REPORT ON SECURITIES ACTIVITY ON THE INTERNET III

OICV-IOSCO

THE INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSIONS

OCTOBER 2003

TABLE OF CONTENTS

REPORT ON SECURITIES ACTIVITY ON THE INTERNET III

Introduction

1. This is the third IOSCO report on the challenges which the Internet, and Internet enabled technologies, have created for regulators, securities firms and investors.

2. When the Internet first began to be used for commercial purposes, it quickly became clear that this medium could have radical consequences. Amid the buzz of pundits, research analysts, consultants and the media, certain broad themes may be discerned. It was predicted that the rise of the Internet and the world wide web would transform the financial landscape, refashion relationships between firm and client, dissolve jurisdictional borders, place the effective providers of financial services beyond the reach of regulators and, at least from a regulatory perspective, create an entirely new set of risks.

3. In the event, the effect of the Internet has been more ubiquitous and less radical than initially envisaged. The fall in world stock markets has reduced the amount of money available for new ventures whilst simultaneously limiting public enthusiasm for spending money on new securities services. The view that Internet transactions take place in cyberspace and are therefore outside the scope of any jurisdiction was exposed as hollow, once courts were possessed of cases. The argument that local regulatory requirements are a unique obstacle to the global market place also had to confront the fact that firms are at a competitive disadvantage in those retail financial markets where they do not have a well known brand name. On the other hand, it was not initially appreciated quite how much the use of Internet enabled technologies would enable front end applications to be integrated with back office administration. The use of e-enabled and related technologies to take paper out of the system, permit straight through processing and ultimately lead to T+0 clearing and settlement has led to better management of some kinds of risk and exposure to new risks, whilst simultaneously exerting considerable downward pressure on costs.

4. For their part, the IOSCO reports have played an important role in injecting common sense into the debate about the implications of on-line securities trading for regulation. The first report, '*Report on securities activity on the Internet*' published in 1998, set the strategic direction by identifying five key principles and making 24 recommendations. The key principles are worth reiterating. They are:

   - The fundamental principles of securities regulation do not change based on the medium.
   - Consistent with the fundamental principles of securities regulation, regulators should not unnecessarily impede the legitimate use of the Internet by market participants and markets.
   - Regulators should strive for transparency and consistency regarding how their regulations apply in an Internet environment.
   - Regulators should cooperate and share information to monitor and police securities activity on the Internet effectively.
   - Regulators should recognize that electronic media and the use of such media are likely to evolve.

5. The report's 24 recommendations covered four broad areas: the application of existing regulatory requirements to Internet channels; the exercise of regulatory authority over cross border securities activities on the Internet; the use of the Internet to foster investor education and transparency; and the use of the Internet to enhance co-operation in enforcement matters.

6. Since the 1998 report all regulators have looked at their requirements on on-line securities activities. They have used the Internet to make their own requirements more accessible to the public, to provide lists of firms that are authorized, to provide other kinds of information that will help investors make informed decisions. In addition, many regulators undertake forms of surveillance to identify Internet securities fraud. The list of initiatives by regulators is a long one and occupies 182 pages of IOSCO's follow up report, '*Report on Securities Activities on the Internet II*' published in 2001.

7. One of the more significant of the recommendations in the first report in 1998 concerned the circumstances in which regulators would not seek to assert jurisdiction over web-sites that are accessible in another country (and which might therefore technically be subject to local requirements) but which are not targeting their activities at that country. The directed at or targeted at test has proved to be a valuable way of providing legal comfort to firms that have no interest in providing services in other countries. The test has been widely adopted both within and outside the securities field. For example, the International Association of Insurance Supervisors has recommended the directed at approach, and this principle also finds expression within the EU in Article 15 of the Brussels Regulation on jurisdiction.[1]

8. The second IOSCO report on securities activities on the Internet built on the foundations of the first report by focusing on six specific issues, which were seen as areas where important risks might arise. These are:

   - System capacity, resilience and security
   - Liability for hyperlinked information on, and communications during, the offering process
   - Day trading, including possible measures to mitigate risk, such as disclosure, margin, suitability and advertising requirements
   - Internet discussion sites, including possible measures to address abuse, such as regulation, conditions for exemption from regulation, surveillance, enforcement, disclosure, investor education and codes of good practice
   - Enforcement, including measures to improve access to information available to Internet Service Providers

9. The present report builds on the work of IOSCO's two previous reports. It marks a departure, in that it incorporates the fruits of the three Roundtables that were held to check that regulators were in touch with the views and concerns of consumers and the industry. The mandate for this work is provided by the Technical Committee, which instructed the IOSCO Internet Project Team to:

   - Organize Roundtable meetings for consumers and industry in Asia, The Americas and Europe;
   - Identify developments which may require regulatory attention;
   - Monitor those developments;
   - Determine whether the identified developments require regulatory attention;
   - Seek to enhance information sharing on regulatory issues concerning the Internet;
   - Seek to achieve consensus on, or identify a range of, regulatory approaches regarding these issues;
   - Liaise with international fora and committees relating to the Internet and e-commerce.

[1] Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters.

10. The current report represents the outcome of the Roundtables and the views expressed there, as well as the material presented by regulators in order to provide a focus for the discussion. The report is more than a summary of the minutes of those meetings, but should not be taken to represent the views of regulators in general or any individual regulator, in particular. The chairman of the Internet Project Team is also a member of the Financial Stability Forum's contact team on e-finance, and the present report is also informed by the work being done by other expert groups in this area.

11. During the preparation for the Roundtables the Internet Project Team found that the most important issues could be grouped into five broad themes. These correspond to the following detailed sections of the report:

- industry trends
- emerging risks
- cross border
- consumer education
- enforcement

12. The IOSCO Internet Project Team circulated material in advance of each meeting to all Roundtable participants. This covered issues which the Team thought important as well as a number of questions designed to prompt debate. (This material was amended after each Roundtable.) The Roundtables were organized regionally. Within each region (Asia, the Americas, Europe) each member of the Team nominated participants. The organizer of each Roundtable in consultation with colleagues from that region then selected from this list those invited to attend and those asked to give a short presentation. The goal was to obtain a broad and representative coverage by industry and consumer interest, region, and technical expertise. Generally, three or four industry or consumer representatives would give a short presentation to focus the discussion that then followed.

INDUSTRY TRENDS

13. One of the interesting themes to emerge from the Roundtables is that there is no single trend that can be discerned. As regards general internet developments, one can see further growth in access to the Internet and greater willingness among consumers to buy goods or services on-line. Some 10 per cent of people in the world now have access to the Internet, though this average masks significant regional differences. Survey evidence also indicates that consumer confidence in the Internet rose by 10-15 per cent in the last year, though US research indicates that consumers are more confident where there is a "familiar trusted intermediary" to guarantee a transaction.

14. In the area of regulated financial services, and in particular, in the area of securities trading, the story is not of general enhanced growth. While there has been a slow but steady increase in the number of consumers who use the Internet to conduct research into or buy financial services of all sorts, this is only part of the story. The fall in world stock markets has led to a 42 per cent average decline in on-line securities activity, and the proportion of trading on the NYSE and Nasdaq represented by on-line brokers has halved in the two years to 2002.

15. The reduction in on-line securities trading has not halted technological development. In particular, the Roundtables were told that technologies used for linking data could provide investors with direct access to liquidity, thereby weakening the gate-keeper role of broker-dealers and disintermediating exchanges.

16. A representative of one of the leading IT-companies in the world identified a number of new technologies that could impact on the internet. These include: voice recognition across devices, online language translation, instantaneous settlement, on demand network application and intelligent broker liquidity finder.

17. Back office issues, in particular, the growth of straight through processing and consolidation among clearing and settlement systems were also identified as important areas for the future. IT experts suggested that horizontal integration, especially between clearing houses using the same trading platforms for different products, would be more useful than vertical integration between exchanges and clearing houses, since it would minimize cost by standardizing the trading, settlement period and clearing process of different products, and facilitating straight through processing.

EMERGING RISK PROFILE

18. The risks created by the use of Internet enabled technologies are not for the most part new ones. However, existing risks may become more significant where the use of Internet enabled technologies creates exposure to the kind of risks, which were rarely encountered in the past, or where failure to identify and manage such risks did not previously lead to a probability of a high and adverse impact.

19. For this reason the Internet Project Team and Roundtables examined the risks created by the use of e-commerce technologies, regardless of whether these risks are new ones, or are merely a different and enhanced manifestation of existing ones. Risks relating to the cross border provision of services and to consumer understanding are discussed in their respective sections.

20. The two main risks the Team and Roundtable focused were IT security and outsourcing, though business continuity was also held to be an important area of risk. As regards IT security, there was general support for the traditional approach which focuses on measures taken to provide for:

    - Confidentiality
    - Integrity
    - Availability
    - Authentication
    - Non-repudiation, and
    - Procedures, such as segregation of duties, access controls and audit trails, designed to ensure that systems cannot be compromised.

21. Within this framework the Roundtables considered that a number of key risks had been heightened by the Internet. These risks were: fraud and money laundering; issues connected with identity management, including identity theft; privacy; and trust. A number of specific IT vulnerabilities were also identified. These were: the growth of worm viruses; hacking into the core backbone networks that route Internet traffic around the world; risks arising from broadband connectivity; and new web technologies, protocols and standards, such as SOAP, Sun's J2EE and Microsoft's .NET, which may make possible for third parties to control remotely insecure computers via HTTP (web traffic).

22. Delegates made a number of suggestions as to how these risks might better be addressed in the light of the fact that senior management in firms is responsible for risk identification and mitigation. Suggestions included: regulatory guidance on IT risk management; making IT security a board responsibility; the

commissioning of IT audits; the appointment of an IT compliance officer, closely linked to the board of management. We recommend that SC3 considers whether these suggestions may have a use in incentivising appropriate risk management within firms.

23. Outsourcing was the other main risk identified. There was no disagreement with the fact that firms cannot contract out of their regulatory obligations. Delegates at the Roundtables stressed that outsourcing was not an easy option. It required time consuming and thorough analysis, the drawing up of detailed service level agreements and their translation into binding contracts. Furthermore, the firm had to retain sufficient expertise to ensure that it was able to monitor not merely compliance with an agreement, but whether amendments were necessary in the light of market developments.

24. The kind of provisions which delegates thought a service level agreement should contain might include:

- qualitative and quantitative performance targets
- evaluation of performance, for example by third parties, internal audits, self-certification
- remedial action and escalation processes for dealing with inadequate performance.

25. There was some discussion but no settled conclusion at the Roundtables about whether regulators should confine themselves to providing guidance on service level agreements or should also specify particular standards that should be achieved. Firms which had experience of large scale outsourcing arrangements argued that senior management was responsible for ensuring that outsourcing operated properly and that guidance was an appropriate regulatory approach to encourage this outcome. We recommend that SC3 reviews how risks relating to outsourcing should be addressed.

CROSS BORDER

26. The ubiquity of cyberspace removes a number of practical barriers to the actual provision of services cross border. A number of firms would like to take advantage of the global nature of the Internet by providing services cross border without having to comply with local requirements in the country where the recipient of the service is based. One of the industry presenters at the European Roundtable cited evidence from a recent paper that mutual recognition of European and American exchanges could lead to a 50 per cent increase in trading volumes, a 60 per cent reduction in trading costs and a 9 per cent reduction in the cost of equity capital for US and European listed firms.

27. However, it was recognized that the public good of greater competition and lower costs of equity also had to be balanced by the need for appropriate standards of investor protection. Industry views on what should be done may be divided into long term goals (for example, mutual recognition) and more immediate needs (for example, better disclosure). Consumer groups, for their part, expressed concern that mutual recognition might expose them to additional risks and make it harder to complain, obtain redress or receive compensation in the event that a firm from abroad failed. It was also acknowledged that whilst local regulatory requirements presented an obstacle to the global provision of services, it is not the only, or necessarily the most important, impediment. It was said that in retail markets success also depends on having an established brand name and a local presence.

28. As regards the industry’s immediate goals, it was argued that regulators should provide greater transparency and clarity, spelling out the regulatory framework clearly to service providers located outside a particular jurisdiction so as to facilitate clear understanding of regulatory requirements. For example, the regulatory

definition of a "sophisticated investor" may differ across jurisdictions. Different jurisdictions may also have different definitions of products, regulated activities, or of the meaning of the term "solicitation."

29. There were also calls for a more harmonized regulatory approach across jurisdictions to minimize not merely industry confusion, but regulatory gaps and arbitrage. It was suggested that the promotion of international best practice by IOSCO would also help in this area. Over the longer term industry representatives advocated a move to greater regulatory harmonization and/or mutual recognition. Whilst, a number of models were canvassed and there was no consensus on the way forward, beyond the desirability of enhanced transparency and the need for greater consumer education about cross border services.

INVESTOR EDUCATION

30. IOSCO's first Report on securities activity on the Internet highlighted the potential of the medium for educational purposes. The second report published in 2001 provided a checklist of the ways in which the Internet has been used by regulators to enhance education by, for example, providing a data-base of filings and of authorized firms, advising investors of investment risks, on-line trading and fraud, assisting investor research via hyperlinks to selected third party sites, and communicating enforcement decisions.

