IMIA – WGP12(00)

**Paper presented at the IMIA Conference in Munich
September 2000**

The Internet and Intranet, Exposures and Insurable Interest

Working Group:
Ing. Mag. Paul Moritz, UNIQA, Wien
Jan F Th. Boogaard, Paevenio, Amsterdam
Anders Lindberg, If..., Stockholm with assistance of David Lindqvist
Chris Blückert, Zurich, Stockholm with assistance of Philippe Tamwelius

Presented by Chris Blückert and Guest Speaker Philippe Tamwelius

Table of Contents

The Internet and Intranet, Exposures and Insurable Interest

What is the history of the Internet?

1969 – The Department of Defence Advanced Research Projects Agency (ARPA) in the United States creates an experimental network called ARPANET. This network provides a test-bed for emerging network technologies. ARPANET originally connected four universities and enabled scientists to share information and resources across long distances. ARPANET continued to expand, connecting many more sites throughout the 1970`s and 1980`s.

1972/1973 – The National Centre for Supercomputing Applications (NCSA) develops the telnet application for remote login, making it easier to connect to a remote computer. FTP (file transfer protocol) is introduced, standardising the transfer of files between networked computers.

1982/1983 – The TCP/IP suite of networking protocols, or rules, becomes the only set of protocols used on the ARPANET. This decision sets a standard for other networks, and generates the use of the term “Internet” as the network of networks which either use the TCP/IP protocols or are able to interact with TCP/IP networks. To keep military and non-military network sites separate, the ARPANET splits into two networks: ARPANET and MILNET.
In 1982 and 1983, the first desktop computers begin to appear. Many are equipped with an operating system called Berkeley UNIX, which includes networking software. This allows for relatively easy connection to the Internet using telnet. The personal computer revolution continues through the eighties, making access to computer resources and networked information increasingly available to the general public.

1985/1986 – The National Science Foundation (NSF) connects the United States six supercomputing centre together. This network is called the NSFNET, or NSFNET backbone. To expand access to the Internet, the NSF supported the development of regional networks, which were the connected to the NSFNET backbone. In addition, the NSF supported institutions, such as universities, in their efforts to connect to the regional networks.

1987/1989 – The NSF awards a grant to Merit Network, Inc. to operate and manage future development of the NSFNET backbone. Merit Network, Inc. collaborates with International Business Machines (IBM) Corporation and MCI Telecommunications Corporation to research and develop faster networking technologies. The backbone is upgraded to “T1” which means that it is able to transmit data at speeds of 1.5 million bits of data per second, or about 50 pages of text per second.

1990-1993 – The ARPANET is dissolved. Gopher is developed at the University of Minnesota. Gopher provides a hierarchical, menu-based method for providing and locating information on the Internet. This tool makes using the Internet much easier. The European Laboratory for Particle Physics in Switzerland (CERN) releases the World Wide Web (WWW), developed by Tim Berners-Lee. The WWW uses hypertext transfer protocol (HTTP) and hypertext links, changing the way information can be organised, presented and accessed on the Internet.

1993 – 1995 – The NSFNET backbone network is upgraded to “T3” which means that it is able to transmit data at speeds of 45 million bits of data per second, or about 1400 pages of text per second. The graphical web browsers Mosaic and Netscape Navigator are introduced and spread through the Internet community. Due to their intuitive nature and graphical interface, these browsers make the WWW and the Internet more appealing to the general public. The NSFNET backbone is replaced 1995 by a new network architecture, called vBNS (very high speed backbone network system) that utilises Network Service Providers, regional networks and Network Access Points (NAPs).

In Summary: The Internet has evolved through a series of advancements in networking and computer technologies. From its beginning in 1969, the ARPANET provided a test-bed for networking research and development. An important development that grew out of ARPANET was the TCP/IP protocols, which provided standard rules for networked computers to communicate with each other. Other significant events included the introduction of the desktop computer, the development of networking tools such as telnet, FTP, gopher and WWW, and the release of graphical browsers. Advancements in networking enabled the NSFNET to upgrade its speed several times, allowing more and more connections.

E-Commerce

This document provides brief information and analysis of e-commerce and exposures due to e-commerce activities.

