Management of Digital Risks

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
+31.20.301.56.78 Fax

reinier.russell@russell.nl
russell.nl

In the Spring 2015 issue of this publication, we addressed the subject of risk management. This article will focus on one particular type of risk – digital risk. Firms' IT systems can be breached both from the inside and from the outside. For example, breaches can come from a network attack (hacking, distributed denial of service [DDoS]), viruses (Trojan horse, time bombs, worms), cybercrime, human error, a failure of the IT provider or power failure. The consequences for an enterprise can be serious – inaccessibility of the network, loss or theft of (part of) the computer system, data destruction, data manipulation, leaking of confidential information or personal data and related privacy issues. What are the legal options to manage these consequences and to ensure the continuity, security and privacy of the network and information systems of the company?

Contracts and Liability

Regarding digital risks, most business owners will immediately think of the security of the software and the quality of the hardware. However, you can limit digital risks and manage any potential negative effects in advance by means of good information and communications technology (ICT) contracts.

Entering a Contract

For the different digital services (such as maintenance and operation of the network system, data processing and data storage) the company will conclude contracts with different ICT suppliers (providers, cloud servers, big software providers, such as Microsoft, Apple and Google). These contracts are often standardized. However, an enterprise does not have to accept such standard contracts unreservedly, and it is advisable to negotiate the contents of such contracts. The contract has to provide clarity for both parties on several basic things: Who is responsible for what? Who has the power to do what? And what are the rights and duties of the parties involved in the service chain? Here, it is vital to observe the liability for claims of clients or third parties.

Besides negotiating the agreement, the use of your own General Terms & Conditions is highly advisable. Make sure that the General Terms are declared applicable correctly. If this turns out to be difficult, try to explicitly exclude specific provisions of your counterparty's General Terms in the agreement, as they often contain far-reaching exemption clauses. Also, check whether the General Terms of the provider contain a unilateral changes clause and make sure that the General Terms can only be changed with your permission or include in any case a notification obligation on the part of the provider in the event of a change in service. Finally, it is important to make clear arrangements in a choice of law and choice of forum clause with regard to the applicable law and the competent court.

During the Contract: Service Level Agreement and Security

The performance of the contract can be implemented via a service level agreement (SLA), which is rather common practice in ICT. An SLA includes, among other things, agreements on the level of quality and availability of the services (technical and functional specifications).

An important risk which has to be considered in the SLA is the security of the ICT systems and the data of the enterprise, especially if work is performed in different locations or in the cloud. Therefore, make agreements on the improvement of the network protection not just by firewalls, but also by means of encrypting and masking data. Authentication systems can provide the enterprise with extra protection against undesirable external factors, for instance, by the use of login codes, (changing) passwords and digital certificates. Also, define who will be responsible in the event of security breaches and thus for the damage of the enterprise, clients or third parties.

In addition, it is advisable to include a notification obligation on the part of the provider in the event of security breaches and other data leaks. You can also include in the agreement a back-up obligation on the part of the ICT provider, so that there will be an alternative besides your own back-ups.

An enterprise should of course also ensure the data privacy of clients and third parties in the network and information systems. The entrepreneur is responsible for correct storage and processing of personal data. Therefore, it is important to include in the agreement with the ICT provider who is or will remain the owner of the data, who has access to the data and/or is allowed to use it. A (mutual) confidentiality clause and a penalty clause can be included in the agreement and serve as a means for the compliance with these agreements. A prohibition to transfer personal data to third parties may also be necessary.

After the Termination of the Agreement

To ensure the continuity of the enterprise, clear agreements must be made regarding the termination of the agreement and what will happen with the data and systems in the event of bankruptcy or the takeover of a supplier. Thus, for instance, make sure to avoid a "vendor lock-in," by which the enterprise is not able to switch to another supplier because the data cannot be transferred (easily) to the new provider. Conversely, it is also important to determine what will happen to the data and systems if the enterprise does not comply with agreements, has outstanding bills, goes bankrupt or is otherwise in default. The enterprise is well-advised to include an obligation on the part of the provider to return the data in the event of the termination of the agreement.

International Regulations

Obviously, all agreements must be in accordance with national and international laws and regulations. This may be rather complex if the enterprise contracts with foreign parties or the data will be stored on a (cloud) provider's system, which is physically located abroad. The enterprise is thus well-advised to investigate who the contracting partners in the service chain are and where the data will be physically stored. By including investigative or monitoring powers, the enterprise can investigate whether the supplier complies with the applicable legislations so that the enterprise can also comply with its legal obligations.

Besides, the nationality of the persons whose data are digitally processed is relevant. For example, on grounds of the current European Data Protection Regulations, businesses from non-EU Member States have to provide an "adequate level of protection" for the storage and processing of personal data of EU inhabitants. A Thai business processing data of Italian customers in the U.S. is also subject to this Regulation, even though there is no physical relationship with Europe. In this case there is a problem because due to the so-called "USA Freedom Act" (formerly, Patriot Act), the United States does not comply with the European regulations. Until recently, transfer of personal data was permitted if an American company committed itself to comply with the "Safe Harbor Privacy Principles." On October 6, 2015, the European Court of Justice decided however, that the United States (American ICT service providers) could not provide an adequate level of protection for personal data. Currently, the European Union and the United States are working on finding a solution for this.

Meanwhile, for the protection of the privacy of EU-citizens, the European Parliament has drawn up a General Data Protection Regulation containing stricter rules and higher fines (see: "New Privacy Rules for European Union Will Apply to Companies Worldwide," *The Primerus Paradigm* Fall 2015). It is expected to become effective in 2017.

Conclusion

Entrepreneurs do almost everything digitally, but the risks of digital business operations are often not fully taken into account. With this article, we have tried to create greater awareness of digital risks and offer suggestions to manage them. Your outside corporate counsel, who knows your business like no other person, will be able to provide advice so that you will be aware of potential risks and be able to cover them legally, if desired. Then you, as entrepreneur, will be able to confidently use all the opportunities provided by the digital work environment. P