31. It was widely felt that these initiatives did not exhaust the potential of the medium to promote public understanding. The three Roundtables and the preparatory work for them identified a number of key areas where further progress might be made. In particular, the question of motivation emerged as a critical issue. Many investors do not take the time to access the material that is widely available nor to learn about the implications of their financial decisions before they are made. It was said that many investors do not know what information is objective and therefore cannot assess how much reliance to place on it. Accessibility is not just a question of being able to find information on a web-site, but also about how comprehensible such information is, for example, whether it is at a length and depth that is acceptable to consumers, whether it is in plain language, whether it is engaging, whether it entices people to learn, and provides them with opportunities to learn by doing, and takes advantage of new techniques of "edutainment." The need to avoid the "dusty brochure syndrome" and the effort and expense required to develop a site and keep it up to date were also stressed.

32. There was agreement that regulators, industry and consumers all have a role to play in improving investor education. Regulators were well positioned to provide objective information in particular about risk and regulatory requirements. Industry could provide check-lists or reminders of measures that should be taken before making important investment decisions as well as analytical tools to help investors with their decision making processes. The idea was also canvassed that a "driving test" might be devised for private investors and that kite-marks might have a useful role to play.

33. Whilst the Internet contains a wealth of information on investments and investing, investors need to be educated about how to undertake research and in particular to be aware that:

- Information may be false and designed to manipulate stock prices, especially information on bulletin boards;

- Portals may receive a fee for any click-through referrals to on-line brokers; and any recommendations may not be entirely objective;

- Information on the web should be validated;

- They should deal only with authorized firms.

ENFORCEMENT

34. The first IOSCO report on the internet contained four recommendations designed to enhance international co-operation in enforcement matters. The second IOSCO report looked in broad terms at the kind of data which ISPs might collect and the extent to which such data might be made available to regulators in enforcement cases. A number of options were canvassed to promote understanding between regulators and ISPs in the area of data retention and data access. It was recommended that SC4 explore the suggested options further.

35. The IOSCO Technical Committee therefore provided fora for the options identified in the 2001 report to be discussed with ISPs and other industry and consumer representatives. Four broad issues were addressed. These were:

    - data collection
    - data retention
    - privacy requirements which prevent data from being collected or retained
    - the technical skills and knowledge of regulators permitting them to make informed used of data that is accessible to them

36. A number of possible approaches were discussed at the Roundtables to take forward the issues mentioned above. Some of these are voluntary, for example, creating an industry-sponsored "Code of Conduct" for ISP data retention. Others envisaged regulators pursuing legislative or regulatory initiatives that would require ISPs to collect and retain certain kinds of data, or remove the legal obstacles created by privacy requirements. While others are designed to improve co-operation and co-ordination between and among law enforcement agencies and ISPs.

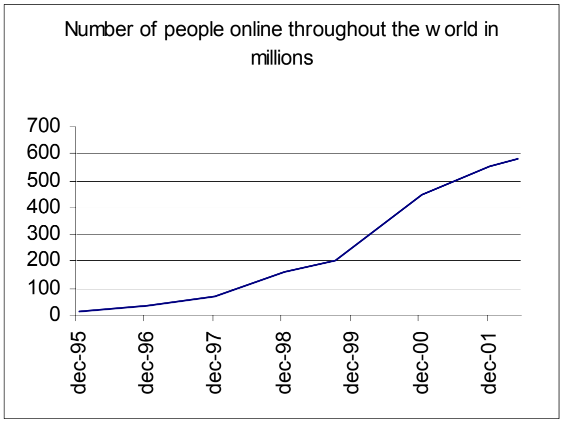
37. The IOSCO Technical Committee makes three sets of recommendations. The first relates to data retention, and in particular to the recommendation that ISPs retain subscriber and traffic data for a minimum of 90 days. The second reiterates previous recommendations in the 2001 report that regulators adopt a range of measures for improving access to ISP information. The third is the suggestion that IOSCO members may need to train their staff in specialized technology skills in order to investigate and prosecute securities fraud conducted over the Internet.

I: Research and Industry trends

1. The use of the Internet by the financial services sector is still evolving. National regulators need to keep abreast of emerging developments. This should enable regulators to proactively allocate resources and shape regulatory policy to anticipate new, and evolving, Internet-related developments within the financial industry. In this chapter we sketch research and trends of the securities industry with regards to the Internet. First we look at consumers/investors; second we discuss brokers and markets. The third and last part of this chapter highlights technological developments.

CONSUMERS

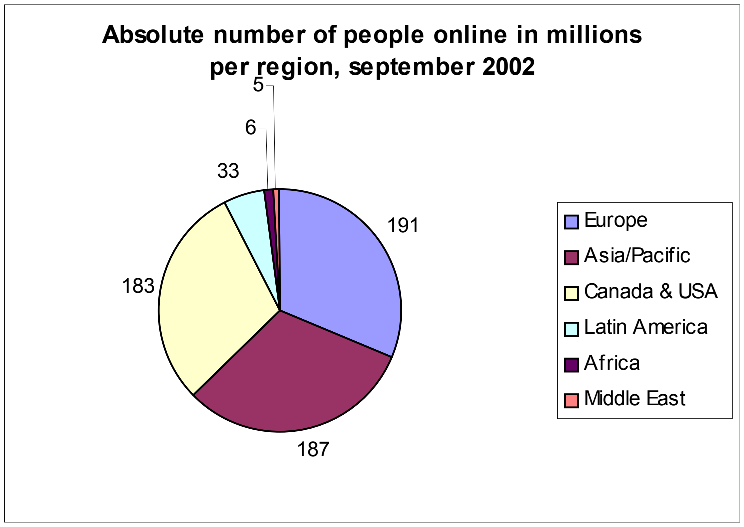
2. An estimated 581 million people were online worldwide as of May 2002.[2] The number of people online worldwide is growing, but still more than 90 out of 100 people worldwide do not have access to the Internet.



Source: www.nua.ie

Divided by the continents in absolute numbers, we see the following pie:

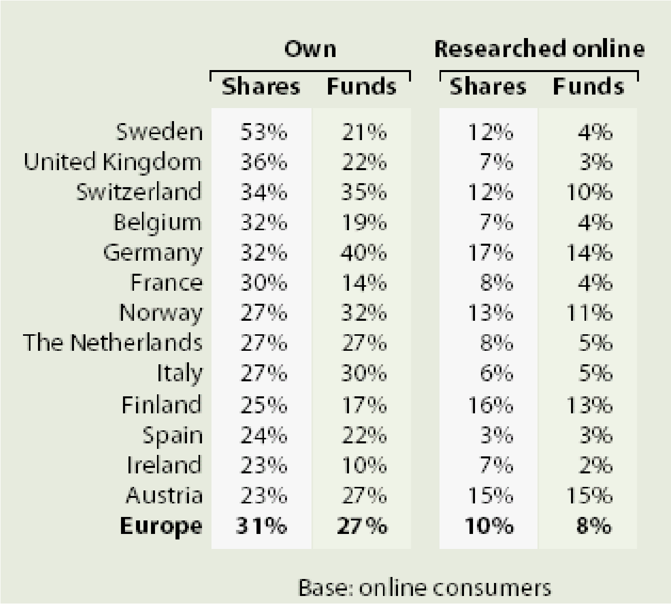
[2] From observing various published surveys over the last two years, Nua made this self described "educated guess"; source: www.nua.ie/surveys/how_many_online/



Source: www.nua.ie

3. These numbers are absolute regional aggregates; underlying differences in percentages per region can be formidable. For example, in Europe we see 68% of people in Sweden online, [3] 57% of people in the UK,[4] 51,8 % in Germany[5] and 0.34% in Albania.[6] In Asia we see percentages vary from 60% in Hong Kong,[7] to 3.6% in China,[8] to 0.02% in Bhutan[9] and Myanmar (Burma).[10] In the US, 59% of the population has Internet access,[11] while 53% of Canadians are online consumers.[12]
4. As one might expect, the growth of Internet use has also led to more people using the Internet to buy and research financial products and securities. Forrester, for example, polled European online consumers and found that 31% of European online consumers own shares; one in three online European share owners researched for them online.

[3] September 2002, 6.02 million people, 67.81%; source: Nielsen NetRatings via www.nua.ie
[4] September 2002, 34.3 million people, 57.24%; source: Nielsen NetRatings via www.nua.ie
[5] March 2003, 33.3 million people; 51,8%; source: @facts via www.atfacts.de
[6] December 2000, 12,000 people, 0.34%; source: eMarketer via www.nua.ie
[7] April 2002, 4.35 million people, 59.58%; source: Nielsen NetRatings via www.nua.ie
[8] July 2002, 45.8 million people, 3.58%; source: CNNIC via www.nua.ie
[9] December 2001, 2,500 people, 0.02%; source: ITU via www.nua.ie
[10] December 2001, 10,000 people, 0.02%; source: ITU via www.nua.ie
[11] April 2002, 165.75 million people, 59.1%; source: NielsenNetRatings via www.nua.ie
[12] March 2002, 16.84 million people, 52.79%; source: Nielsen NetRatings via www.nua.ie



	Own		Researched online	
	Shares	Funds	Shares	Funds
Sweden	53%	21%	12%	4%
United Kingdom	36%	22%	7%	3%
Switzerland	34%	35%	12%	10%
Belgium	32%	19%	7%	4%
Germany	32%	40%	17%	14%
France	30%	14%	8%	4%
Norway	27%	32%	13%	11%
The Netherlands	27%	27%	8%	5%
Italy	27%	30%	6%	5%
Finland	25%	17%	16%	13%
Spain	24%	22%	3%	3%
Ireland	23%	10%	7%	2%
Austria	23%	27%	15%	15%
Europe	**31%**	**27%**	**10%**	**8%**

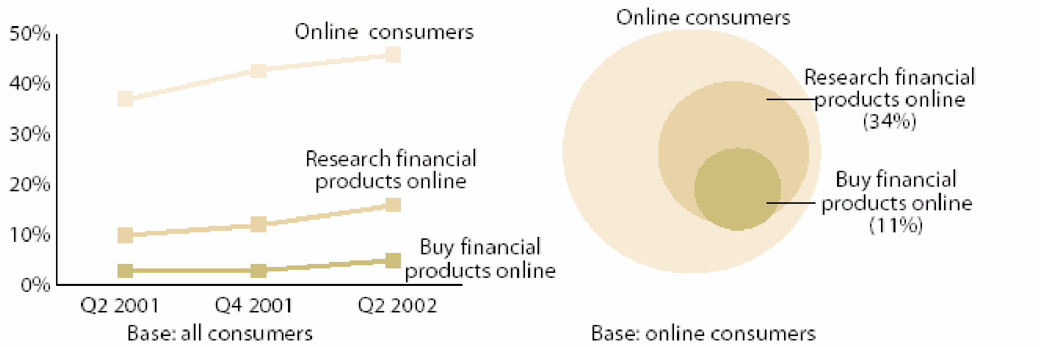
Base: online consumers

Source: Forrester Personal Finance Europe Consumer Technographics Data Overview, May 2002

5. According to Nielsen-Netratings more than 85% of all Internet users utilize their connection for e-mail; general web surfing and product/service research followed a distant second and third at 65% and 63% respectively.

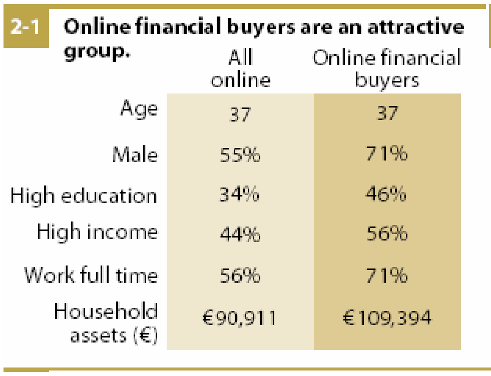
6. The number of people who buy and research financial products (insurances, mortgages, loans, securities, etc.) online is growing.

1-1 Online financial research and buying keep on growing.



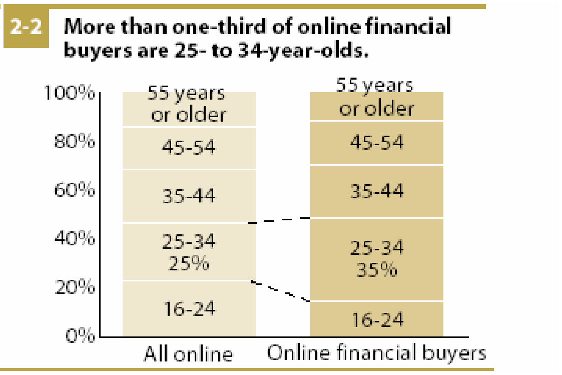
Source: Forrester Why Consumers Buy Financial Products Online, September 2002

7. According to a Forrester report in 2002, people who buy financial products online are more affluent, higher educated and more likely to work full-time than other people who are online.