To understand why this technology affects us as much as it does, it is best to start with some historical numbers. It took radio 38 years to reach 50 million people; TV took 13 years and cable TV took 10 years to reach 50 million people. In the six years since the birth of the World Wide Web, more than 214 million people are on-line every day. This number is growing rapidly. To say that the Internet is the future is wrong – the Internet is absolutely the technology of today. In the future, the Internet will probably be an important part of our life and a matter of course, like the TV is today.

Several independent analyses of the Internet including e-commerce have resulted in almost the same conclusion: **The Internet is one of the biggest and most interesting technology-based revolutions that has ever happened in the world.**

It is important to remember that human hands construct the Internet and it is made to make our lives easier. Today web technology is not so user-friendly, but in the near future this will change so that it will be possible to access information from the Internet without being a computer-person. The technology will most likely move into our living-rooms and be accessed via the TV. It is of course more interesting to surf the Internet on the sofa instead of sitting in front of a computer in a workroom.

What is e-commerce?

Since the Internet and e-commerce derive from the USA, here is a definition of what e-commerce is:

"Electronic Commerce is defined as doing business electronically. This includes the sharing of structured or unstructured business information by any means (such as electronic mail or messaging, World Wide Web technology, electronic bulletin boards, smart cards, electronic funds transfers, and electronic data interchange) among suppliers, customers, government bodies, and other partners in order to conduct and execute transactions in business, administrative and consumer activities."

This definition of e-commerce was adopted in December 1997 by the United Nations Centre for Facilitation of Procedures and Practices for Acquisition, Commerce and Transport. The European Community has also adopted this definition.

The interesting thing about this definition is that it says that e-commerce is much more than having a website. Normally, becoming a part of the e-commerce sector often starts with having a website. But e-commerce includes other technologies as well, for example RAS servers, the old BBS technology, and the new WAP technology.

E-commerce is divided into two parts: Business to Business (B2B) and Business to Customers (B2C). An example of B2B is a company that communicates and does business with its subcontractors via e-mail and over the Internet. An example of B2C is a private person ordering a book or CD from a company over the Internet.

It is expected that in 2000, B2B will generate more than USD 1 billion and B2C more than USD 500 million. It follows that B2B is clearly the larger of the two activities and the fastest growing industry on the Internet.

Intellectual property?

A company's intellectual property could include all kind of trademarks and copyrights, trade names, mask works, trade secrets, know-how and confidential or proprietary business information (including ideas, research and development, formulas, compositions, manufacturing and production processes and techniques, technical data, designs, drawings, specifications, customer and supplier lists, pricing and cost information and business and marketing plans and proposals), software (including data and related documentation), all other proprietary rights, all copies and tangible embodiments thereof (in whatever form or medium), and all rights under any leases, licenses, franchises, permits, authorizations, agreements (including secrecy, non-disclosure, and work-product assignment agreements) and arrangements with respect to such assets.

What kinds of risks exist for e-commerce companies?

A few examples:

E-mail.

Sending e-mails is not a secure way of sending information: roughly 90% of all e-mails pass an Internet server in the USA before reaching their final destination. To read someone else's mail is, according to hackers, a very easy thing to do. This kind of hacking has many names, among them "Mail-Sniffing". We must therefore take much more care when sending e-mails with sensitive information. This will change so as to be better and more secure in the future, but it doesn't seem to be a very high priority on the developers' list.

WAP, Mobile Internet, "Always Online".

Mobile Internet is, in my opinion, the second IT revolution. The rather slow but functional WAP technology has been a very hot topic during the past year. The security of WAP technology has been a disaster because the technology has had problems with implementing to normal Internet-related firewall technology. Even though not secure, the use of mobile technology is growing rapidly. One of the most important things to realize is that the technology is here and that it will be more and more important in the future. The concept "Always Online" is being developed by Ericsson and means that your mobile phone will be ready to access e-mails, Internet information and similar information just like the SMS technology works today, i.e. it will not be important to find a computer to access the Internet –

you will be able to do so directly from your mobile phone and/or handheld computer. Blue Tooth technology will soon be included in your mobile phone and this will make communication between the phone and your handheld computer or similar equipment much easier and more secure.

