VOLUME II

Chapter IX: An Application of Cyber Risk Management Against Money Laundering and Cyberspace

1. Introduction

To date, that "money laundering is an economic crime" should be recognised by individuals engaged in any financial services worldwide. The perception is, however, likely to vary from person to person, industry to industry or country to country. Unlike homicide or robbery, criminalizing money laundering substantially implies the inability to convince the general public of its illegality. The majority of crimes, which are categorised as economic crime or financial crime, such as insider dealing or breach of trust, often show this propensity to a greater or lesser extent. The grounds for this are: 1) short history since the notion of criminalising those practices is only moderately developed, and 2) considerably little direct impact upon the everyday life of the general public as a result of an economic crime being committed. Money laundering has distinctive characteristics. Nowadays, many financial institutions provide training and education to their employees, about money laundering. Implementing a strict "know your customer" rule is one of those policies. In other words, it is self-defence for financial institutions to protect their financial systems from exploitation by launderers. Nevertheless, without an understanding of its illegality, it is open to question whether any policy can achieve results.

Furthermore, with the rapid development of computer technology, cyberspace has been regarded as a possible hotbed for laundering money. The point is whether or not cyberspace money laundering shares characteristics with its counterpart in the three-dimensional world. If so, it is crucial to clarify the differences so that further appropriate methodologies or policies to fight it can be developed. The aim of this chapter is to explore further the potentiality of money laundering in cyberspace by applying the analyses conducted in chapter I to VI.

2. Money laundering and financial institutions

Money laundering is explained as:

> "[It] denotes any act or attempted act to conceal or disguise the identity of illegally obtained proceeds so that they appear to have originated from legitimate sources. "

The International Criminal Police Organization (ICPO) adopted this definition originally, and then the United Nations Office for Drug Control and Crime Prevention (ODCCP) also introduced it in its "Model legislation on laundering, confiscation and international cooperation in relation to the proceeds of crime" published in 1999[722]. Equally there have been other

[722] Model legislation on laundering, confiscation and international cooperation in relation to the proceeds of crime is designed for countries that are willing to enact or modernise anti-money laundering law. See 'United Nations Office for Drug Control and Crime Prevention (ODCCP), Global Programme Against Money Laundering',

countermeasures against money laundering considered by the many different organisations concerned, such as the Council of Europe, Financial Action Task Force (hereinafter "FATF") and the OECD since the late 1980s. The UN International Drug Control Programme (hereinafter "UNDCP") estimated illegal drug trafficking reached about $400 billion a year worldwide in 1998, rising to $1 trillion a year thus far[723]. This illegal profit is considered to be laundered. It is said that the volume is estimated at two to five percent of the world's gross domestic product[724]. If the impact of money laundering is so enormous, what could be the reasons for it being so obscure and unappealing to the general public? The potential reasons are, firstly, whether illicit money is US$400 billion or 1 trillion, it is recognised as proceeds of drug trafficking or other such offences. Hence, money laundering is merely a secondary outcome. In fact, money laundering was initially criminalised in its relation to the fight against narcotic problems. Many countries, which are keen to fight money laundering, have successfully implemented anti-money laundering regulations beyond the level that the first EU Directives required. They have already covered a wider range of predicate crimes than drug trafficking, which the first EU Directives obliged its member states to follow. Unlike the first Directive, the proposal of the second EU Directive shows the extension to all serious offences[725]. That is to say that money laundering is an extension to drug trafficking or other serious offences. Indeed, "illicit gains" being generated as a result of any unlawful offence or activity, such as bribery, corruption, organised crime or financing terrorists, is laundered. Recommendation 4 of the revised version of the Forty Recommendations clearly places importance on urging each member country to 'extend the offence of drug money laundering to one based on serious offences[726]. However, nothing has changed the fact that a primary crime must have been committed before money is laundered. Even if a primary crime becomes the centre of public attention, the secondary crime

---

<http://www.imolin.org/ml99eng.htm>. (print out on file with author).

[723] See 'UN General Assembly Special Session on the World Drug Problem', <http://www.odccp.org/adhoc/gass/ga/20special/featur/launder.htm> and 'Global Programme Against Money Laundering', <http://www.odccp.org/money_laundering.html> (print out on file with author).

[724] See 'The Financial Action Task Force on money laundering', <http://usinfo.state.gov/journals/ites/0501/ijee/fatffacts.htm> (print out on file with author).

[725] See 'Proposal for a European Parliament and Council Directive amending Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering', <http://europa.eu.int/comm/internal_market/en/finances/general/com352en.pdf>. 'Second Commission Report to the EUROPEAN PARLIAMENT and the COUNCIL on the implementation of the Money Laundering Directive', <http://europa.eu.int/comm/internal_market/en/finances/general/launden.pdf> and 'Money laundering: EU Directive to be extended', <http://europa.eu.int/comm/internal_market/en/finances/general/launden.htm> (print out on file with author).

[726] The Forty Recommendations was originally published in 1990 by FATF and was revised in 1996. See 'Financial Action Task Force on Money Laundering, The Forty Recommendations', <http://www1.oecd.org/fatf/40Recs_en.htm> (print out on file with author).

of laundering scarcely attracts the same public attention.

Secondly, the huge impact of economic crime is in inverse proportion to the amount of public attention it draws. The said proceeds of crime, equivalent to two percent of the global GDP, is far too exorbitant to give the majority of people more than an indistinct impression. In other words, not only money laundering but also economic crime in general lacks direct substantial or material damage to impact the public psyche. In fact, most economic crime is committed against either firms or society, not individuals. As a consequence, an individual would not recognise the victim of economic crime which has been committed, even if a firm which one belongs to or society as a whole suffers from it. For example, a case of bribery and corruption is most likely to be committed when person X wants to be facilitated to pursue a specific purpose by person Y. A bribe, for instance of £1 million, is given from X to Y. This money belongs to X, and technically no one would be harmed by this activity. However, it is clear from any political corruption case that the activity definitely harms a sound economy or society, and produces strains and kinks.