2-1 Online financial buyers are an attractive group.

	All online	Online financial buyers
Age	37	37
Male	55%	71%
High education	34%	46%
High income	44%	56%
Work full time	56%	71%
Household assets (€)	€90,911	€109,394



2-2 More than one-third of online financial buyers are 25- to 34-year-olds.

Source: Forrester, Why Consumers Buy Financial Products Online, September 2002

8. Many consumers fail to make online purchases because of continued reluctance to engage in transactions with intermediaries that are not familiar and trusted, according to a study by researchers at the University at Buffalo School of Management.[13] The perceived risk to consumers is reduced considerably if a "familiar, trusted intermediary" guarantees the transaction. Another finding of the study was that Internet shoppers are more willing to risk their credit card information when presented with a financial incentive, such as prices that are lower than what is available offline.

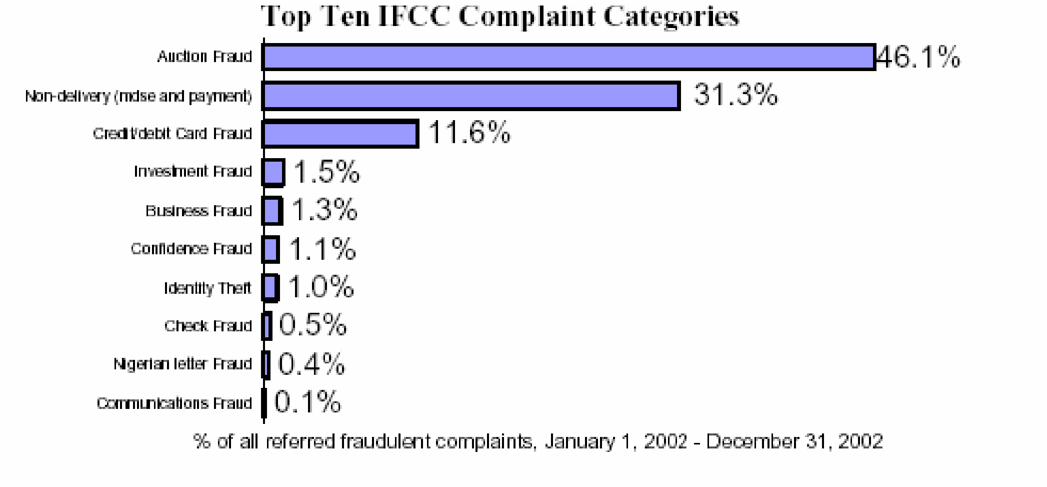
INTERNET FRAUD

9. The Roundtables considered fraud as one of the key risks which has been heightened by the Internet. What are the facts on internet fraud? The available information is rather fragmented, but can provide some insight.

10. In the US the Internet Fraud Complaint Center (IFCC) [14] received over 75,063 complaints from Internet users during 2001. Most of the complaints received involved computer intrusion and hacking and child pornography, rather than Internet fraud. Auction fraud accounts for nearly 43 percent of all reported Internet fraud in the US, while investment fraud accounts for only 1,5%.

[13] source: www.buffalo.edu/news/fast-execute.cgi/article-page.html?article=59430009. The study was based on a Georgia Institute of Technology Web survey of 4,000 individuals of various age, income and education

[14] The Internet Fraud Complaint Center (IFCC), which began operation on May 8, 2000, is a partnership between NW3C (National White Collar Crime Center) and the Federal Bureau of Investigation (FBI). IFCC's primary mission is to address fraud committed over the Internet. This mission is met by facilitating the flow of information between law enforcement agencies and victims. (http://www1.ifccfbi.gov/strategy/2002_IFCCReport.pdf)



11. According to a report commissioned by the Confederation of Asian and Pacific Accountants and conducted by the Australian Institute of Criminology, between 5 and 10 percent of all online transactions in the region involve fraud.[15] The report covered 21 countries in the region and found that online fraud was "hugely under-reported and hard to track down." It also said that criminals were using the Internet to launder money. The report focused on securities and investment fraud, information piracy and consumer fraud.

12. IDC[16] surveyed more than 12,000 European citizens in 14 countries about their worries regarding credit card and home banking fraud, file theft, email fraud, and computer viruses. The fear of complete or partial loss of data due to computer viruses ranks first, closely followed by the fear of credit card information theft. Online or offline computer data theft ranks at third, while email security and home banking are fairly safe in the eyes of European consumers.

13. The Yahoo!/ACNielsen Internet Confidence Index[17], a quarterly study designed to measure confidence levels in Internet products and services is currently in its second year of analysis. Yahoo!/ACNielsen Internet Confidence Index for US consumers shows that the confidence rose by 15% in 2001, with a slight decline and stabilization in 2002.

E-BROKERS, MARKETS AND REGULATORS

14. In all Roundtable sessions there was a common opinion that there a little or no solid, real-time research sources available. Available date show the following trends. In early 2000, online brokers accounted for 45% of trades on the New York Stock Exchange and NASDAQ, dropping to 22% in April 2002[18]. About 66% of all executed orders on the Italian Stock Exchange are generated online.[19] However, 2002 was a year of closure or consolidation for internet-only brokers. There is a decline of 42% in average online activity, as shown by Deloitte's survey on online securities trading.

[15] The report is available via www.capa.com.my/

[16] Source: www.idc.com/getdoc.jhtml?containerId=pr2002_06_24_154308, June 24th, 2002. IDC provides worldwide analysis, market data and startegical guidance for the IT industry.

[17] Source: www.acnielsen.com/news/corp/2003/20030117.htm

[18] Source: www.businessweek.com/magazine/content/02_16/b3779101.htm posted April 22, 2002

[19] Source: Italian Bank at IOSCO Roundtable Meeting Amsterdam, March 2003

15. Finance and investment sites manage to keep the customer interested[20]. Data from Nielsen NetRatings shows that 44% of active Internet users visited a finance site in January 2002, and each user spent an average of 21 minutes at that site. During the European Roundtable Meeting in March 2003, market participants expressed that a 'clicks and mortar' approach may be best: combining computing with traditional customer coverage may attract the most customers.

TECHNOLOGICAL DEVELOPMENTS

16. The Internet is a medium of communication. The use of the Internet itself does not alter the principles of securities regulation. However, the speed, power and possibilities of computers and networks sometimes cause regulators to the idea that this medium could have radical consequences. The idea was that the rise of the Internet and the World Wide Web would transform the financial landscape, refashion relationships between firm and client, dissolve jurisdictional borders, place the effective providers of financial services beyond the reach of regulators and, at least from a regulatory perspective, create an entirely new set of risks. In the event, the effect of the Internet has been less radical than initially envisaged. That is why it is good to try to strip down new technology to what it really implies for markets and consumers.

Data and Research

17. Due to the Internet, the volume of information is growing exponentially. The directly accessible Web is growing at a rate of 7.3 million pages per day.[21] In March 2003 the search engine www.google.com provided a search of 3,083,324,652 web pages. Most of this information is free.

18. Delegates at the Roundtable meetings suggested that data linkage is the key to future developments. With data linkage the there could be "disintermediation" of stock exchanges. End users want direct access to the liquidity pool, a development that may weaken the role of the broker/dealer as gatekeeper. Customers need to be linked at the pre-trade (information), trade (transaction) and post-trade (credit ring) steps. The following success criteria were mentioned at the Roundtables: cost savings, advantage of sharing information, integrity of system and users, geometric search reach and ability to work with current business models.

19. The Internet facilitates the distribution of research reports. Research is delivered more quickly and to a wider audience. The research is not new, but the dissemination is cheaper and faster. A representative of one leading IT-company suggested that new technology within the next five years that may have an impact on the internet include: voice recognition devices, online language translation, instantaneous settlement, on demand network application and intelligent broker liquidity finder.

Order Execution

20. Internet and computer technology also reduces the commissions intermediaries charge investors, by driving down transaction costs and increasing investors' abilities to "comparison shop." The Roundtable participants

[20] Source: www.nua.com/surveys/index.cgi?f=VS&art_id=905357706&rel=true posted February 28, 2002. After finance sites, news and information sites were the next stickiest, with the average visit lasting 15 minutes and 47 seconds. Family and lifestyle sites (including children's sites) were next, followed by search engines, portals and community sites.

agreed that, as more than 80% of the value of a trade is in settlement and clearing, the ability to provide low cost clearing and settlement is critical. This entails development of industry standard which will help lowering the cost of transaction and facilitating efficient STP (Straight Trough Processing). Low value services may be out source to utilities network providers. Online brokers have to provide service that can differentiate it from others such as investment advising.

21. In addition, Roundtable participants indicated that lots of cost inefficiencies in online trading are due to the non-existence of STP and the lack of common clearing and settlement standards and systems. This hurts retail investors by increasing online trading costs, which, in turn, reduces market liquidity. Although STP is good for the security industry, brokers, particularly the small ones, are sluggish to its development. It was suggested in the discussion at the Hong Kong Roundtable, that STP will deprive brokers the opportunity to profit from idle funds pending for clearing and brokers and therefore some of them are not willing to spend significant amount to upgrade their system. However, the technique and security is complicated and investment costs are high.

22. IT experts suggested that horizontal integrations, especially those among clearing houses and using same trading platforms for different products, are more useful than vertical integrations between exchanges and clearing houses. It minimizes costs by standardizing the trading, settlement period and clearing process of different products. It also enables STP. However, horizontal integration happens infrequently because, according to some delegates, inertia exists for investors to move to a new system, for brokers to invest in a new system and for service providers to change their systems.

23. Developing technology also leads to the question of how far e-brokers can go. Automated transaction suggestions could be in conflict with the "duty of care." The Internet and technical development can provide more service to people like real-time online customer service and real time updated account status.

Standardization

24. Standardized IT development platforms can lead to reduced costs, and can result in shorter time to market for e-brokers and trading systems, (e.g., the developers of Java coined the phrase "Write once, run everywhere.") These reduced barriers to entry could result in increased competition and more innovation.

25. Standardization enables consumers to trade everywhere using various new devices (PDA's, cell phones), which means quicker availability of access and clearing and settlement.

26. Standardization of data exchange protocols (e.g., XML, SOAP, WSDL) can improve and hasten investment strategies, companies reporting, or simply comparing e-brokers' fees.

27. Public Key Infrastructure (PKI) is another example how standardization can lead to efficiency gains, in this case by increasing security.

[21] How Much Information?" Hal Varian and Peter Lyman of the School of Information Management & Systems at Berkeley. Source: www.berkeley.edu/news/berkeleyan/2000/10/25/infor.html posted at October 25th, 2002

Technology trends and regulators

28. In one of the discussion sessions a statement was made that there is a need for more international best practices and guidelines, transparency of rules, monitoring and enforcement. It was stated that regulators should “monitor methodologies rather than dictating rules.” A question was raised if there is the necessary infrastructure in place to allow the changes being discussed. There appears to be a large amount of demand for trading cost information and analysis.

29. In response to the questions on new business cases, there would be increasing demand for aggregation and integration of services. One example mentioned is aggregation of financial data across accounts and relationships. A more robust financial management function will be needed. Delegates suggested that a major regulatory issue will be the question who owns the data. There may be a shift from intermediaries who control the data and access to data to making data available to investors to use how they choose. New models will arise from the data issue.

CONCLUSION

30. Risks can be reduced but will never be eliminated. Technology can do many things, but efficiency gains depend on implementation factors, e.g. costs and the extent to which common standards are being used. Roundtable participants agreed that most of the barriers for Internet trading embedded in regulations are already vanishing, but other barriers, e.g. commercial, still exist which may hinder horizontal integration and cross border trading. More consultation between regulators and industry will benefit both parties in that regulators can make better regulations with better understanding of the development of internet and the industry and industrial practitioners can have a better understanding of the thinking and important elements of the regulation.

II. Emerging Risk Profile

1. This section on the profile of emerging risks builds on the work contained in the second report of the IOSCO Technical Committee, '*Report on securities activity on the Internet II.*' That report contained a lengthy discussion of issues related to system capacity, resilience and security. Most of material and associated recommendations focused on issues of system capacity and resilience. Less attention was given to issues relating to security. Furthermore, whilst outsourcing was mentioned, it was not considered as an explicit risk issue.

2. This section aims to address these two gaps as they relate to the use of information technology (IT) and specifically the Internet. The risks discussed in this section, as well as the Roundtable sessions that provided much of the material for it, aim to fill these two gaps. IT provides the backbone for securities firms, whether or not they have a presence on the World Wide Web. Many of the issues that are relevant for the management of non-Internet enabled technologies are also relevant to the control of Internet enabled ones. But the potential for overlap did not seem to us to be a good reason to ignore the main risks in order to focus on the handful of IT related questions which are relevant mainly to cyberspace. We have therefore chosen to focus on two critical questions, which were less extensively discussed in the previous report, as well as a handful of less far reaching issues.[22] Two of the major risk areas are:

   - IT risk/ Security controls
   - Outsourcing

3. Two specific areas, which do give rise to risk, are discussed in the next two sections: risks that arise for regulators, firms or their customers when the use of technologies with a global reach are confronted by national or local jurisdictions; and the need for greater consumer awareness of the information that the Internet has made available, the tools to analyze it, and the need to understand what such data does and does not mean.