Employees’ Internet Access.

Providing employees with access to the Internet is normal practice in many companies today. There is a lot of information on the Internet that can be used in companies. This information is usually free to read and to use, but one must remember that someone has done the information input and that up to 95% is someone else’s property. You are allowed to read the information on the Internet and sometimes to copy it to your own computer, but you are not always allowed to use it, for example, in your own advertising. The perils connected with employees having access to the Internet include sending and receiving e-mails, sending and receiving files and similar information/files, and using the Internet. The exposure for a company could be theft of intellectual property, online chatting, and distribution of information about the company that is not public, gossip and slander, and negative publicity for the company.

Website.

Why does a company have its own website? Normally there are two reasons. One is to inform others of the company and to market its activities. The other reason is to promote active e-commerce with clients and other companies. Having your own website or a website in co-operation with others shows that you exist, which is very important for a company wanting to do well in business. The perils of having your own website may include the risk of providing incorrect information, viruses, hackers and denial of access. The potential exposure of incurring a third party claim stems from the possibility that someone has relied on incorrect information provided by you and as a result has made an unwise or incorrect decision The site can be infected by viruses and thereby also infect visitors’ computer systems. A third potential problem could be problems with access for clients and customers. If the site is free and the information is public, the risk of a third party claim should be fairly low. If, on the other hand, a client has signed an agreement with a company saying that the company will provide the client with information and the client is denied access to the system, this is much more likely to result in a third party claim.

Split of Network.

This is another interesting way of doing business. There are a few different definitions of this kind of co-operation-based relationship. When, for example, a merger is conducted between two companies, they would of course like to put their websites together so that different clients can find information about the new company. To merge two companies and their different IT systems is, naturally, a hard nut to crack, but the market has seen several examples of successful merging, as in the case of Ford-Volvo.

Hacker.

What is a hacker?

The actual definition of a hacker can be divided into several sub-definitions; for example cracker, swifter, sniffer, script-kiddies, lamer kid etc. The common denominator in these definitions is that they consist of people who want either to steal information from a company's databases, to destroy a company's databases or simply to see how far they can go in accessing other companies' networks or computers via their own computer. The Internet contains hundreds of "hacker sites" where hackers can exchange information. This information and software exchange can, under the current regulations, be wide open for the public. The normal definition of a professional hacker is a "Cracker". This person constructs his/her own "hacking-software" to make it possible to hack into a company's system. Furthermore, a Cracker is a person who performs the hacking on a commission basis, i.e. there are clients in the background who order these kinds of job.

Sniffer

Another sort of a hacker is a "Sniffer", who shadow-connects to the Internet directly via another person's connection. The Sniffer can then see exactly what the "sniffed" person does, for example encrypted passwords, e-mail information etc. This kind of fraud is very difficult to discover and also to prove, since it's not possible to see where/how the Sniffer came into the account or how he received access to sensitive information in an e-mail. The problem with Sniffers can entail repudiation cases.

"The good guy"

A hacker can also do good things, such as assisting software companies with information about bugs, programming errors or similar defects in their software. Many large software companies have been assisted by hackers in their development of new software and in finding latent programming errors.

"The bad guy"

