

INTERNATIONAL ASSOCIATION OF INSURANCE SUPERVISORS



RISKS TO INSURERS POSED BY ELECTRONIC COMMERCE

OCTOBER 2002

Risks to Insurers posed by Electronic Commerce

The expansion of electronic commerce, especially via the internet, results in important new challenges for the regulation and supervision of insurance. To ensure that the insurance consumer is protected, supervisors must:

- identify the risks posed by electronic commerce;
- ensure that these risks are being well managed; and
- develop appropriate supervisory strategies.

This paper focuses on the first point – the identification of risks. It is expected that supervisors will use this information, and subsequent papers describing how the risks can best be managed, when monitoring and inspecting companies that use electronic distribution channels for product sales. The scope of the paper includes information given by the insurance companies about their products, coverage provided and the servicing of contracts and claims handling.

Contents

Background	3
Strategic Risks	4
Operational Risks.....	6
Transaction Risks.....	7
Data Security risks	8
Connectivity risks.....	9
Conduct of Business Risks.....	9

Background

1. The internet was originally used as a channel for data transmission. It offered – especially universities and research institutes – a fast and efficient means of communication. During the last few years, the internet has developed into a commercial environment. Use of the internet in business-to-business commerce is growing very fast; firms are also developing strategies for business-to-consumer commerce. Already, through the internet, an insurance consumer can:

- obtain information about insurance products and insurance coverage;
- perform product comparisons;
- apply for, and in some cases conclude, an insurance contract; and
- have contracts serviced and claims handled.

2. The internet provides a system that is both efficient and constantly available. Through it, companies can market and provide information to more people in more locations. They can use the

internet to service customers after insurance contracts have been drawn up. Also the ability to review policyholder account details and make electronic payments online, could potentially prevent cancellations. At the same time it may save costs, which could result in lower premiums for consumers in the long term. However the cost of implementing the new technology is significant.

3. Nevertheless companies should be conscious of the strategic risks associated with an internet strategy. Strategic risks are critical and are discussed in more detail below. As time goes by, new insurance products designed specifically for sale on the internet will be developed and competition will intensify.

4. In addition, while some insurers may be using existing lines - such as business interruption - to cover the risks posed by e-commerce, new underwriting opportunities will undoubtedly arise. In fact, some insurers now specialise in underwriting internet operations, including hacking risk. There are many other known and yet-to-be-identified risks for which products could be developed, including the risks in settling claims across borders or the risk of data not being properly protected. In certain cases these new underwriting possibilities may lead to long-tailed risks.

5. Commerce carried out on the internet relies on the support of a solid technological framework. Processing and transferring information is accomplished at great speed. Data security must be assured and systems must be in place to identify computer viruses. The cost of properly implementing this technology is great. Companies need to build or acquire the appropriate hardware and software; some companies do this by outsourcing. Reliance on outsourcing leads to other risks.

6. The internet raises many legal questions. Some, from a supervisory perspective, are critical; for example which country's legislation should apply and which supervisory authority has jurisdiction. Consumers' identities can be difficult to authenticate over the internet. This increases the opportunity for criminal activity, such as money laundering and insurance fraud. Concerns about computer hacking can take on new dimensions.

7. This paper discusses risks posed by electronic commerce that are new or different in scale or impact from traditional business conducted through other distribution channels. Insurers reputations are at stake, especially because in this electronic age errors can multiply and spread quickly. Insurance supervisors will want to be assured that these risks are being properly identified and addressed within each company depending on their level of involvement in electronic commerce.

Strategic Risks

8. Strategic risks arise when a company, engaging in a new business strategy, does not think through the implications that the decision on electronic commerce will have on other parts of the organisation or the company as a whole. Without a clearly thought out and all encompassing strategic plan, the risk of mistakes occurring increases and the chances of the strategy succeeding decrease.

9. Entry into electronic commerce may be a result of customer or marketplace demand on the insurer. Most insurers are engaged in e-commerce in some form, in large part due to the increasingly important role that e-commerce and the internet have on the global economy. Competitive insurance

companies are forced in this regard to utilize e-commerce in some way or lose their competitive edge.

10. The decision to engage in electronic commerce requires a precise analysis. For example, when the board of directors of a company and executive management make the decision to engage in electronic commerce, they must consider:

- what are the distinctive features of electronic commerce and what are the associated operational risks;
- how electronic commerce fits with the strategic orientation and the priorities of the company and how it helps achieve those;
- whether electronic commerce fits the company's image;
- who will be the target group for this channel of distribution and will new products have to be designed to meet any specific needs of this target group (and which markets will be excluded);
- what will be the effect on consumer satisfaction;
- what implications will this new distribution channel have on traditional business – can they co-exist or be combined; what savings will result; will the business be profitable;
- whether to develop strategic alliance on the internet;
- whether to use portals to group insurance products; and
- what information will be supplied to the consumer.

