measures to protect its computers and networks will probably not be able to invoke a stipulation excluding liability if a lack of security causes damage.

If legal means are not sufficient to limit the liability of a company and directors, the financial consequences can be limited by cyber insurance and directors' liability insurance.

Privacy

The importance of cybersecurity is underlined by the privacy laws and high penalties for infringement on privacy.

Personal data is usually processed by means of ICT. In Europe, strict rules apply to this that can affect companies worldwide. The basic principle of the regulations is that they apply to the processing of personal data from Europeans even if the processing takes place outside Europe.

A breach of the security obligations has severe financial consequences. The Dutch Data Protection Authority (Autoriteit Persoonsgegevens; AP) can currently impose a maximum fine of EUR 820,000 per breach or 10 percent of the annual turnover.

As of May 25, 2018, the AP will be able to impose a maximum fine of 20 million euros or a fine of 4 percent of the worldwide annual turnover should this amount be higher.

Conclusion

The board of a company has the ultimate responsibility for cybersecurity and can be held personally liable in the event of breaches. The board has to examine the organization and (ICT) company processes for compatibility with the existing regulations. In addition, the board has to make sure that both managers and supervisors have expertise in this area, for instance by appointing a chief information officer to the board. Employees must be familiar with the cybersecurity policy, for instance via the staff handbook or internal training. In contracts, liability for cybersecurity problems can be limited to the greatest extent possible. Should this not be enough, insurance can also be a solution. P