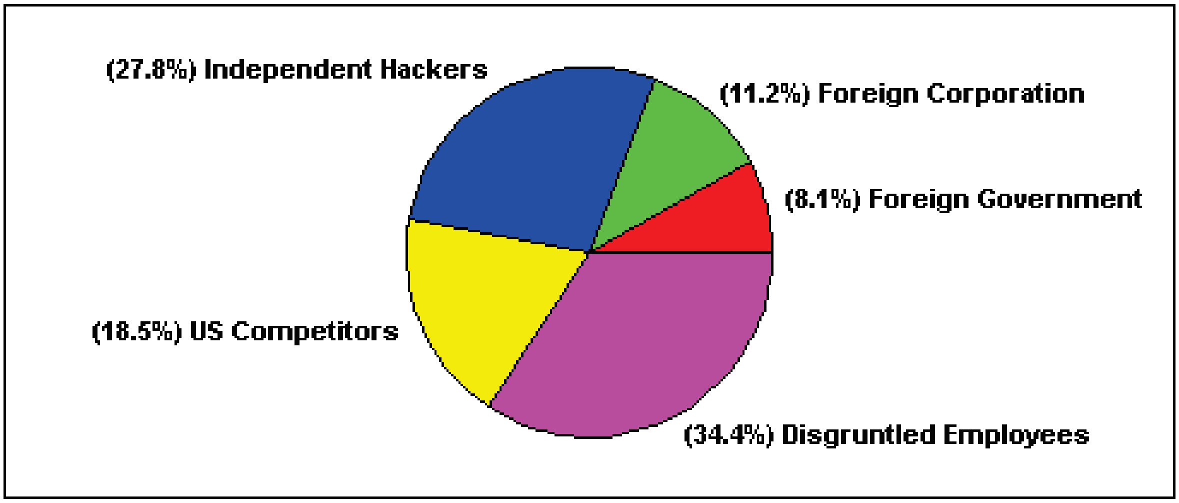
Professional international hackers can, without much difficulty, gain access to a company's system, make a copy of the company's database and sell it to a competitor. It is very important to know and to understand that a market for stolen Intellectual Property exists and is undoubtedly going to increase in the future. A hacker can also be a disgruntled employee or an employee wanting to earn some easy money. In fact most damage due to hackers comes from disgruntled employees, as shown below.

Social engineering

This is a growing problem for most companies. An example of social engineering is if someone contacts an employee of a company under the false pretence that he will upgrade the employee’s software, and in the process obtains the employee’s user ID and password. In about 70% of all these cases, the contacted people will give away their passwords and user IDs.
Why? Probably because most companies don’t have any documented policy or IT security plan for their employees.

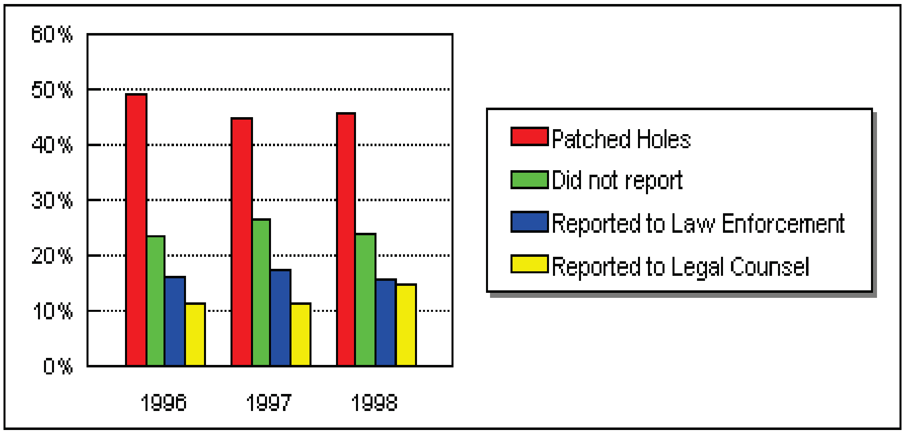
Who performs an attack?

A US-based study shows that over 30% of illegal intrusions in networks and computer systems are made by disgruntled employees. One explanation for this fact is that employees have easy access to their company's computer system and to sensitive information.