IT RISK/SECURITY CONTROLS

4. Effective security is the foundation for e-commerce. Without levels of security which command confidence, consumers, firms and regulators would be unwilling to see the Internet as more than a global shop-window. Critical on-line risks for securities firms and their customers include:

   - unauthorized trading
   - reliance on incorrect financial information
   - on-line fraud, including ID theft
   - unavailability of a service or component of a service
   - breaches of privacy

[22] Given current market conditions, it has not been suggested that issues related to day trading need further attention. These were extensively discussed in the previous IOSCO report, '*Report on securities activity on the Internet II.*'

- disputed trades.

5. The following non-exhaustive criteria list a set of considerations which may be useful in helping firms to determine whether their systems and controls do properly manage the kind of security risks mentioned above. They are:

   a) Confidentiality: ensuring that information is accessible only to an authorized person or system. (Internal firewalls and the use of encryption, as well as entry restrictions may be indicated.) Inadequate controls may result in:

      - Unwanted disclosure of personal data, transactions, activity, presence on the Internet, etc.
      - Stealing IDs
      - Impersonation, leading to unauthorized (illegal) transactions
      - Unauthorized usage and inability to detect this in a timely fashion and/or identify the perpetrator
      - Distributed denial of service attacks, leading to communication impossibilities, or to a firm itself unwittingly becoming an agent for a distributed denial of service attack against another web-site;
      - Traffic analysis by unauthorized third parties, possibly enabling commercial espionage, e.g. foreknowledge of mergers or acquisitions.

   b) Integrity: safeguarding the accuracy and completeness of the information and its processing. Firms need to address the risk that inadequate controls could expose their data to corruption and this might result in:

      - Non-compliance with rules and regulation, leading to illegal transactions
      - Presentation of incorrect data, whether unintentionally or malevolently (e.g. hoaxes, churning)
      - False presentation, or the use of incomplete information for transactions
      - Manipulation of data, leading to unauthorized transactions
      - Viruses, leading to loss of data, unauthorized access to or manipulation of data, unavailability of systems, etc.
      - Cyber extortion, selling data stolen from (or illegally obtained from) securities firms
      - Logic bombs, with the potential to blackmail firms.

   c) Availability: ensuring that an authorized person or system can access the data or service. Since firms will wish to enable their customers to trade, and regulators require firms to be able to properly process transactions during business hours, firms need to address the risk:

      - that the site is not reachable, and there is no possibility to trade, or to get or give information; or
      - that parts of their own site are not reachable, whether as a result of a denial of service attack or for some other reason, e.g. lack of capacity; or
      - that the firm is unable to provide timely access to the site or parts of the site.

   d) Authentication: ensuring that the identity of the person or system processing information is verified. Spoofing, sniffing or other malicious programs can result in unauthorized access by using authorized, stolen ID’s. Securities firms must therefore ensure that they properly authenticate identity in such a way as to exclude unauthorized individuals or systems. PINs, passwords, smart cards, biometrics, and digital certificates[23] are currently the main ways used to address the risk that:

- A firm's information security (IS) system fails to identify attempts by unauthorized persons to access accounts of the firm or customers;
- A firm's IS system fails to require re-authentication.

e) Non-repudiation and accountability: ensuring that the persons or systems cannot deny their actions. (Firms that use digital certificates will need to ensure that they properly identify and manage the risks of this technology, see paragraph [31].)

6. Firms need to consider how their systems that are supposed to provide confidentiality, integrity, availability, authentication and non-repudiation might be compromised. They will therefore wish to ensure that their controls cannot be bypassed in the migration to the Internet. These controls include segregation of duties to reduce the risk of internal fraud and ensure that transactions and assets are properly authorized, recorded and safeguarded. In particular, those designing systems will need to address the risk that:

   - a single employee (or outsourced provider) could enter, authorize and complete a transaction;
   - those developing a system also operate it and are able to make unauthorized changes to it.

7. Authorization and access controls within securities firms (or outsourced providers) are essential to ensure that segregation of duties operates in practice. Securities firms need to ensure that they have systems in place to address the risk that:

- Authorization data-bases are not tampered with;
- Authorizations are continuously updated and verified.

8. Effective audit trails are an essential part of risk management, enabling firms to monitor attempts to compromise their internal controls. Securities firms that offer on-line trading will, in particular, wish to ensure they have adequate logs to address risk arising from:

- The opening, modification or closing of a client account
- Any transaction with significant financial consequences
- Any authorization granted to a customer to exceed a limit
- Any granting, modification or revocation of systems access rights or privileges.

9. The summary provided above is not intended to be comprehensive. New technologies have the capacity to facilitate new business models and to create risks, including risks to existing systems. Firms will therefore need to ensure that they remain alert to the possibility of unexpected consequences and emerging, new threats.

10. The considerations listed above are drawn from current views of good practice as well as the second report of the IOSCO Technical Committee and the Basel Committee's 14 risk management principles in electronic banking. These considerations cover a large number of risks in high level rather than specific terms. At the Roundtables delegates provided valuable contributions, especially as regards some specific current risks or risk areas which they considered most important.

[23] Biometrics can be used as a way of authentication where a physical attribute of an individual, e.g. a fingerprint or iris scan, matches those previously recorded for that individual. A digital certificate is based on the fact that data can be encoded with one mathematical algorithm, and decoded with a different, unique but related algorithm.

11. Delegates thought that a number of key risks had been heightened by the Internet. Among these were fraud and money laundering; issues connected with identity management, including identity theft; privacy; and trust. Like many issues highlighted by the Internet, none of these are new questions in and of themselves. At the Roundtables it was pointed out that the use of the Internet made transactions and the gathering of information 'frictionless.' It was suggested that while the development of straight through processing had reduced clerical errors, it also meant that there was less scope to correct mistakes or identify attempts at fraud, unless systems were specifically programmed to do so. In addition, personal information could now be collected anonymously from dispersed sources at little cost in terms of time, travel or money.[24] While there was some skepticism about how well informal controls and human intervention did work in the pre-Internet age, it was not disputed that where controls had relied on the cost and inconvenience of data collection and on, albeit sometimes haphazard, human oversight, the question of how to formalize and implement appropriate electronic safeguards in an automated environment had to be considered.

12. Another delegate noted that technological improvements may create significant challenges for other parts of the system. For example, increases in transaction speed may have an impact on risk mitigation. A credit check that takes 1/10 second has a considerable cost in a world in which trades are executed in 1/1000 of a second. Delegates were told that in some instances there is customer pressure to circumvent these broker-dealer controls.

13. It was also argued that increases in transaction speed may have a broader impact across the whole market. For example, glitches in the system (such as a mis-keyed order) may have a ripple effect through the market as automated trading and arbitrage systems take advantage of the trading opportunity. Some exchanges have sought to address these risks by placing size limits on orders, price banding, and time order cancellations, so that orders are automatically cancelled after a certain time.

14. Some delegates noted that it was not easy to find a balance between risk management and speed, that is between the number of automated checks to program into automated trading software and the commercial need to seize a short-lived arbitrage opportunity, before another firm's automated trading software had done so.

15. A number of specific IT vulnerabilities were also identified. It was suggested that Internet worms will become more sophisticated and will spread very quickly. Like the Slammer virus, the primary problem will be the traffic such viruses produce and which cause a denial of service effect. It was thought that the infected systems themselves will be a secondary concern. It was predicted that future worms will be similar to Slammer but will exploit a webserver vulnerability rather than a rarely used SQL[25] service. This means that the Slammer solution, i.e. the service provider blocking the service, will not work as it will prevent webservers from functioning.

16. A further prediction was that some attackers might turn their attentions to the core backbone networks that route Internet traffic around the world. These core networks, owned by companies such as Worldcom, are not well understood by the larger Internet community. Should hackers be able to compromise core networks, they will be in a position make portions of the Internet disappear.

17. Broadband connectivity (e.g. ADSL or cable) was also considered likely to be a source of risk. Broadband home users have permanent Internet connections and may host their own services. These home networks will rarely be well defended and will be a ripe target for hackers who want to use them as “zombie” systems from

[24] There are also some web-sites that create new sources of information to be tapped, for example those which allow old school friends to provide personal information that is often publicly accessible.

which to launch attacks at other (possibly corporate) targets. Broadband connectivity also increases the attraction of home working via remote links. Firms need to build into their defenses the awareness that compromise of these remote systems may result in another means of attack into corporate networks.

18. An additional source of identified risk is web services. Web technology is becoming increasingly sophisticated. Several protocols such as SOAP and development standards such as Sun's J2EE and Microsoft's .NET are encouraging the next generation of the web. This will consist of direct computer-to-computer interaction and transaction processing via the web, rather than human interactive webpages. It was argued that this concept of fully distributed systems opens up significant risks to the systems running these services, as it may be possible to remote control insecure computers via HTTP (web traffic).

19. These examples of specific current risks highlight the fact that standards of IT security and controls need to be informed by the nature of the threats that exist and also be appropriate to the business model of a firm, to the risks created by this model, as well as to the use made of particular technologies. In the Roundtable discussions some participants thought that regulators should set out their own IT security standards or endorse existing ones (e.g. ISO 17799). It was argued that firms would then know whether or not their approach to security was consistent with good practice. Others, however, argued that regulators were not best placed to form an expert view about IT security. Inevitably, they would be relying on external expertise, and a regulatory view would not therefore add significantly to what was already known. Furthermore, in such a fast moving area, firms that waited for a standard to be up-dated would be exposing themselves to risk. In addition, delegates felt that the levels of security that are appropriate depend on precisely what a firm is doing, and that appropriate solutions will therefore vary widely.

20. Regulators do not have to specify particular standards or solutions in order to have an interest in encouraging firms to enhance their IT systems and controls. One IT academic with security expertise expressed the view that providing good levels of IT security (whether over the Internet or through other channels, e.g. ATMs) is not ultimately a question of technology. In his view the critical question is how technologies are deployed. Failures of security that lead to customer losses generally occur with the connivance of insiders, he argued, and therefore stressed that effective internal controls are critical, particularly controls on IT systems operators.

21. The same academic argued that the incentives on firms to create a secure environment for the technologies they use are often insufficient. He said that in jurisdictions where firms are required (in the absence of proof on their part of fraud) to bear the cost of disputed transactions, the number of such disputes is lower than in countries where firms are able to transfer the risk of security failures to third parties, whether customers or retailers.

22. This comparative insight highlights the relevance of the recommendation made in the previous IOSCO report that regulators consider how to encourage firms to address risks relating to capacity, resilience and security.

23. Four suggestions were made at the Roundtables for encouraging firms to address IT security risks. One was providing guidance on important risks associated with the use of the Internet for securities trading. The information presented in paragraphs 4-19 may be helpful in this regard. A second was that IT security should be a board responsibility with accompanying accountability at the level of senior management. This would require sufficient expertise at the highest levels of decision-making, and in some cases might require new appointments, since board members and top managers may not be fully aware of the risks inherent in Internet usage. A third suggestion was that each firm takes steps, such as commissioning IT audits of their systems, to ensure that its board would know whether or not it could be satisfied that its IT infrastructure was adequately

[25] Structured Query Language

secured. Lastly, it was suggested that firms create a specific IT compliance officer, preferably closely linked to the board, to conduct an audit of the adequacy of a firm’s IT security controls, including those at any outsourcer, at least every two years.

OUTSOURCING

24. Outsourcing IT systems is a growing and widespread practice which can confer significant benefits to firms while at the same time affecting their exposure to operational risk through: first, significant changes to people, processes and systems; and second, reduced control over the people, processes and systems used in the outsourced activities.

25. Firms cannot contract out of their regulatory obligations, and for this reason alone it is important that the risks of reduced control are managed effectively throughout the life cycle of a firm's outsourcing arrangements. Outsourcing may be viewed as falling into four phases:

- The decision on whether or not to outsource, or change an existing outsourcing arrangement.
- The drafting of an outsourcing contract,
- The implementation and maintenance of an outsourcing arrangement,
- Dealing with the expected or unexpected termination of a contract, so as to ensure business continuity, especially where the outsource service provider fails.

26. The decision to outsource an important function needs careful analysis of a number of issues. These may include:

- the organization and reporting structure for outsourcing arrangements (including senior management oversight);
- whether the outsourcing contracts, service level agreements and relationship management framework allow it to monitor and control its exposure to the risks of outsourcing people, processes or systems;
- how the proposed outsourcing arrangements will affect the firm's risk profile, business strategy and ability to meet regulatory obligations;
- the financial soundness and technical expertise of the service provider;
- how a smooth transition to the service provider will be effected;
- the possibility that outsourcing might create a risk for business continuity, for example where a service provider is itself used by several firms. Firms will therefore need to have appropriate contingency arrangements in the event that a service provider is unable to continue to provide a service.

