The Internet - Opportunities and Risks from an Insurance standpoint

Report By Cologne Re

A Few years ago, the Internet was something only for specialists and accredited IT experts - now, it has already become a part of everyday life. Today, the website is not only a trademark of communicative Companies, it also increasingly performs the function of providing direct access to clients, goods and services. Following modest beginnings, the sale of products - generally termed electronic commerce - has undergone a dramatic development in the last few years and the forecasts are breathtaking. Convenience for The client, transparency of prices and services and the possibility of choosing from a genuinely worldwide range of products are the most important advantages of this sales channel.

The insurance industry must also adjust to this development. Whereas, at the initial stage, the insurers websites were still very Much restricted to providing company and product-specific information, there are now clear signs that the development is leading to a supply of more comprehensive services. The range comprises not only insurance and investment products but also assistance in the event of a claim and during the settlement of a claim, as well as the provision of information which creates direct added value for the client. This could consist, for instance, of the results of corporate research, of statistics, or useful addresses for all walks of life, or cross-references to the offers of associated or other non-competitive players. In the beginning, mainly products which Needed little explaining were offered via the Internet, i.e. private customer business, but in the USA there is clear evidence that this medium is becoming increasingly important for the placement of more sophisticated commercial and even industrial business. A role that is not to be underrated is also played by the major brokers, who are using the Internet more and more both for registering risk information and making the first contact with the client, and for placing risks in the insurance market.

However, with the growing importance, which the medium is acquiring as a marketing channel for the value-added chain of companies, the susceptibility of companies to Internet-specific liability risks is also increasing. Furthermore, the minute companies open themselves to the outside, they enter a global marketplace whose rules are largely characterized by traditional, territorial rights and responsibilities and are therefore multi-facetted. The growth chances that might arise, as a result of a skilful sales strategy on the Internet is thus to be weighed against the risks which must be recognized and whose implications for the corporate results must remain under control. From the insurers point of view, the challenges are twofold: on the one hand, it will be essential to identify the companys own growth and result potential and utilize it to the full. On the other hand, the risk situation of the companies operating through the Internet must be analyzed, the risk transfer requirements assessed and - if the existing range of products does not suffice - a suitable new product developed. Most of the risks emanating from the Internet is directly connected with its structure and the way it works. The Internet is not a single, specific network, but rather the link between numerous networks and servers, which, irrespective of hardware and operating systems, use a common, defined transmission standard (the so-called TCP/IP protocol). Data, which a user would like to send via the Internet, is split into several (packages) by the Internet program. By means of the TCP/IP protocol these data packages are furnished with details of the addressee, the sender, the total quantity and the order of all the packages belonging to the message. The individual packages are then forwarded on by every router (computers which control the transmission of data between different networks) at which they arrive. In this connection, the (route of the individual package essentially depends on the available line capacities. In this way the individual data can arrive at their objective via different routers. Thus, in contrast to a telephone conversation or a telefax, it is not necessarily a defined transmission path, which is used. Although, originally, the Internet was very much designed with security in mind - namely, so as to safeguard communications between computers even in the event of a nuclear attack on the United States, the further technical development of the medium has been turbulent and uncontrolled. Past malfunctions may permit the conclusion to be drawn that with the growing complexity of network technology on the one hand and

rising commercial utilization on the other the imponderables of network failures will also increase. Some past losses illustrate this problem:

In November 1997 the American domain name administrator Network Solutions fed two files with erroneous domain names into the network. 1.3 million Internet addresses with the top level domain endings (coin) and (net) could not be reached in large sections of the network for hours on end.

- In April 1998, due to a software error, the network of AT&T in Basking Ridge collapsed for twenty hours, cutting off about 6,600 business clients from the network. The breakdown of a sub network had direct consequences for those users located within the networks dial-in area. Presumably, the cause was a maintenance command, which generated a flood of routing messages, paralyzing the network in the process.
- In Germany in August 1998, a fire at a central telephone exchange of the Telekom cut off around 50,000 lines for several days. Claims for damages snowed in, due above all to the loss of profits suffered by companies dependent on telephone and online sales. It is assumed that the Telekoms total loss adds up to millions of German marks.
- A survey conducted in Germany by the Cologne Re in May 1998 revealed that technical interruptions had occurred at approximately 30% of Internet service providers.

The Internet is particularly sensitive to the breakdown of high-performance lines, so-called backbone systems. Technical problems are pre-programmed if a high volume of data, which has previously been processed via these (data highways), has to be processed at the same speed via the (country roads) of the secondary networks. A marked change in transmission speed, causing network overload and failures associated with such overload, can slow down or render impossible vital business transactions and have disastrous financial consequences for the suppliers of such services. Online banks mail order companies and all businesses whose added value is heavily dependent on correct data transmission are the direct victims of such technical failures.

Additional risks result from passwords or other sensitive data being intercepted in the network during transmission. It is conceivable that the sender of a message could thus incur a loss and subsequently lodge a claim against the developer or operator of the encryption software. Finally, in the purely technical sector a risk exists in that the interface between the internal EDP world of a company and the Internet is not adequately safeguarded by so-called (firewalls). Through such gaps outsiders can often gain access to sensitive information on the company itself, its business partners or even private clients. A number of topical incident show just how explosive this subject is:

- In October 1998 Microsoft admitted that the Internet Explorer granted access hard disks by a few JavaScript command soft was thus reaction responding information around the Internet by an expert in computer technology. Netscape had also previously admitted the existence java similar security gaps.
- In March 1998, in America, unknown hackers sabotaged innumerable computers installed at government agencies and I universities. The attackers used the Internet to invade computers with the operating system Windows NT, where, by depositing an insoluble problem, they overburdened the memory and caused the system to crash.
- In the summer of 1996, the server of the access provider Public Access Networks Corporation, which at the time supplied around 1,000 commercial websites, was virtually made to crash by hackers when it was bombarded for hours with requests for information. The server was down from Friday till the following Monday. As the principal shareholder and cofounder, Alexis Rosen, said:

(If things go on like this, we could be banker week). It was only solve the problem hackers temper attacking.