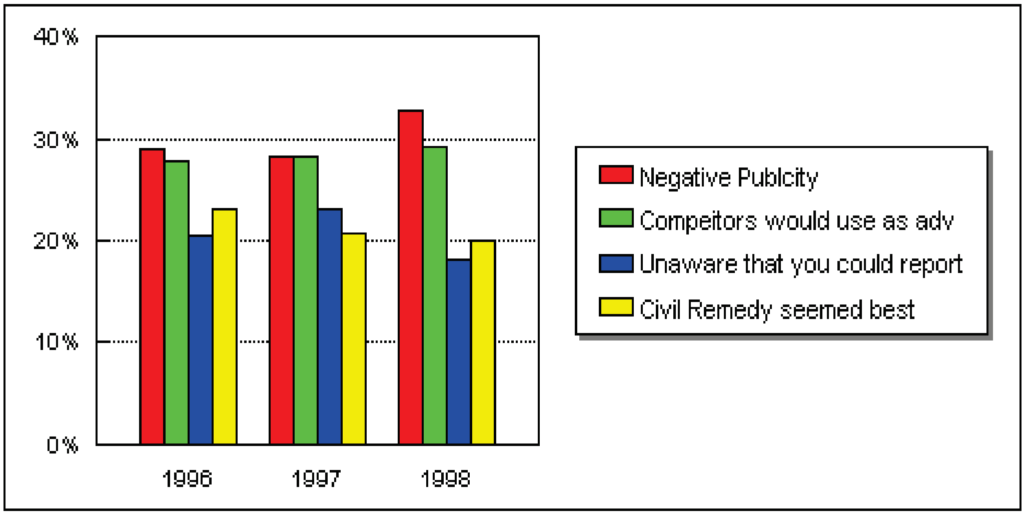
Since a market for stolen Intellectual Property exists and is growing every day, the professional attacks are probably going to be a big threat for companies in the future. It is possible to order a copy of, for example, a competitor's client list. This information can be worth ten times more to the company that orders the information than to what they pay the hacker. The hacker will nevertheless receive a relatively high payment for a quick job.

What actions are taken after an attack?



It is interesting to note that in 50% of the cases where companies have been subject to intrusions, they only patch up the hole or the holes, i.e. find out how the hacker entered and then fix the hole in the firewall. In 25% of the cases, they didn't report that they had had the intrusion, in some cases not even to the management of the company. In 15% of the cases, they did report the attack to the law enforcement and in 10% of the cases they did report it to the legal counsel of the company.

Why wasn't the attack reported?

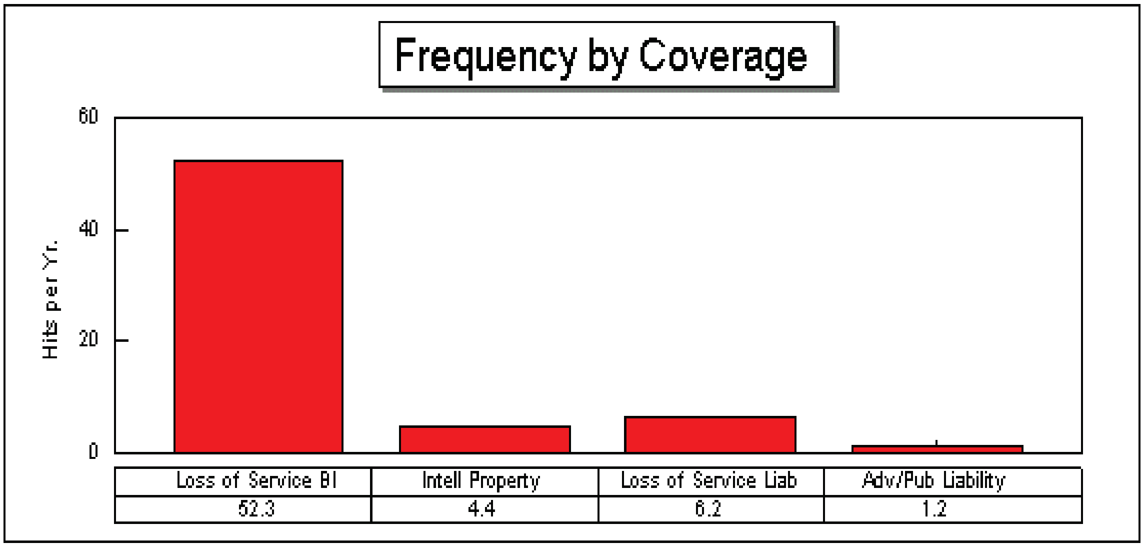


Negative publicity and fear of competitors using the attack to their advantage in marketing are the two main explanations why attacks are not always reported. No company wants negative publicity because of its lack of security, and furthermore companies do not always know that intrusions and attacks should be reported, or to whom the incident should be reported. This is a European problem, where the police have not been very informative about how they handle applications.