27. Delegates at the Roundtables stressed that outsourcing was not an easy option, though it was said to be less difficult than managing a joint venture. Outsourcing required time consuming and thorough analysis, the drawing up of detailed service level agreements and their translation into binding contracts. Furthermore, the firm had to retain sufficient expertise to ensure that it was able to monitor not merely compliance with an agreement, but whether amendments were necessary in the light of market developments. Those who had been involved in considering whether or not to outsource reported that sometimes perceived advantages of moving a function to an external provider did not survive analysis.

28. Matters which firms might wish to consider when negotiating an outsourcing contract include:

- notification and reporting requirements
- the kind of access that might be needed by the firm, its auditor, regulator, etc.
- intellectual property and information ownership rights, confidentiality agreements, Chinese walls, etc.
- the need for, and adequacy of, any guarantees or indemnities
- compliance with the firm's own policies, for example on information security
- arrangements to ensure business continuity and the extent to which facilities that provide the outsourcing are or are not available to provide business continuity for third parties
- approval processes for changes to outsourcing arrangements
- agreed conditions for terminating outsourcing arrangements.

29. Delegates at the Roundtables considered that the most important issue for firms entering into outsourcing arrangements was the drafting of the service level agreement. A service level agreement should specify what the service provider will, in fact, do. The kind of provisions an agreement might contain include:

    - qualitative and quantitative performance targets
    - evaluation of performance, for example by third parties, internal audits, self-certification
    - remedial action and escalation processes for dealing with inadequate performance.

30. There was some discussion at the Roundtables about whether regulators should confine themselves to providing guidance on service level agreements or should specify particular standards that should be achieved. Firms which had experience with large-scale outsourcing arrangements argued that senior management remained responsible for ensuring that outsourcing operated properly and that guidance was an appropriate regulatory approach to encourage this outcome.

OTHER ISSUES

31. There were a number of other risk areas which were identified as important. These are:

    - Disaster recovery
    - Digital signatures
    - Internet discussion sites
    - Best buy and portfolio management systems

Disaster Recovery Planning/Business Continuity Planning (DRP/BCP)

32. Since the events on 11 September 2001, firms, regulators and governments have devoted considerable energy to the question of how best to ensure that business can continue in the face of a large-scale disruption. Many firms now draw a business continuity plan and document their arrangements to manage possible disasters.

33. It is important that such plans are kept up to date and take account of the fact that a disaster may be concentrated within a sector or a geographic area. Firms may wish to assess how long disruptions might last and the impact arising from, for example, the loss or failure of internal or external resources (e.g. people, systems, or other assets), or the loss or corruption of information.

34. The experience of 11 September provided an important lesson. It was reported at the Roundtables that critical transaction processing systems were resilient. The problems came from the organizational side, because while the IT systems continued to be able to function, key individuals were unable to get to work.

Digital certificates supporting electronic signatures

35. The technology behind digital certificates supporting electronic signatures ('electronic signatures') is finding an increasing use among securities firms. The technology can be used bilaterally to enhance existing standards of security. In this model a firm issues its client with an 'electronic signature.' The signature replaces the currently ubiquitous log-on and pin numbers but would not be recognized by anyone other than the issuing firm. No complex regulatory issues arise from the limited use of this technology.

36. However, the technology can be deployed in a dispersed manner, so that a signature issued by a firm to its customer could then be used by that customer in transactions with third parties. These services might include: use of the Internet to open accounts with broker dealers or banks, to enter into contracts, to make binding declarations to the tax authorities or other entities, or to send payment instructions. Electronic signatures, therefore, seek to ensure that:

- communications can be transmitted securely and confidentially, so that others cannot read them, even if they are intercepted;
- all parties know that their counterparty is who he or she purports to be;
- communications cannot be altered in transmission, so that the parties have confidence that the data received is the same as that sent; and
- binding assent can be provided in a communication, such that the other party can act with confidence on the basis of the instruction or contract.

37. It is not, as yet, clear that a business model exists which would support the mass-market provision of electronic signatures using open systems. (At the Roundtable it was reported that over 50 per cent of firms have not thought about the issue.) In many countries the provision of 'trust' services, such as electronic signatures, fall outside the scope of financial service regulation. Nonetheless, regulators have an important interest in this area, since the provision of electronic signatures gives rise to risk in a number of important ways. The main areas are:

- Money laundering and other types of financial crime, in so far as electronic signatures are relied upon as a means of providing evidence of a person's identity;
- The issuance of electronic signatures by firms (for example, broker dealers active in the provision of trust services) will be exposing these firms and ultimately investors to considerable risk and potential liabilities, in the event that the issuance and revocation of thousands of electronic signatures are inadequately managed;
- The acceptance of electronic signatures issued by other firms – firms will need to appreciate that not all signatures are equal and will therefore need to have robust systems in place and check that the signature has not been amended, suspended or revoked.

38. Electronic signatures, if used in a multi-lateral dispersed manner, are likely to raise other questions which regulators will want to address. This is an issue which regulators will want to keep under review in the light of market developments.

Internet discussion sites

39. A great deal of information and opinions about securities investment are available through Internet Discussion Sites (IDS), chat rooms and similar multi-user mechanisms. Of particular significance for regulators is the fact that IDSs can be a cheap and effective way of disseminating false or misleading information about securities markets. Regulators should therefore be aware of the risk that IDS facilities might be misused, and consider how best to deal with that risk in the context of the regulatory framework that operates in their jurisdiction. The IOSCO Report on Securities Activity on the Internet II described – with regard to the different regulatory frameworks – the different possible approaches to dealing with this issue. These include:

- Regulating IDS, whether directly or indirectly by exempting them from regulation where they meet minimum requirements
- Surveillance and enforcement
- Disclosure and investor education
- Codes of practice.

40. At the Roundtables there was discussion of the practicability of imposing regulatory requirements on operators of bulletin boards. It was suggested by some industry representatives that although regulators should be concerned about market manipulation, the appropriate way to address these concerns is to focus on the fraudsters. It was argued that proposals that would require operators of discussion sites to monitor bulletin boards for market manipulators would be unworkable. ISPs everywhere would have to hire investment bankers in order to recognize cases of market manipulation. They would then have to report cases to regulators. An additional complication is that the ISP would have to identify the poster, despite the use of Internet aliases. Furthermore, ISPs would have to continually archive these postings, and there is always the possibility that statements could be made on general bulletin boards, e.g. a sports discussion site, that might be interpreted to be investment advice.

Best buy and portfolio management systems

41. There are a large number of software programs, which seek to analyze investment portfolios and identify best buys. In some jurisdictions these kind of software programs will be viewed as providing a regulated activity (that of investment advice), and the provider of the service will, therefore, need to be Authorized and will be held responsible for the accuracy of the advice provided. Whatever the regulatory status of these software programs, they have limitations, which those relying on their conclusions or recommendations need to realize. These limitations include:

- determining the level of risk which is appropriate for a person’s individual circumstances involves analyzing his or her circumstances and making a set of judgments about them which may be difficult to automate;
- potential flaws in the program – the more complex the product area the harder it will be to avoid software error;
- there may be a lack of clarity as to what criteria are used to analyze portfolios, assess suitability or determine a ‘best buy’;
- an important aspect of a service may not be considered by the program, e.g. speed of execution;
- the software may not interrogate the whole market, but only major brands.

RECOMMENDATIONS

42. The IOSCO Technical Committee has concluded that it should consider ongoing activities in the area of emerging risks that fall broadly into two categories. These are:

    - Monitoring
    - Facilitating

43. We conclude that each of the emerging risk areas we have discussed should be kept under periodic review, in line with the overall recommendation that there should be a yearly Roundtable for regulators and an industry Roundtable every other year. In particular, we suggest that a close watch be kept on the Internet dimensions of three emerging risk areas: fraud and money laundering; identity theft and identity management; privacy and trust.

44. In addition, we consider that in the areas of IT risk/security controls and outsourcing, regulators can play an important role in facilitating or incentivising good standards of risk management. Possible ways of enhancing this are discussed in the following paragraphs.

IT risk/security controls

45. The approach of the IOSCO Technical Committee is set out in the '*Report on securities activity on the Internet II*.' The report states (at page 18) that:

    > "Regulators may wish to consider whether online brokers have an interest in properly addressing risks relating to system capacity, resilience and security. Regulators may also wish to ascertain broker-dealers' interest in developing adequate contingency plans in the event of a failure in capacity, resilience or security. This does not mean that regulators should impose specific technology. Because information technology is an area in which new developments occur extremely quickly, there is a risk that such a prescriptive approach could result in systems that are inappropriate, inefficient and out of date."

46. Based on the Roundtable discussions, this conclusion remains correct. One theme that emerged strongly throughout the Roundtables is that the crucial issue in the area of IT security is not which specific technologies are used, but rather the identification of risk and its subsequent management. Risk identification, management and mitigation are pre-eminently the responsibilities of senior management. The Roundtables discussed the following suggestions for improving risk management by firms in the area of IT. These are:

    - Providing guidance on important risks associated with the use of the Internet for securities trading. The information presented in paragraphs 4-19 may be helpful in this regard;
    - Making IT security a board level responsibility with accompanying accountability at the level of senior management;
    - Requiring firms to take steps, for example commissioning external IT audits of their systems, so that the Board would know whether or not it could be satisfied that its IT infrastructure was adequately secured;
    - Requiring firms to create a specific IT compliance officer to conduct a regular audit (possibly every two years) of the adequacy of a firm's IT security controls, including those at any outsourcer.

47. The IOSCO Technical Committee also will consider whether these suggestions may have a use in incentivising appropriate risk management within firms.

Outsourcing

48. Like successful IT security management, successful outsourcing is a management issue. The Roundtables stressed that if outsourcing were to achieve its objects, prime consideration had to be given to service level agreements. (There was some debate, but no settled conclusion, about whether regulators should issue specific outsourcing standards, as opposed to guidance. Large firms with experience in outsourcing seemed to favor guidance.) Nonetheless, regulators may wish to have regard to the specific considerations listed in our discussion (paragraphs [20-25] above) and we recommend that SC3 review how risks relating to outsourcing should be addressed.

Other areas

49. Our analysis of the other issues discussed in this section of the report do not lead to any specific recommendations beyond the need to keep developments under review.

III: CROSS-BORDER ISSUES

Background

1. The global nature of the Internet and its ability to provide fast and seamless links between financial service providers and investors in different jurisdictions has fuelled the growth of cross-border activities in securities. Traditional notions of geographical borders have become obsolete. Whilst cross-border securities issues have long existed, these issues have become starker due to the nature of the Internet. Cross-border issues are important to any discussion of the Internet and the regulatory issues that the Internet creates. [26]

2. Cross-border securities activities, facilitated by the Internet, present both benefits and challenges to global securities regulators. Cross-border activities can help deepen securities markets and enhance liquidity. There is potential for the reduction of trading costs, lowering the cost of capital and increasing economic growth. On the other hand, as described in the two previous IOSCO Internet Reports, cross-border securities activity via the Internet, if not properly managed, can impede a securities regulator's efforts to protect investors and enforce national securities laws.

3. This chapter builds on the work contained in the two earlier IOSCO Internet Reports, "Report on Securities Activity on the Internet I" and "Report on Securities Activity on the Internet II" (the "Internet I" and "Internet II" Reports). The focus of these earlier reports was on clarifying the circumstances under which regulators may assert regulatory jurisdiction over financial services provided via the Internet, *e.g.* whether the offer of services targets residents of the regulator's jurisdiction, whether the offeror accepts orders from or provides services to residents of the regulator's jurisdiction, and whether the offeror uses E-mail or other media to "push" information to residents of the regulator's jurisdiction.

4. The matters raised by participants attending the three Roundtables build on these earlier issues. In particular, Roundtable participants discussed a number of risks associated with cross-border transactions. In mitigating these risks, financial service providers recognized that they have to ensure that they are aware of and meet the requisite legal and regulatory requirements in the countries in which they market their services. At the same time, Roundtable participants agreed that investors, likewise, should be aware of the risks to which they are exposed when engaging in cross-border transactions.

5. Regulators are similarly confronted with issues arising from cross-border transactions. The challenge for regulators is to balance the maximization of the many legitimate benefits of the Internet against any downsides such as potential misconduct. As Roundtable participants pointed out, regulation can either enable or discourage the provision of cross-border services in securities, while technology continues to evolve very quickly. This creates an onus on regulators to keep abreast of new developments, and react swiftly but sensibly.

6. In the cross-border context, certain key issues were raised in the Roundtables:

[26] In the context of this chapter, "cross-border" securities activities mean the provision or solicitation of services where the provider and the recipient are located in different jurisdictions.

- Transparency and clarity regarding regulatory requirements;
- Regulatory approaches to facilitate cross-border transactions; and
- Consumer protection.

GREATER REGULATORY TRANSPARENCY AND CLARITY

7. In addition to the technological costs impeding cross-border services, several Roundtable participants included understanding and complying with differing regulatory structures as a legal cost. According to these participants, any discussion of the costs of providing cross-border financial services must include:

   - The costs associated with having to acquire a good understanding of the legal and regulatory regimes of foreign markets, in order to mitigate legal and regulatory risks; and
   - The compliance costs associated with having to observe regulatory requirements in different markets (e.g. multiple licensing fees, different disclosure requirements *etc*).

