Your data is at risk!

An All-digital supply chain management offers significant advantages: The cost of data entry can be reduced and the entire process shortened. But how realistic is complete digitisation in the near future? An internationally oriented supply chain encompassing several participants involves considerable legal and IT-problems.

When Information is passed on from one participant to another, it has to pass through a number of interfaces. If it is exchanged across international borders, the compliance requirements are even more stringent. This is due to the fact that the communication and storage of data is governed by different rules and regulations in different countries. This also applies to the question of the extent to which electronic documents are acceptable in the first place, or whether the laws of the countries concerned (still) require the use of original, hard-copy documents.

Who owns the data?

Safety-related issues arise in the context of transmission. The data passes through the systems of the most varied participants and under certain circumstances, even systems in various different countries. Who sets the standards which these participants have to comply with? This is linked with the difficult-to-answer legal question: Who is the real owner of the data and who is responsible for its safety? Even more questions arise: How are security factors configured in the various systems? Specifically, are there access possibilities which are difficult to rule out? How can it be ensured that the data is not copied, stored or passed on in the external systems without authorization?

Data storage and archiving: Who has access?

On the other hand, the storage and archiving of documents poses yet another challenge to the safety factor. What is decisive here is which solution is selected. Is cloud storage feasible? Who gets access rights in this case? Or does the company (which company?) use its own data storage facilities? Should a common portal be created for all participants concerned? Each of these solutions has its own specific vulnerabilities that allow unauthorized access to the data.

Data theft with fatal consequences

It should be clear that digital supply chains in particular, in addition to the benefits mentioned above also harbour tangible risks of data theft. These can have serious consequences for the companies involved - especially if the data contains sensitive information on subjects such as pricing, CRM or production secrets. If this information falls into the hands of competitors, criminal organizations or rogue government agencies, this can, in extreme cases, threaten the very existence of a company. For example, it is assumed that the theft of the 1.5 million dollar shipment of iPad Minis at JFK-Airport in New York in November 2012 was made possible by a data leak.

Malware and Trojans

In addition to the theft of data, there is also the risk of files being infected with malware. If as a result, data is corrupted, distorted or rendered unreadable, this can cause very perceptible problems in the supply chain. The installation of espionage tools such as Trojans, which enable access for data theft and espionage, is also conceivable.

GSL Consulting LLC
Hagartenstrasse 25
CH-4562 Biberist

Phone : +41 41 500 68 85
Fax: +41 41 500 68 86
www.gsl-consulting.ch

The discussions so far show that EDP-based Supply Chain Management requires very diligent preparatory work. EDP-experts and jurists must work together to frame codes of conduct, standards and technical specifications, to ensure that unauthorized access to data is precluded in each and every link of the supply chain, whether by thieves or a result of infiltration of malware. In doing so, they will have to deal with the problem that each of the different participants involved have individually customized IT environments that often differ substantially from one another. This complicates communication of the individual systems with each other and also the setting up of common standards.

Solutions: Don't throw the baby out with the bath water

Existing approaches have hazardous vulnerabilities. GS1 standards do indeed allow a reliable exchange of information while neglecting the issue of unauthorized access to the data. More effective is the outsourcing of the data flow and data management to a central reliable service provider, of the type envisaged in the guidelines of the National Institute of Standards and Technology (NIST). In attempting to avoid risks it is not very helpful to provide as little sensitive data as possible. In certain cases this nullifies the benefits of using EDP, since restricted data access permissions lead to delays and increased consultation and processing costs. The development of 'smart' action-packages by jurists and EDP experts is a more cost-effective alternative in the long term.

Conclusion:

The digitisation of the Supply Chain is, on the one hand, a powerful tool to accelerate the flow of goods and to minimise costs. On the other hand, it involves not merely the increased use of information technology but also legal and technical problems and risks for data security which need to be addressed specifically. Otherwise the hazards of damage can be enormous.

Thorsten Vogl / Legal Advisor / Associate GSL Consulting LLC

The original German version of this article appeared in the magazine "procure.ch - Procurement Management - 03/2015

GSL Consulting LLC
Hagartenstrasse 25
CH-4562 Biberist

Phone : +41 41 500 68 85
Fax: +41 41 500 68 86
www.gsl-consulting.ch