Conclusion:
Hacking and similar fraud will in the future be part of a company's ordinary day. Hackers will be increasingly professional, with better software and better instruments. If a hacker really wants to enter a company's computer system, he will be successful in over 90% of cases.

Claims analysis

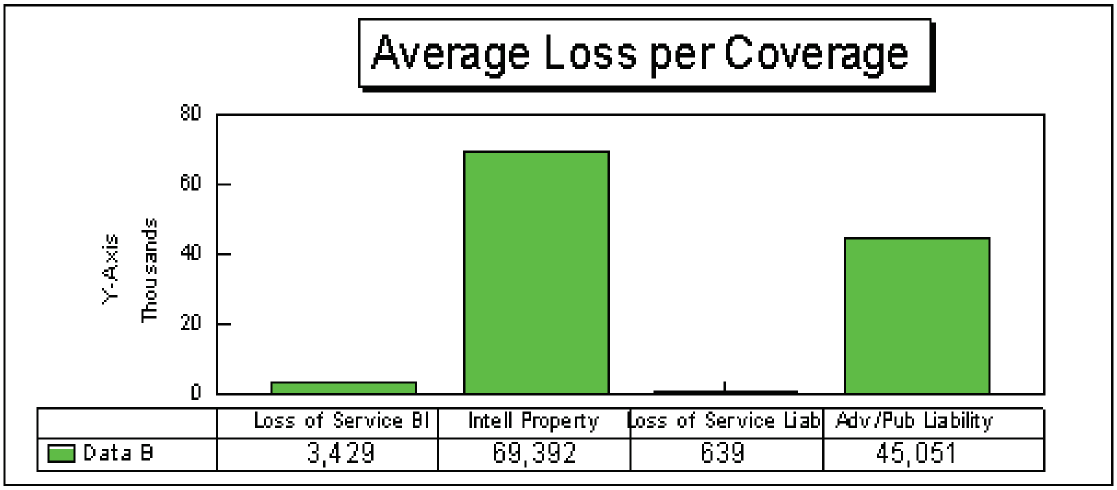
Another interesting analysis shows that the most frequent electronic-based claim is Loss of Service (i.e. Business Interruption). Loss of service is also a part of everyday life for an e-commerce company. Claims due to Intellectual Property, Loss of Service Liability and Advertising/Publishing Liability are not at all that frequent.



Loss of Service BI	Intell Property	Loss of Service Liab	Adv/Pub Liability
52.3	4.4	6.2	1.2

But……

The next part of the analysis shows that the most expensive claims are, on the other hand, claims due to damage to the company’s Intellectual Property and claims caused by the company’s advertising and/or publishing liability. These kinds of claims can certainly do much more damage to the company and influence the company’s financial status. They can also without doubt destroy the company’s future on the market.



	Loss of Service BI	Intell Property	Loss of Service Liab	Adv/Pub Liability
🟩 Data B	3,429	69,392	639	45,051

Examples of e-risk based claims

Employee

If an employee enters a chat room using his computer at work, he can by mistake or through malevolence cause the company damage due to the spread of misdirected information. Professional and international hackers frequently scan chat sites and become familiar with people who are “free-spoken” on these sites.

Internet Service Provider (ISP)

What kind of liability does an ISP have for sites that are registered on its server? Normally it is possible for a person to register a site without any control from the ISP Company, for example a pornographic or racist site. The most famous claim in this category is the claim against AOL regarding the killings at a school in Littleton, Colorado. What kind of liability does an ISP have for registered sites in its system/server?

Intellectual Property

Examples of companies that have been subject to electronic-based fraud are Amazon.com, Volkswagen, Ford etc. All these companies have been exposed to other companies using their name, copyright, trademarks etc. on the Internet. These kinds of claim are growing rapidly and many lawyers in the UK specialize in handling such claims.

Viruses

Today’s viruses are very intelligent and can in fact totally destroy the hardware of a computer or a network. A new virus is born somewhere in the world every 15 seconds, although most of these viruses never actually enter the market.

The problem of preventing viruses is, strangely enough, growing every day

The problem regarding viruses vs. existing anti-virus software on the market is that it is not possible for the programmers of anti-virus software to keep up with all new viruses. Normally the release of anti–virus software is made after a new virus has been released onto the market.