8. To mitigate these costs, several Roundtable participants called for *greater regulatory transparency and clarity*. These participants suggested that regulators should spell out their regulatory frameworks more clearly to financial service providers located outside a particular jurisdiction so that these providers could more easily and more thoroughly understand their regulatory obligations.

9. Most of the risk and concerns surrounding cross-border issues relate to uncertainties and unfamiliarity with differences in the legal and regulatory regimes in different jurisdictions. Regulatory rules may not be consistent across jurisdictions – for instance, the definition of what constitutes a "sophisticated investor" may differ across jurisdictions. Different jurisdictions may also have different definitions of products (e.g., that of "securities") or regulated activities, which may consequently result in different regulatory treatment for the same activity. Another example cited would be what constitutes "solicitation" – in some jurisdictions, mere access to a website by residents of a particular jurisdiction could trigger of regulatory requirements in that jurisdiction, whilst other jurisdictions require more active "marketing" by the service providers. The differing definitions of what may be regulated causes confusion to global service providers and their clients alike.

10. Consequently, some Roundtable participants asked for greater clarity and transparency in regulation. This would be useful in facilitating understanding as well as compliance by market participants.

REGULATORY APPROACHES TO CROSS-BORDER TRANSACTIONS

11. Several industry participants argued for a more harmonized regulatory approach across jurisdictions to minimize not merely industry confusion about what regulations apply to them, but also regulatory gaps and arbitrage. There were suggestions for non-prescriptive approaches to be adopted so that they can be more flexibly applied and more readily adapted to changes in technology. It was suggested that the promotion of international best practices by IOSCO would also reduce regulatory gaps and arbitrage.

12. Roundtable participants noted that there exist several different regulatory models that securities regulators could use to facilitate cross-border transactions, including:

Regulatory Harmonization

13. Some Roundtable participants suggested that securities regulators could facilitate cross-border transactions by harmonizing their regulatory standards. Several argued that regulators could consider moving towards harmonization of regulatory standards and practices by first agreeing on the regulatory areas in which there are significant commonalties. In the Asian Roundtable, the varied stages of market developments and structures across different jurisdictions in the Asia-Pacific region were, however, cited as impediments to meaningful harmonization of regulatory standards. Furthermore, the statutory mandates of securities regulators are established by national legislatures, frequently making regulatory harmonization impossible without legislative harmonization. It was also suggested that industry could itself ameliorate the transactional issues raised by varying regulations in different jurisdictions by adopting the most stringent standard required by regulators on any given matter.

14. Some participants in the Americas Roundtable noted that the lack of national harmonization in some jurisdictions impeded efforts to achieve international harmonization and that harmonization would be meaningless without parity in how the primary markets are regulated.

15. Despite these hurdles to mutual recognition, one Roundtable participant suggested that IOSCO members could work towards this goal through steps to enhance their understanding of each other's regulatory regimes. The work by IOSCO's Asia-Pacific Regional Committee is one such step.

"Home-Host" Concept

16. Some participants in the Asia and Americas Roundtables suggested a "home-host" regulatory approach for cross-border financial service providers similar to that used in the banking sector. Under such an approach, securities regulators would reach arrangements with each other by which these regulators would partition among each other certain regulatory functions where cross-border intermediaries are concerned. These intermediaries would then be subject to only one set of regulations when operating in either jurisdiction. In order to assist making such regulatory allocation of responsibility, participants at the Americas Roundtable suggested that more thought should be given to define the regulatory interest in specific issues and how those issues relate to oversight.

17. However, as with regulatory harmonization, statutory mandates established by national legislatures may limit the authority of securities regulators to delegate these responsibilities to their foreign counterparts. Furthermore, unless the regulatory structures were very similar, a home-host approach could promote the very regulatory arbitrage it is designed to counter.

Mutual Recognition

18. Some Roundtable participants, particularly in Europe, proposed securities regulators adopt a mutual recognition approach to regulation. Under this approach – an example of which is the European Union Passport system – a group of jurisdictions reach an agreement by which each jurisdiction recognizes the regulatory oversight of the other jurisdictions. This mutual recognition permits intermediaries licensed and regulated in one jurisdiction to operate in the others without being subject to additional or competing sets of licensing and regulatory requirements.

19. Several Roundtable participants suggested extending of the EU passport approach to other jurisdictions. These participants proposed that IOSCO could play a role in facilitating this, or other forms of multilateral recognition schemes. Other participants, however, noted that the EU jurisdictions share a common legal system and common overarching institutions such as the European Commission, European Court of Justice and other EU-level entities, making mutual recognition feasible. Mutual recognition could be difficult in jurisdictions that do not share such an overarching legal system.

Creation of Safe Harbors and a "professional" regime

20. At the Americas Roundtable, participants suggested that regulators could facilitate cross-border transactions by creating "safe harbors" that would specify what conduct could and could not be done and make such requirements as transparent as possible. Others suggested that lack of common regulatory definitions – such as differing meanings and regulatory requirements with regard to "institutional" and "sophisticated" customers – is a barrier to cross-border transactions by global firms. Participants urged regulators to adopt common definitions if possible.

21. Implicit in the call by some participants for common definitions of "institutional customer" is the recognition that there are reasonable distinctions in the ability of customers to take care of themselves in the marketplace. Some participants noted that in approaching a regulatory issue regulators should adopt a "risk-based" approach and look at the qualities of the customer, the type of product and where the securities or margin are held in deciding how to apply the regulatory framework.

INVESTOR PROTECTION

22. Another main concern of cross-border transactions relates to investor protection. Roundtable participants agreed that regulators need to identify the additional or unique risks arising from cross-border activities and institute appropriate measures for the management or reduction of these risks Securities regulators need to satisfy themselves that they have sufficient mechanisms in place to ensure adequate and proper regulatory oversight of intermediaries who offer securities services from overseas jurisdictions.

23. Roundtable participants, however, also agreed that investors invariably face additional risks in a cross-border environment, and should be made aware of them. They need to understand the differences in regulatory standards between their home jurisdiction and the foreign jurisdictions in which they invest in order to be able to make informed investment choices.

24. The Roundtable members agreed, therefore, that the challenge for regulators is to educate the investing public on the additional risks of trading via the Internet in a cross-border environment, and to do so without being overly prescriptive to the extent of unduly restricting the use of the medium. Participants in the Americas Roundtable suggested that enhanced disclosure – such as to the allocation of regulatory responsibility in a given transaction – was an essential element of customer protection.

RECOMMENDATIONS

25. IOSCO members should strive to make their regulatory frameworks transparent and clear to all market participants.

26. IOSCO members should consider the fact that Roundtable participants repeatedly drew attention to the issue of barriers to cross-border transactions

27. Regulators should play an important role in educating consumers on the specific risks of cross-border transactions.

28. In general, regulators should try to encourage flexible, non-prescriptive approaches so that regulation can adapt to the rapid changes in technology.

IV: Investor Education

1. Recent statistics and new evidence presented by participants at the three IPT Roundtables indicate that investors are increasingly turning to the Internet for investment purposes, including for online trading, information and investment-specific research, general communication, and portfolio monitoring.

2. In the past, many retail investors, working through full-service brokerage firms, used investment advisers as well as brokers in deciding on where to invest. The migration to discount online brokerage services may encourage investors to trade without the advice of an investment adviser or broker. However, the Internet has not removed the need for informed decision making and research, things that, in the past, investors may have received with the assistance of professional advice. As investors increasingly make their own decisions, they require knowledge about the products they are purchasing online and the inherent risks these products pose. For investors who use the Internet to research their investment options, understanding that not all information available over the Internet is objective or accurate is critical to making informed investment decisions. Investors will also want to know how they can use the Internet effectively as a research and investing tool.

3. Complicating the task of investor education, the global nature of the Internet means that consumers may access the web-sites of providers in other countries whose products may not be accompanied by familiar forms of disclosure and risk warnings and which may have a complex structure that give rise to unfamiliar risks.

4. Given the importance investor education has for investors using the Internet to trade and research securities, each of the IPT Roundtables included a session where participants discussed ways to improve investors' understanding of the risks and benefits of using the Internet as part of their investment decision-making. The participants of the IPT Roundtables identified a number of investor education issues they believe require a response from industry, consumers and regulators. This paper summarizes the issues identified at the Roundtables:

ISSUE: EDUCATION

5. Industry participants held a number of views with respect to investor education. The main challenge with respect to investor education, several participants suggested, is to motivate consumers to use the resources and information that is developed. Many investors do not take the time to learn about the implications of their financial decisions before they are made. Participants agreed that while investor education cannot be mandated, there are many strategies available that could boost investor interest and engagement in investor education resources, resulting in better-informed investors.

6. Roundtable participants outlined a number of principles they believe would lead to successful investor education that would be useful to investors. They stated that objectivity is important and that regulators are in a good position to provide objective education.

7. Many participants noted that there is a huge amount of information currently available to investors. But, the quality of that information must be at a level that addresses the different needs of different investors. Educational resources should be at a length, depth and language acceptable to consumers. Just as important, the content of these resources should be clearly and compellingly written and presented — the message of investor education will be lost if it is not presented in an interesting fashion and in the "plain language" that

non-specialists will understand. The challenge is how to get investors to use the information available and to help them identify and separate "good" information from that which is potentially false, misleading or irrelevant. Furthermore, investor education must be engaging to all investors needing this information in order to gain and hold their attention. "Edutainment" may be one solution by which investors can be "enticed" to them to learn through interactive tools whereby investors "learn by doing" in fun and interesting ways.

8. One participant also argued that, in that individual's experience, an investor's understanding of the risks an investment poses cannot necessarily be inferred by the value of his or her assets. This participant suggested that high net worth investors can be just as lacking in the knowledge they need to make informed investment decisions as novice investors.

9. Roundtable participants had a number of suggestions that would help to motivate investors to learn from objective investor education programs:

   - Because online investors get their educational information in places other than the Internet, educators should use traditional mediums as well as the Internet to distribute key messages and educational information. Organizations wishing to alert the public about the risks involved in relying on information obtained from the Internet should consider using channels of communication that have the widest scope of circulation, such as newspapers, magazines, radio and television.

   - Educators should attempt to reach investors at the "point of sale." One of the best times to provide investors with investor education materials and resources is at or just before the point where they make an investment decision — in other words, precisely at the time when they may be in most need of and most receptive to this information.

   - Investor education tools and websites developed by regulators need to be state-of-the-art and keep up with technology to compete with information provided by industry websites and other information found on the web. They also need to be dynamic, properly maintained and timely. Regulators should avoid the "dusty brochure syndrome", i.e., simply posting a print brochure online.

   - There needs be full marketing and promotion plans developed for educational websites in order to raise awareness of the resources and increase usage. Creating public awareness about scams and frauds and generally warning investors about various strategies used by scam artists is an important role for regulators. Creating awareness of the role of regulators is also important.

   - Media need to be engaged to market the message and let investors know what investor education tools are available to them.

10. Roundtable participants agreed that better-informed investors have more confidence in their abilities to make decisions and work with financial intermediaries and, thus, more confidence in investing the capital markets themselves.

Regulator's Role in Education

11. Many regulators have identified the investor education needs of both online and traditional investors and often take a role in investor education and awareness, thereby helping to proactively protect investors from the risks of using the Internet for investment purposes. The Roundtable participants agreed that there is an important role for regulators in the provision of investor education and they believe that regulators should step

up their efforts in this area. Specifically, Roundtable participants stated that regulators should provide novice investors with simple (easy to use and plain language) tools and resources that address the following areas:

- Basics

  Roundtable participants suggested regulators should help investors understand the basic fundamentals of investing including the various product choices investors have and the value of diversification. Youth in high schools should be targeted for basic information through curriculums to prepare for their transition to financially-aware adults.

- Risk

  Roundtable participants also suggested that regulators should educate investors about various types of risk. This includes the risk of using poor or biased information as well as the traditional type of investment risks such as market risk, inflation risk, credit risk etc. It was suggested that investors do not understand risk properly, often leading to inappropriate investment decisions. More typically, investors resist 'learning' about the risk/reward relationship stressing that they want zero risk and a 25% return.

- Regulations

  Several roundtable participants believed regulators should encourage the general public to learn about the securities laws and rules and regulations in place to protect them. According to these participants, if investors know about the requirements imposed on the industry, they will help in policing the industry by asking the right questions and identifying gaps in compliance. If they know that brokers need to be registered to sell securities and that it is easy to check registration, they will check – protecting themselves from unlicensed scam artists.

- Rights and Remedies

  Roundtable participants believe regulators should encourage investors to become aware of their rights and remedies in the event of a complaint or a problem with an investment or an intermediary.

- Dealing with Licensed Intermediaries

  Regulators should educate the public in how best to deal with a licensed intermediary (how to choose an advisor, working with an advisor such as questions to ask, qualifications, experience etc., registration requirements to look for and client's responsibilities like checking statements, informing advisors about changes in their financial situations).