- In April 1998 a 16-year-old schoolboy in Germany cracked the access code for the online services provided by the Telekom and its rival, AOL, with the help of a spy program, a so-called (Trojan Horse).
- In March 1998 in Switzerland, a bank customer was granted access to another customers bank statements because the Internet bank offered only a limited number of dial-in windows and the customer

33% of Internet service providers stated that they had already been the victims of at least one incident of hacker intrusion. As opposed to the frequently voiced opinion that most attacks are harmless and without any serious effects, the study showed that the destruction of data can, in practice, have a very serious economic impact. Last but not least, media risks and personal injury need to be addressed.

These risks are of a non technical nature and materialize if third-party rights or objects of violated by caption of texts, pictures, music, etc. The nature of media risks is similar to the insurance of newspapers/ periodicals or advertising agencies. However, the pressure for ever faster reporting and providing of content is intensifying as a result of the Internet, a development which can lead to errors in the researching or processing of information. In addition, the global nature of the Internet represents an increase of risk, which remains hard to determine at this point. Whereas the risk can be geographically limited in the case of print media through circulation, language, and distribution channels, the global retrievability and accessibility (and replicability) of a web site means an uncontrollable opening towards the outside. The situation is aggravated by the increasing use of so-called links, which refer to the web pages of other providers and other sources of information, It is not yet clear to what extent a provider of a home page who inserts a link to another web site can be held responsible for the contents of the other site. In this field, a whole row of prickly, unsolved legal questions arise, such as
What law is applicable, or which court has jurisdiction.

A loss may also be caused by false information, e.g. if the reader of a stock exchange online service makes wrong investment choices because of misleading information, or if someones health suffers as a result of advice published on the Internet.
One risk that is often underrated is that e-mail actually intended only for internal corporate purposes might filter through to the outside and cause major damage to the company, as the following two cases demonstrate:

- In 1995, Norwich Union employees circulated e-mail with-

In the company reporting about alleged financial difficulties of the rival Western Provident Association, which found its way outside some time later, causing the rival company to sue for slander. In July 1998, Norwich Union was fined
450,000 pounds sterling

- In October 1997, a manager of The Hungarian Postabank mass-distributed an e-mail to customers asking them to close their accounts because the bank was, according to him, in financial trouble. It was only thanks to the rapid intervention of the Hungarian government and the owners that the bank was saved from subsequent bankruptcy.

As we have seen, a large number of parties associated with the Internet are exposed to liability risks, which are either of an entirely new nature or, in a quantitative sense, greatly magnified. From an insurance point of view, it must be noted that the existing legal uncertainties will, above all, become manifest in considerably higher legal defense costs, which, in cases where corresponding liability covers have been taken out, will ultimately be borne by insurers.
This gives rise to the question of whether the described risks are included in and covered by existing insurance concepts, or whether there is a need for an extension of current products or even entirely new insurance products.

There is no universal answer to this question, as there is no worldwide standard for liability insurance policies. Yet it is important to note that losses incurred by Internet risks are first and foremost pecuniary losses, rather than bodily injuries or property damage. This often means that these losses are either excluded from standard employers liability and product liability policies, or are at least restricted by a sub-limit for pure financial loss.
In many cases, liability claims resulting from the violation of intellectual property rights and copyrights are a standard exclusion and therefore not covered unless re-introduced via a separate insurance clause. Whereas gaps in coverage are thus likely to emerge in the normal employers liability and product liability policies of industrial enterprises, the situation is different when it comes to the third party liability policies of the IT companies involved. Here, as a rule, financial loss is covered. In many scenarios, software developers, hardware manufacturers, IT service providers or network providers will be exposed to claims for damages either directly or by way of subrogation. Under many policies, however, claims resulting from computer virus damage, defect of title or malfunctioning firewalls are excluded. Also, the limits of indemnity still tend to be relatively low. Newspapers, magazines and marketing agencies are normally armed with comprehensive insurance protection for Internet risks. With regard to the print media, it is important to note whether foreign claims are excluded or not. In the case of advertising agencies, defects arising from the technical performance of contracts are frequently excluded. This creates a gap in coverage when the advertising agency itself carries out part or all of the programming of a website on behalf of a client.

Finally, it cannot be ruled out that this risk may add to the exposure of D&O policies as well. If a company is particularly vulnerable to risk through its presence on the Internet, its directors are obliged to take suitable risk management measures.
In view of the growing importance of the Internet as a sales channel, insurers must include the risk situation arising from this exposure in their underwriting considerations at an early stage. In sum, an analysis of current coverage concepts shows that neither policyholders nor insurers
Are fully aware of the exposure stemming from the The result will be gaps in coverage, insufficient limits of indemnity or the inadvertent coverage of claims and ensuing defense costs for insurers.

In the end, the technical and legal risks of transactions over the Internet will lead to growing demand among those liable for comprehensive insurance protection. It is up to the insurance industry to face this challenge and both design and market its products in line with the requirements it anticipates.