Another serious issue is that many companies don’t regard viruses as a threat to their activities. They buy anti-virus programs, update them infrequently and do not realize that there can be hundreds of new viruses on the market, which they are not protected against.

To solve the problem of viruses, companies need to use the new intelligent virus-filter programs that exist and that can scan every external e-mail at the e-mail server before it transmits them to the receiver. If, for example, an e-mail server is spammed (when someone sends hundreds or thousands of e-mails to a server with the aim of knocking the server out of action) the virus filter recognizes this and stops all e-mails in advance. Companies with this kind of virus filter were not infected when the “I Love You” virus was distributed on the Internet a few months ago.

Conclusion: We must be aware that today’s viruses are much more harmful then they used to be. Companies must take the virus problem seriously, and more money should be invested to prevent viruses damaging companies’ computer systems.

E-commerce insurances

Insuring e-risks is a very interesting activity and also a very risky business.

Here are just some interesting points to note:

First, the future for most pure e-commerce companies will be rather uncertain. Competition on the e-commerce market is tough and many companies will therefore most likely have to reorganize and in some cases change their business direction. This might prove difficult in the case of a specialized business. Many companies have financial problems and do not have enough capital to make new investments.

The players on the insurance market include Fidelity and Deposit/Zurich Financial Services, AIG, Chubb, Cigna (Secure Systems), and some Lloyds Syndicates (products like Computer Info and Data Security).

Players outside the traditional insurance industry are, for example, Marsh McLennan (Net Secure) and a few consulting firms (mostly on a financial basis).

What kind of e-risk coverage is appropriate?

The insurance coverage should include the following:

Business interruption and loss of profit. □ Coverage for E-risk-based business interruption

Intellectual property (IP) □ Damage to the insured’s IP due to hackers, viruses or programming errors.

Interruption of service liability □ Coverage for claims from clients due to denial of access.

Electronic publishing liability □ For example infringement of copyright, trademark, trade name etc.
Liability regarding material that defames a person or organization through libel, slander, product

		disparagement, trade libel etc.
Public relations expense	□	PR expenses due to e-risk loss.

The coverage should also include Extortion, Theft, Crime etc.

Underwriting department

Insuring e-commerce exposures is a highly specialized and rather risky business. There are two parts that one must keep in mind when insuring e-risks. The first part, and probably the most important, is that the underwriting department **must** know the risk and how the insurance covers the exposure. Remember that each and every e-commerce company has its own exposure and activity and that each e-commerce activity is different from another.

The second part is that the insurer must be able to insure high insurance amounts, i.e. have high reinsurance capacity. To insure a small online trading company could require, for example, a total insurance e-risk limit of USD 50 million.

In brief, we can say that e-commerce is “only” a way of doing business and is normally not part of the company’s liability like, for example, a manufacturer. Another example is that a bank must have normal insurance coverage for professional indemnity, bankers blanket bond, property insurance etc., and after that some kind of e-risk coverage.

ART and/or Coinsurances outside the traditional insurance market

An alternative to a traditional insurance solution is to insure the exposure through an ART solution. It may also be interesting to insure e-risks by way of co-insurance between an insurance company and, for example, a bank.

Part 3

Map out (internet) and summarise links to adequate "literature"

A mapping of links to the areas risk exposures and insurable interests could be most extensive including risk exposures in connection with e-commerce, security systems, management. The following list is a choice of the most relevant links.