Industry's Role in Education

12. Roundtable participants believed that industry also has a role in investor education. Industry participants should develop their own resources, which could include alerts, checklists or reminders of the measures that should be taken in order to make an informed investment decision. In addition, industry should use information that is up-to-date and accurate on their websites. They should monitor the accuracy of the content of their websites on a regular basis. (See below for discussion on standards/trust-marks.)

13. The participants noted that more product distributors are developing investor resources. Investment firms are increasingly offering analytical tools, asset allocators and calculators to help investors with their decision-making process. In addition, financial adviser associations and dealers are offering lists of available advisers

online. Other Roundtable participants pointed out that industry sources of information may be useful but are not completely objective. Regulators' information could be provided on industry sites as well and industry could offer hyperlinks to investor education developed by regulators. This type of hyperlink could be encouraged but disclaimers that state that the regulator is not endorsing the industry site would need to be provided. Intermediaries should be encouraged to cooperate with colleges or learning institutions to have online investment education courses on their websites.

Consumer's Role in Education

14. Several Roundtable participants stated that consumers often claim to know more about investing than they really do. These participants asked whether regulators and/or consumer associations could develop a "financial driving test" so people could evaluate their knowledge level before making decisions. Regulators could help facilitate this by working with consumer groups. Consumer groups should be encouraging their constituents and members to learn about the potential repercussions of their financial decisions.

RESEARCH ON THE NET

15. Those attending the IPT Roundtables agreed that investors should know the source and reliability of research, information and "educational resources" they find on the Internet. Many investors turn to Internet discussion sites or chat rooms for tips on stocks. One obvious problem is that the information on these chat lines may be unreliable. There are an increasing number of examples of how these types of communication vehicles are used to disseminate false and misleading statements about stocks and markets and many jurisdictions have brought enforcement actions as a result of stock manipulation on Internet chat lines.

16. According to Roundtable participants, educational needs surrounding information from the Internet include:

    - Investors should be educated about the ease by which information can be falsified, manipulated and quickly disseminated via the Internet. Consequently, investors should be encouraged to check all sources and verify information with trusted third parties.

    - Investors should to be educated about any fees Internet portals are receiving and the involvement of the portal with the broker/dealer. Investors should know the pros and cons of dealing with a portal and realize that they are being referred to sources that may not be objective. When portals connect investors with content provided by third parties, they may be perceived to be endorsing specific securities even where this is not intended. Investors should also know that portals may track their personal information and provide it to the broker/dealers with whom they are linked.

    - Financial consumers need to be educated on how to validate research and information found on the Internet. Regulators could develop tools such as online registration or filing research websites similar to SEDAR, EDGAR or SOPHIE to help investors conduct research over the Internet more effectively. Consumer and investor groups could promote those tools to their members.

    - Reminders should be given to investors to validate information obtained from the Internet with approved licensed intermediaries before making an investment decision.

SUITABILITY

17. Roundtable participants also discussed the various ways jurisdictions approach "suitability." As a general matter, there are two broad ways in which consumers may be protected from making investment decisions that are not suitable for their circumstances. One is to ensure that accurate information is available about an investment and that consumers are able to apply their knowledge of the product to their circumstances. The other is to impose a regulatory requirement on intermediaries to determine the suitability of an investment for a particular investor. There are considerable differences in how jurisdictions approach this issue. Country practices towards execution-only business tends to fall into four broad categories:

- Jurisdictions in which intermediaries are required to determine suitability in respect of each transaction;
- Jurisdictions in which intermediaries are required to conduct an initial suitability test to determine the client's risk profile; so long as the client keeps within that profile the broker dealer does not have to consider the suitability of each buy or sell decision made by the consumer;
- Jurisdictions in which the consumer determines his or her own risk profile and also decides whether a transaction is suitable for his or her circumstances;
- Jurisdictions in which the consumer is free to make his own decisions within the framework of the client agreement.

18. The second, third and fourth approaches all place the onus on investors to know about the investments they are choosing. The third and fourth options, in addition, place the onus on the consumer to decide the various investment strategies that should be considered when making investment decisions, such as diversification, asset allocation and risk/return relationships. There was some discussion that regulators should encourage intermediaries to provide tools, or provide tools themselves, which would help investors monitor their risk tolerance levels. Some firms offer tools that enable consumers to assess their own level of risk and then to monitor their portfolio in relation to their stated risk appetite. Tools such as these are likely to play an increasingly important role in helping consumers to construct a balanced portfolio.

MONITORING STANDARDS / TRUST-MARKS

19. During the Roundtables, there was a great deal of discussion about who, if anyone, should monitor investor education materials provided over the Internet, if standards should be set and if trust-marks or certification marks have a role to play in validating investor education. It was suggested that consumers, industry and regulators should all be responsible for monitoring investor education resources on a regular basis to confirm that what is placed on websites is not false or misleading.

20. As such, participants argued that the financial industry should to be involved in raising the bar on investor education on the Internet as its reputation is hurt by those who commit scams and provide misleading information via the Web.

21. Similarly, local and worldwide consumer and investor associations may have a role to play in establishing guidelines for conduct and other standards for investor protection that can form the basis for certifications and trust-marks useful to investors. For example, Consumers International, a global federation of non-profit consumer groups, recently conducted an assessment of investment-oriented websites, concluding with a series of suggestions on how businesses should improve the disclosures they make on their Internet sites. Likewise, Roundtable participants suggested that multilateral organizations may also have a role to play.

One example cited was a set of online securities trading guidelines proposed by the Organization for Economic Cooperation and Development (OECD).

22. Taking this one step further, several participants proposed that regulators work together with consumer groups to establish such guidelines or a validation structure. However, it was also pointed out that trust-mark development and monitoring is operationally expensive. If regulators become involved in developing trust-marks, criteria for trust-marks or in certifying materials or courses, there will need to be a consistent monitoring mechanism entailing extensive resources. The logistics involved in such a program could be daunting.

23. Against this background, other participants suggested that a validation system is “wishful thinking” and that “caveat emptor” is more realistic and conveys the message that investors carry some of the responsibility for the soundness of their investment decisions. Consumer group participants, however, although agreeing that investors shoulder responsibility for verifying investment information that comes to them via the Internet, a third-party validation system nonetheless has real potential for boosting investor confidence.

V: Enforcement and Internet Service Providers

1. As the world is increasingly interconnected through the Internet, the Internet also is increasingly being used as a tool to commit securities fraud. Whereas a traditional "boiler room" scam in the past would require a dozen individuals using telephones for many hours just to reach a few hundred potential victims in their own geographic area, a single person using the Internet can now "spam" tens or even hundreds of thousands of potential victims throughout the world in a matter of minutes. If only a small percentage of these individuals respond to these solicitations, the mathematics of fraud can now mean millions of dollars lost and thousands victimized.

2. Furthermore, Internet-related securities fraud is not limited to boiler room scams and spam. Internet discussion boards and websites are also frequently used by those committing securities fraud. Often, Internet Service Providers themselves can be indirect victims, as many individuals who commit fraud over the Internet use false email addresses or "spoofed" websites that can damage the reputations of even those ISPs with strong anti-spam and anti-fraud procedures. Legitimate businesses likewise suffer as the fear of rampant fraud deters consumers from transacting business via the Internet.

3. Of course, securities fraud is not new even if the medium is. However, the fact that the Internet is both relatively new and relatively unregulated poses challenges for law enforcement authorities. The IOSCO Internet II Report concluded that some of the difficulties securities regulators now face might be eased through a dialogue with Internet Service Providers (ISPs) and others in the Internet "industry." Greater awareness by securities regulators of what ISPs do and are capable of doing might assist regulators in prosecuting those who defraud investors via the Internet. In turn, ISPs might learn more about how securities frauds are perpetrated over the Internet, how they can better assist law enforcement agencies, and how they can better protect their customers from Internet securities fraud. ISPs and others in the Internet and high-tech industry were invited to the IPT Roundtables in an effort to facilitate this dialogue.

KEY ISSUES

4. Roundtable discussions regarding securities law enforcement and ISPs centered on four key issues:

   - The availability to regulators of various kinds of information that, at one time or another, are held by, originate with, or pass through ISPs;
   - ISP data retention requirements;
   - Privacy issues; and,
   - Educating regulators in how technology can be used to perpetrate securities fraud.

Information Availability

5. As the IOSCO Internet II Report noted, information held by ISPs frequently can be very useful to regulators investigating securities fraud conducted via the Internet. Yet, as a practical matter, such information is only of value if the information (a) is retained by ISPs in a useful form and (b) is legally accessible by the regulator.

6. The Roundtable participants confirmed that these two issues continue to vary by ISP and jurisdiction.

7. Depending on the jurisdiction and the ISP, at one point or another, many (though not all) ISPs maintain traffic data such as user IP addresses, session logs, and user log-on identification information.

8. Depending on the type of service, ISPs may also have access to:

   - Telephone caller identification information (for dial-up services),
   - Subscriber information (including name, address, telephone and other billing information), and
   - Content information (the content of emails, bulletin board and chat room postings, etc.)

9. However, as discussed below and in the IOSCO Internet II Report, ISPs vary considerably in the degree to which they retain such information and for how long, and regulators vary by the degree to which they are knowledgeable about ISP data, and whether they can obtain this information from ISPs and share it with their IOSCO counterparts in other jurisdictions.

Data Retention Requirements

10. In contrast to the record-retention requirements widely imposed on market intermediaries (for example), many jurisdictions do not mandate how long ISPs must retain traffic, subscriber or content information, or else impose a retention requirement only if a law enforcement agency or court formally issues a retention order. As discussed below, some jurisdictions even place strict limits on how long ISPs may retain information in order to protect the privacy of ISP subscribers.

11. As a group, Roundtable participants expressed three different – and not entirely compatible – opinions regarding the role securities regulators should play with regards to establishing legal ISP data retention requirements. Many industry participants opposed the suggestion that regulators create data retention requirements, claiming that data retention technology is expensive and hiring compliance staff prohibitive to firms in an industry where many have fewer than 20 employees and some as few as five. On the other hand, other Roundtable participants welcomed data retention requirements as offering ISPs guidance on how long different types of information should be kept – provided, these same participants noted, that these requirements sheltered ISPs from civil liability resulting from potential breaches of privacy laws.

Privacy Issues

12. Roundtable participants also noted the inherent conflict between the information needs of securities regulators and other law enforcement authorities, and legitimate concerns over privacy. Some participants noted that the privacy laws in some jurisdictions require ISPs to destroy customer information once that information is no longer needed for business purposes. Similar privacy laws can limit the legal authority a securities regulator may have to request or compel ISPs to produce such information – and, as a necessary consequence, also limit the ability of a securities regulator to share such information with foreign counterparts.

Training Regulators

13. Several roundtable participants also suggested that global securities regulators should consider specialized training for some members of their enforcement staff. Greater technology training will enhance the abilities of securities authorities to investigate and prosecute securities fraud conducted over the Internet. Greater

technical knowledge and skill will also enable fraud investigators to request the most relevant information from ISPs and other companies that may have records that can be of use in an investigation.

ADDRESSING ISP AND ENFORCEMENT-RELATED ISSUES

14. Roundtable participants discussed a variety of approaches regulators, ISPs and investors might consider when addressing securities fraud conducted via the Internet. These approaches (some of which were also proposed by the IOSCO Internet II Report) include:

    - Creating an industry-sponsored "Code of Conduct" for ISP data retention;
    - Continuing a dialogue between industry and regulators to better inform ISPs of the types of information regulators need in order to prosecute and prevent securities fraud;
    - Educating investors about how to avoid falling victim to securities fraud via the Internet by, for example, regulators placing warnings on their websites about common scams and advising investors to check the license status and disciplinary history of anyone offering them securities over the Internet;
    - Pursuing legislative or regulatory initiatives that require ISPs to retain subscriber and traffic data that may assist regulators in investigating and prosecuting Internet-related securities fraud;
    - Having regulators seek statutory powers allowing them to compel the production of relevant data from ISPs and share this information with their foreign counterparts;
    - Seeking amendments to privacy laws so as to allow securities regulators to access ISP-held Internet traffic and subscriber data while shielding ISPs from potential civil lawsuits resulting from their good-faith cooperation with securities law enforcement authorities; and,
    - Coordinating proposed ISP-data retention requirements with other law enforcement agencies so that different domestic regulators and agencies do not impose different requirements.

RECOMMENDATIONS

15. As a result of the Roundtable discussion, the IOSCO Technical Committee will consider initiatives to encourage or require ISPs to retain certain data that most frequently proves useful in Internet-related securities fraud investigations and prosecutions. In particular, the IOSCO Technical Committee will consider whether it is advisable for IOSCO members to pursue, separately or in cooperation with other regulatory or law enforcement agencies, legislation or industry initiatives such as codes of conduct to have ISPs retain subscriber and traffic data for a minimum of 90 days.