11. This list is not exhaustive and the impact on the solvency of the company should be the overarching consideration in the analysis. The solvency impact may well be prohibitive. In addition, the company should be wary that:

- the global nature and rapid development and growth of electronic commerce will put pressure on its planning and implementation of online-operations, in particular, product design and technological applications;
- while the internet may be an efficient way of conducting insurance business, it is far from cost free. In addition to systems costs, establishing and maintaining customer awareness of the website may involve significant advertising costs;
- brand loyalty may evaporate in the face of price competition, and a significant number of consumers – particularly in the case of personal lines – may move their business between insurers. Furthermore, there is the potential that sales will decrease because of the absence of personal contact;
- aiming for savings in distribution costs through online commerce, may result in some customers being neglected, particularly those not used to these new sales channels. Also if the focus is on savings, necessary investments in research, product innovation, data security and risk management might be neglected;

- increased global competition can narrow profits. Increased competition may arise from new entrants to the market linking insurance sales to the provision of other internet services, notably electronic banking;
- while internet technology enables a greater amount of speed in the processing and transfer of information, it complicates the management of information; and
- increased speed and number of policyholders can increase traditional insurance risks, for example, it could increase incidents of adverse selection or inadequate disclosure by consumers.

12. The internet provides enhanced opportunities for companies to operate in new geographical or product markets. In pursuing these opportunities it is important that the management of a company appreciates the nature of new risks they may be assuming, and – where services are provided on a cross-border basis – has assessed the legal and insurance environment in which they are conducting business. New markets will require careful planning prior to entrance. The drain on resources will be considerable and pressure for quick profits may lead to unwarranted risks.

13. The board of directors and management need to choose strategies that reflect the company's desired risk profile, functional capabilities and solvency. It must decide how its internet strategy will influence the company's philosophy, the way it conducts business, and its financial situation. Without a well thought out strategy, the decision to engage in electronic commerce may result in an unwarranted increase in risks at the operational level and an unproductive drain on resources.

Operational Risks

14. Operational risks in an electronic commerce environment relate to risks that arise as a result of a failure or default in the information technology infrastructure. An insurance company is prone to operational risks when the application and use of internet technology is not well managed. The need for know-how and expertise is crucial in this area.

15. An insurers' information technology infrastructure can be deficient in many ways. For example, it may not:

- have the capacity to handle increased traffic and process transaction volumes;
- be scalable (i.e. have the ability to expand or scale down);
- be accessible at all times due to a lack of fault tolerant technology;
- be secure from internal and external disruption; or
- be accessible, compatible, or interoperable in every market.

16. Increasingly, as electronic commerce expands, companies are outsourcing all, or part, of their information technology operations. Third party providers are being used to:

- develop websites;
- develop insurance-related internet applications; and
- manage the information technology infrastructure (i.e., hosting servers).

17. These activities require insurers to have appropriate policies and controls in place to deal with areas, such as, procurement, contract negotiation and specification, and contract management. In addition, they need to be able to assess the service provider's operational viability, financial liquidity and project management skills.

18. Skilled information technology and project management specialists are also necessary for delivering insurance-related internet solutions. Companies need skilled staff – in particular skilled resources at their call centres – to support the business processes used by internet consumers. The increase in demand and continued restricted supply of skilled personnel will lead to increased costs.

Transaction Risks

19. A transaction risk is considered to be the risk of any unauthorised alteration or modification to texts, information or data transmitted over computer networks between an insurer and its client, or vice versa. Transaction risk can arise both through electronic commerce on-line and off-line through traditional communication mechanisms. Transaction risk arises in electronic commerce where the source and responsibility for the problem lies in the technology (e.g., with the technological server that receives and sends on data), and not with the insurer or the client. This transaction risk also includes information which is hosted on the server or website of a “partner” third party (such as an agent).

20. The terms of an insurance contract must be invariable for the parties to it. When marketing insurance over the internet, companies must be able to guarantee that, once agreed to, the terms of the insurance contract will not change, unless, of course, there is mutual consent or an agreed process.

21. Companies must have sufficiently reliable technical resources to guarantee the integrity of the information and data transmitted over the web. If not, and consumers perceive this risk, the development of internet insurance marketing will, in the most optimistic scenario, be slowed.

22. Both parties need to be assured that they will receive all information and data transmitted by the other party in a timely manner. Timeliness is particularly important because the payment of the claim will be in accordance with the terms of the contract in force at the time the insurable event occurred. Both parties must have agreed to and have the same information regarding the terms of the contract and subsequent amendments.