Action plans

http://www.cert.org/tech_tips/root_compromise.html
”The CERT Co-ordination Centre in conjunction with AusCERT outlines the essential steps from start to finish on what to do in the event of a system compromise in a UNIX or NT environment. For those looking for a crash course on Incident Handling, this is a good place to start.”

http://www.securityfocus.com/data/library/sim006.pdf
”This document published by Carnegie Mellon SEI serves as a very comprehensive guide to such topics as establishment of security policies, preparation for responding to incidents, analyse of available information to characterise an intrusion, communication between significant parties involved, collection and preservation of admissible evidence, and more.”

http://www.networkmagazine.com/magazine/archive/2000/01/0001def.htm
”Rik Farrows presents a sound introduction to Incident Handling and setting up an Incident Handling Team. He also touches upon involving and contacting law enforcement.”

http://www.enteract.com/~lspitz/hacked.html
”Lance Spitzner offers practical advice on how to properly log events in order to track intruders and assess damage and steps towards recovering from a host compromise.”

http://www.sunworld.com/swol-03-1999/swol-03-security.html
”Security related real world scenarios that a network administrator may face are depicted in Carole Fennelly's piece on Incident Response. She goes on to suggest possible solutions for each situation.”

Computer Emergency Response Teams

http://www.cert.org/nav/alerts.html
The Carnegie Mellon Software Engineering Institute CERT

http://www.auscert.org.au/Information/advisories.html
The Australian CERT

http://www.cert.dfn.de/eng/
The German CERT

Insurance products for internet related services

http://home.aigonline.com/home/
Internet Professional Liability Insurance & Electronic Data Processors Professional Liability Insurance

www.beazley.com
Presentation of the product: “Computer Information & Data Security Insurance (CIDSI)”

www.cainagency.com
Cyberspace Liability Insurance & Webmaster Liability Insurance

www.aforbes.co.uk
Alexander Forbes offer Cyber Insurance Cover

www.goirg.com
Information Risk Group offer Computer Information & Data Security Insurance

www.insurepoint.com

www.insuretrust.com
INSUREtrust Electronic Information Errors & Omissions Liability is offered amongst others.

www.jswum.com
J.S. Wurzler Underwriting Managers offer Breach of Security Losses Insurance amongst others.

www.zurich.com
Zurich offer *E-Risk*

http://www.rsx.co.uk/
Site map /Digital Risks, Network and Online Risks or Technology Risks

Literature

www.nuco.com/nucatalog
E-Risk: Liabilities in a Wired World. The National Underwriter Company.

http://www.iss.net/on-line_store/amazon/
A thorough list of safety literature

Newsletters & Mailing lists

http://e-newsletters.internet.com/
http://e-newsletters.internet.com/mailinglists.html
There are a number of different lists at internet.com and PostMaster Direct, the world's largest supplier of opt-in e-mail announcement lists have joined forces to provide you with information and valuable offers by e-mail.

http://xforce.iss.net/maillists/otherlists.php
An extensive list of mailing lists provided by ISS with a detailed description of every link.

http://www.ecommercetimes.com/
The E-Commerce Times is a free online publication that provides daily news, special reports, and success stories, in addition to an e-commerce products and services guide. The publication's tagline is "Everything You Need To Know About Doing Business Online" and content is 100% e-commerce.

http://www.zdnet.co.uk/misc/newsletter_info.html
ZDNet UK News

http://www.theregister.co.uk
http://www.technewsworld.com/

Research Papers and white papers

http://www.deter.com/unix/
A listing of Unix security information and tools.

http://www.cert.org/research/JHThesis/index.html
An Analysis of Security Incidents on the Internet 1989-1995 (provided by CERT)

Sites with information regarding anti-virus tools and viruses

http://www.drsolomon.com
http://www.mcafee.com
http://www.symantec.com
http://www.cultdeadcow.com/
http://www.counterpane.com/index.html
http://www.welcome.to/Net-Bus/
http://surf.to/netbuster
http://www.atremo.se
http://www.cnet.com/software/0-3745-7-120645.html
http://www.whatis.com
http://www.virusbtn.com/

Security Sites

http://www.securityfocus.com/
The serious security information page

http://www.hackershomepage.com/
The history of hacking

http://www.zdnet.co.uk/news/specials/1999/07/hackers/

http://www.hack-net.com/
The British perspective

http://www.rsasecurity.com/
For security professionals

http://ciac.llnl.gov/cgi-bin/index/bulletins
CIAC Information Bulletins are distributed to the Department of Energy community to notify sites of computer security vulnerabilities and recommended actions.

http://xforce.iss.net/
A large searchable database

http://www.stanford.edu/group/itss-ccs/security/Advisories/
A huge list of security links – mostly technical information