16. The Roundtable discussions have also confirmed the value of the range of measures available that IOSCO members for improving access to ISP information contained in the IOSCO Internet II Report. Consequently, the IOSCO Technical Committee repeats its recommendation that regulators, individually and collectively, should explore these options in the interest of facilitating domestic and cross-border investigation and prosecution of securities fraud via the Internet.

17. As a consequence of the Roundtables, the IOSCO Technical Committee also alerts its members that specialized technology skills may be necessary in order to investigate and prosecute securities fraud conducted over the Internet. Securities regulators may wish to devote resources to training members of their staff in these skills where Internet-related securities fraud is a problem.

VI: Summary of Discussions[*]

ISSUES	MONITOR	LEAVE TO MARKET	FACILITATE	EDUCATE	REGULATE	IPT RECOMMENDATIONS
I. Industry Trends A. New technology will have impact on use of internet, in particular: • Security • Convenience • Efficiency	• Monitor		• Need for infrastructure and global approach to services levels		• Anticipate changes rather than react to them	Discontinue IPT as standing working group. Developments can be monitored through other Committees and [b] annual roundtables
B. Data • Ownership of data • Access to Data • Linkage of data • Integrity of Data • Privacy issues • Volume of Data		• Codes of Practice • Policies on Privacy	• International Standards and protocols		• Prompt Response to emails by dealers • Greater Transparency • Of information	
C. New types of transaction markets and services • Portfolio management • Bulletin Boards • Aggregation and integration of	• Monitor	• Leave to market			• Anticipate • changes rather than react to them	

[*] This chart reflects a summary of participants' comments and not a consensus

ISSUES	MONITOR	LEAVE TO MARKET	FACILITATE	EDUCATE	REGULATE	IPT RECOMMENDATIONS
services • Credit services • Internet Discussion sites • Broader access to services						
D. Impact on Best Execution E. Greater competition among services and service providers			• Provide greater competition			
II. Emerging Risk Profile • Outsourcing • Time delays • Security risks • System failures • Capacity planning • Aggregation • Lack of time to make corrections • Unauthorized trading • Privacy breaches	• Monitor developments	• Codes of Practice • Develop service level agreements.		• [Educate]	• Require independent auditors • Standards or guidelines for outsourcing	Refer to SC 3 to consider • outsourcing issues • IT risks/security controls
III. Cross-border • Equivalent Regulator • Jurisdiction • Consumer protection • Lack of			• Transparency and understanding of Requirements	• Additional Risks	• Streamlining of requirements • Greater co-operation • Bilateral Arrangements on	• Implementation of IOSCO and common standards should facilitate reducing unnecessary barriers to cross-border services

ISSUES	MONITOR	LEAVE TO MARKET	FACILITATE	EDUCATE	REGULATE	IPT RECOMMENDATIONS
transparency and clarity regarding regulatory requirements • High cost of IT infrastructure					the basis of compatible regulatory structures • Harmonization of rules to facilitate mutual recognition	
IV. Investor Education • Quality of information • Different needs for different investors • Timing (Point of Sale) and effectiveness • Consumer confidence • Quality of websites • Success of investor education – objectivity – no product to sell • Education must be supervised, controlled and labeled • Challenge is to motivate consumers to learn • Content at Appropriate level • Plain language	• Monitor development of trust markets	• Trust mark certificates • Codes of Conduct • On Trustmarks – See Monitor section • Need government, industry and consumer groups to decide on appropriate standards.	• ISO trust mark schemes • On Trustmarks • Hyperlink to regulator’s site	• target novice investors – basic rules, simple tools, need basic fundamentals, education about risks (all kinds) are key (including risk of using poor or unbiased information), educate about protection in place (so they know to check registration), Realize not everyone is online – use traditional promotional tools as well. • Point of sale strategy – reach investors when making decisions • Engage media to market info • No dusty brochure syndrome	• Require financial websites to provide a checklist of information • Certificate of courses and materials. • Criteria for trust marks • Regulators should move to validate content – virtual gatekeeper – certify courses or programs • Should monitor chat	• More publicity about regulator’ websites Content of regulators’ • Develop programs to raise public awareness of risk of fraud. • Develop and maintain attractive, user friendly web-sites

ISSUES	MONITOR	LEAVE TO MARKET	FACILITATE	EDUCATE	REGULATE	IPT RECOMMENDATIONS
				• Cutting edge technology • Marketing and promotion plan • Financial driving license – need to complete risk profile, objectives and experience before invest online		
V. ISPs • Availability of information • Privacy issues • Record retention requirements • Training		• Codes of Conduct	• Co-operation with other authority to determine what is needed with ISP and among government agencies		• Requirements regarding record retention • Legal process for individually identifiable information • Chat-room content	• Refer to SC4 to consider making recommendations for legislation on retention issues • Regulators should develop forensic skills related to the use of technology

GLOSSARY

3G	3G is a short term for third-generation wireless, and refers to near-future developments in personal and business wireless technology, especially mobile communications. This phase is expected to reach maturity between the years 2003 and 2005.
ADSL	ADSL (Asymmetric Digital Subscriber Line) is a technology for transmitting digital information at a high bandwidth on existing phone lines to homes and businesses. Unlike regular dialup phone service, ADSL provides continuously-available, "always on" connection.
ATM	ATM (asynchronous transfer mode) is a dedicated-connection switching technology that organizes digital data into 53-byte cell units and transmits them over a physical medium using digital signal technology. Individually, a cell is processed asynchronously relative to other related cells and is queued before being multiplexed over the transmission path
B2B	On the Internet, B2B (business-to-business), also known as e-biz, is the exchange of products, services, or information between businesses rather than between businesses and consumers.
B2C	B2C is short for *business-to-consumer*, or the retailing part of e-commerce on the Internet. It is often contrasted to B2B or *business-to-business*.
Backbone	On the Internet or other wide area network, a backbone is a set of paths that local or regional networks connect to for long-distance interconnection. The connection points are known as network *nodes* or telecommunication data switching exchanges.
Broadband	In general, broadband refers to telecommunication in which a wide band of frequencies is available to transmit information. Because a wide band of frequencies is available, information can be multiplexed and sent on many different frequencies or channels within the band concurrently, allowing more information to be transmitted in a given amount of time (much as more lanes on a highway allow more cars to travel on it at the same time).
Denial of service attacks (DoS)	On the Internet, a denial of service (DoS) attack is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have. Typically, the loss of service is the inability of a particular network service, such as e-mail, to be available or the temporary loss of all network connectivity and services. In the worst cases, for example, a Web site accessed by millions of people can occasionally be forced to temporarily cease operation. A denial of service attack can also destroy programming and files in a computer system.
Digital certificate	A digital certificate is an electronic "credit card" that establishes your credentials when doing business or other transactions on the Web. It is issued by a certification authority (CA). It contains your name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real.
DRP	disaster recovery plan (DRP) - sometimes referred to as a business continuity plan (BCP) or business process contingency plan (BPCP) - describes how an organization is to deal with potential disasters.
ECN	Electronic Communication Network. An electronic system that brings buyers and sellers together for the electronic execution of trades. It disseminates information to interested parties about the orders entered into the network and allows these orders to be executed.
GPRS	General Packet Radio Services (GPRS) is a packet-based wireless communication service that promises data rates from 56 up to 114 Kbps and continuous connection to the Internet for mobile phone and computer users. The higher data rates will allow users to take part in video conferences and interact with multimedia Web sites and similar applications using mobile handheld devices as well as notebook computers
HOAX	Usually an email that gets mailed in chain letter fashion describing some devastating, highly unlikely type of virus. Hoaxes are detectable as having no file attachment, no reference to a third party who can validate the claim, and by the general tone of the message.
HTTP	HTTP (Hypertext Transfer Protocol) is the set of rules for transferring files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web. As soon as a Web user opens their Web browser, the user is indirectly making use of HTTP. HTTP is an application protocol that runs on top of the TCP/IP suite of protocols (the foundation protocols for the Internet).
I-mode	i-Mode is the packet-based service for mobile phones offered by Japan's leader in wireless technology, NTT DoCoMo. Unlike most of the key players in the wireless arena, i-Mode eschews the Wireless Application Protocol (WAP) and uses a simplified version of HTML, Compact Wireless Markup Language (CWML) instead of WAP's Wireless Markup Language (WML).
ISO	ISO, founded in 1947, is a worldwide federation of national standards bodies from some 100 countries, one from each country
ISP	An ISP (Internet service provider) is a company that provides individuals and other companies access to the Internet and other related services such as Web site building and virtual hosting. An ISP has the equipment and the telecommunication line access required to have a point-of-

	presence on the Internet for the geographic area served.
J2EE	J2EE (Java 2 Platform, Enterprise Edition) is a Java platform designed for the mainframe-scale computing typical of large enterprises. Sun Microsystems (together with industry partners such as IBM) designed J2EE to simplify application development in a thin client tiered environment. J2EE simplifies application development and decreases the need for programming and programmer training by creating standardized, reusable modular components and by enabling the tier to handle many aspects of programming automatically
Logic bomb	In a computer program, a logic bomb, also called slag code, is programming code, inserted surreptitiously or intentionally, that is designed to execute (or "explode") under circumstances such as the lapse of a certain amount of time or the failure of a a program user to respond to a program command. It is in effect a delayed-action computer virus or Trojan horse. A logic bomb, when "exploded," may be designed to display or print a spurious message, delete or corrupt data, or have other undesirable effects.
PDA	PDA (personal digital assistant) is a term for any small mobile hand-held device that provides computing and information storage and retrieval capabilities for personal or business use, often for keeping schedule calendars and address book information handy
PIN	A PIN is a personal identification number. PINs are commonly assigned to bank customers for use with automatic cash dispensers. They are also used, sometimes with a security token, for individual access to computer networks or other secure systems
PKI	A PKI (public key infrastructure) enables users of a basically unsecure public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority.
Slammer virus	This worm virus is being referred to as the SQLSlammer, W32.Slammer, and Sapphire worm. The propagation of this malicious code has caused varied levels of network degradation across the Internet and the compromise of vulnerable machines. The Slammer viras/Sapphire Worm was the fastest computer worm in history. As it began spreading throughout the Internet in January 2003, it doubled in size every 8.5 seconds. It infected more than 90 percent of vulnerable hosts within 10 minutes. The worm infected at least 75,000 hosts, perhaps considerably more, and caused network outages and such unforeseen consequences as canceled airline flights, interference with elections, and ATM failures.
SOAP	SOAP (Simple Object Access Protocol) is a way for a program running in one kind of operating system (such as Windows 2000) to communicate with a program in the same or another kind of an operating system (such as Linux) by using the World Wide Web's Hypertext Transfer Protocol (HTTP)and its Extensible Markup Language (XML) as the mechanisms for information exchange
Spam	Unsolicited e-mail on the Internet.
Spoofing	On the Internet, "to spoof" means to deceive for the purpose of gaining access to someone else's resources (for example, to fake an Internet address so that one looks like a certain kind of Internet user). E-mail spoofing is the forgery of an e-mail header so that the message appears to have originated from someone or somewhere other than the actual source
Spy-ware	Stand-alone programs that can secretly monitor system activity. These may detect passwords or other confidential information and transmit them to another computer. Spyware can be downloaded from Web sites (typically in shareware or freeware), email messages, and instant messengers. A user may unknowingly trigger spyware by accepting an End User License Agreement from a software program linked to the spyware.
SQL	Structured Query Language: is a standard interactive and programming language for getting information from and updating a database.
STP	straight through processing: an automated internal and external trade process from inception to completion without manual handling or redundant processing.
Trojan Horse	A program that neither replicates nor copies itself, but causes damage or compromises the security of the computer. Typically, an individual emails a Trojan Horse to you-it does not email itself-and it may arrive in the form of a joke program or software of some sort.
Virus	A program or code that replicates; that is, infects another program, boot sector, partition sector, or document that supports macros, by inserting itself or attaching itself to that medium. Most viruses only replicate, though, many do a large amount of damage as well.
WAP	WAP (Wireless Application Protocol) is a specification for a set of communication protocols to standardize the way that wireless devices, such as cellular telephones and radio transceivers, can be used for Internet access, including e-mail, the World Wide Web, newsgroups, and Internet Relay Chat (IRC).
WebTrust	WebTrust is a consulting and certification process for Certification Authorities that reduces certain business risks and provides assurance to customers. A certificate authority (CA) is an authority in a network that issues and manages security credentials and public keys for message encryption. As part of a public key infrastructure (PKI), a CA checks with a registration authority (RA) to verify information provided by the requestor of a digital certificate. If the RA verifies the requestor's information, the CA can then issue a certificate.
Worm virus	A program that makes copies of itself; for example, from one disk drive to another, or by

	copying itself using email or another transport mechanism. The worm may do damage and compromise the security of the computer. It may arrive in the form of a joke program or software of some sort.
WSDL	The Web Services Description Language (WSDL) is an XML-based language used to describe the services a business offers and to provide a way for individuals and other businesses to access those services electronically.
XML	XML (Extensible Markup Language) is a flexible way to create common information formats and share both the format and the data on the World Wide Web, intranets, and elsewhere.