23. Consequences or examples of transaction risk arising from faulty information or flaws in the system are:

- the insurance company is not able to offer its customers certain insurance products;
- the insurance company offers its customers an insurance product that does not correspond with the customer's specifications;
- the insurance contract entered into through internet is not clear, possibly missing some standard clauses;
- an electronic signature is not recognised;
- the company's internet platform is used fraudulently or for criminal purposes; and
- customers may dispute the validity of or refuse to acknowledge legitimate communications and transactions¹

24. Transaction risks are closely related to the data security risks and legal risks of insurance companies. If uncontrolled they can damage both the marketing image of the insurance company and its reputation more generally, particularly when legal conflicts arise between the company and the policyholders.

Data Security Risks

25. Because electronic commerce relies on extensive technological applications and networks, data security risks are significant. Data security risks are considered to be the risks of losses, unintentional changes or leaks of information or data in computer systems.

26. Data security risks in electronic commerce in insurance services can be grouped into two main categories. First, a data security risk is identified within the system of an insurance company. This could be caused by technical flaws, such as, the incompatibility of the data systems or parts of the system, information leaks, or information loss. Data security risks may also be caused by errors in external links to the systems.

27. Data security risk also arises from intentional or negligent external data breaks. In these cases, for instance, a customer's personal data could be accessed illegally by, for example, 'hacking',² 'sniffing',³ or denial of service attacks.⁴

28. Such security risks may cause problems in identifying external and internal users of the system. They complicate, and in some cases negate, the company's ability to authenticate information and data. Information concerning, for example, an insurance contract may be changed

¹ This point subsequently added per Working Group on E-Commerce meeting 16 July 2003

² Usually the practice of breaking into the system without authorisation.

³ Usually the use of software programs that are illegally inserted on the net to capture user passwords as they are being used in the system.

⁴ Overwhelming a server with such a large number of requests that it will not be able to proceed with ordinary requests and the system may fail.

within the system without authorisation after the system has been broken into. In these cases, not only relations with the individual customer, but also more extensively the reputation of the insurance company, will suffer. Because of the scope of internet technology applications and their many effects, an insurance company must take data security risks into account when preparing its operational and strategic plans. Several different security levels may be necessary to minimise data security risks.

Connectivity risks

29. Connectivity risk is the risk that a failure in one part of the system may impact all or other parts of the system.⁵ It is particularly acute in an electronic commerce environment because the underlying systems are extensive and process data (and, potentially, problems) rapidly. If any part of the internet's operational system is damaged or modified as a result of negligent or intentional actions, the effects on an insurer's systems can be devastating. For example, the insurance company may fail to provide service to clients who have bought insurance contracts over the internet; eventually this will impact their reputation.

30. There are a number of measures companies can implement, such as contingency, recovery and disaster planning and establishing back-up facilities, to minimise these risks. However, many of these measures are complex and need to be executed with care.

Conduct of Business Risks

31. Insurance laws and regulations, particularly with respect to conduct of business issues, have been developed with the view that business will be conducted on a person to person basis, with paper documentation. Electronic commerce poses many new issues with attendant risks, such as:

- authenticating the identity of the customer;
- verifying and maintaining the security of electronic documents and signatures;
- assuring electronic notification of contract-related information treats the interests of the insurance company and the client fully and fairly;
- ensuring that the format and style of presentation, which may need to be altered to be transacted electronically, meets requirements for disclosures and disclaimers;
- providing the policyholder with a proof of coverage that is acceptable to regulators or other third parties;
- accepting electronic payments in lieu of cheques, drafts and cash; and

⁵ An example of connectivity risk is this incident that occurred recently in a securities company. The main frame got soaked due to leakage in the sprinkler system, which resulted in breakdown of LAN, Internet connection and electronic trading service systems. As a result, both online and offline trading services had to be suspended. It took them 5 days to restore their systems back to normal.

- meeting records retention requirements through electronic means, including personal information protection measures.

32. In addition, many jurisdictional questions arise because on the internet business is conducted “virtually” and across many borders. As a result, insurance companies may face the reputation, legal and other risks caused by the problems that insurance consumers will have regarding jurisdictional questions. Insurance consumers or supervisors may have problems in determining:

- if an undertaking that is active on the internet has a legitimate right to provide insurance services – for example, is the company or an agent licensed to sell insurance;
- the location of company and, therefore, whether, by whom and how it is supervised;
- what legislation would be applied to insurance products offered;
- whether consumer redress in the event of a dispute is available and, if so, on what terms; and
- what legal measures can be taken against a company in another jurisdiction.

33. Full disclosure to the consumer is essential. The insurance company providing service over the internet must as a minimum give consumers information about who they are and who has licensed them to operate. In addition, they must clearly describe the characteristics of the products that they offer.

34. Insurance customers may not be aware of the risks they face in conducting business on the internet until a problem arises and this may be too late for a supervisor charged with policyholder protection to act effectively. Further guidance in this respect is contained in ‘IAIS Principles on the Supervision of Insurance Activities on the Internet’.