Thirdly, money laundering is an intricate story to understand. There used to be nothing strange in the question "why is money laundering illegal?" even from a person engaged in law enforcement. There is no definite answer to this. Perhaps it is because, as mentioned in the first place, money laundering cannot be criminalised alone without a predicate crime. No one denies the illegality of a predicate crime, such as organised crime or corruption, or that the money involved is unlawfully gained. Some people apparently cannot find a connection between these facts and criminalising money laundering. Their theory seems to be that "money is money" even if it belongs to a criminal. In reality, there is no visible taint to stigmatise such ill-gotten money — the face value of a bank note cannot be reduced because of its owner.

Then what is the chief purpose in controlling money laundering? What would happen if it were not an illegal activity? The purpose is that it has a strong preventative function to avoid further crime being committed using laundered money. It is possible to say that it is remote or indirect from money laundering itself to some degree. After all, the purpose of fighting money laundering technically does not have to be the prevention of a repeat offence of laundering. As the Second Commission Report expressed, transparency and soundness are principles in financial markets, thus a money laundering offence is very likely to cause instability as markets react against tainted money contaminating financial markets, whether rumoured or true. It also warned that market officials would be corrupted as a consequence of obtaining contaminated money. Once the market's integrity is lost, it would take a long time and tremendous efforts to rebuild[727].

[727] See 'Second Commission Report to the EUROPEAN PARLIAMENT and the

Since the 11th September 2001 tragedy in the USA, many countries have agreed to fight terrorism. One of the countermeasures to prevent further terrorism has been to expose the financing of terrorists and, moreover, to make it difficult for terrorists and their supporters to launder money. It remains, however, irresolvable that these tactics have achieved the maximum result since it is doubtful whether instructions on money laundering are carried out at all levels of financial institutions. It is still doubtful that everyone involved in financial services understands the illegality of money laundering, but the September 11th tragedy has implanted "imminent danger" of terrorism in their collective psyche, accordingly raising consciousness toward money laundering.

As previously mentioned, money laundering inflicts vulnerability on a sound economy. If a financial institution is involved in a laundering process unknowingly, the money, which has been deposited in by a launderer, would eventually be confiscated by the relevant authority. In cases where the institution is knowingly involved in the offence, it would be found guilty and be subject to punishment. This implies not only a criminal or civil penalty being imposed (such as being fined) but also losing a good reputation, being sued by shareholders and so on. For instance, some cases, such as the Bank of New York or the Bank of Credit and Commerce International (hereinafter 'BCCI') proved the huge potential risk that all levels of employees in financial services industry became involved in the laundering of money. To avoid a worse or the worst case scenario, it is critical to implant a right and sustainable understanding to thwart money laundering being committed in the first place. To train employees in the practical means of preventing an offence is the next crucial step. Before pursuing an in-depth analysis on the means for financial institutions to fight money laundering, there is another issue to be discussed: the difference between money laundering in cyberspace and in the material world.

3. The feasibility of money laundering in cyberspace

Since the conception of business transactions in cyberspace became widespread in the 1990s, the possibility that cyber-technology would be abused as a means of committing money laundering has been rumoured. The possibility materialised, and surpassed conventional money laundering offences, with it being remarkably easy to commit an offence without leaving behind any positive evidence at the time. It is crucial to distinguish whether money laundering in cyberspace is practically different from that of the ordinary means and if so, to what extent is it different? This differentiation will facilitate the combat of potential money laundering offences in the future.

COUNCIL on the implementation of the Money Laundering Directive', *supra* n.710.

To begin with, it is an unclear issue as to where the line should be drawn between money laundering in cyberspace and ordinary money laundering. For instance, 'cyberspace' itself is not clearly defined. Moreover, it is unknown whether electronic money transferring technology amongst banks is cyber-technology or not. Having been used by financial institutions for some time, it is not an entirely new business model. It would be imprudent to consider any activity which is described as "electronic" as a business or technology belonging to cyberspace. If that is the case, what is "cyberspace"? Gibson defined it as "a consensual hallucination" and Benedikt stated that "Space, for most of us, hovers between ordinary, physical existence and something other[728]." It would be better to understand it by its characteristics than by comparing oblique ambiguous definitions. In general, cyberspace is, at least, a virtual space where a great deal of various information is accessed through computer networks. In addition to this, it must have multi-way vehicles, open to the general public and accessible from anywhere. As it is perceived tacitly by the majority of computer users, cyberspace is simply a space where all types of vehicles are exchanged, such as electronic messaging systems (e-mail), online meetings, the purchase of products by individuals, business transactions and so on. From these standpoints, the said electronic transactions amongst the financial institutions could possibly be interpreted as "a business transaction in cyberspace" in a wide sense although, strictly speaking, they do not meet other conditions such as public accessibility. Is it then possible to commit money laundering through the electronic money transferral system? It is possible, but doubtful, since the said system is used in two or more banks internally to transfer money. It could be possible to say that it is merely a part of the whole banking system and is not an independent method or technology for criminals to abuse solely for the purpose of laundering money. In this situation, is the offence categorised as money laundering in cyberspace? It is unlikely. When a launderer commits an offence, he does not have any intention of abusing a specific system to launder illicit money, but determines to launder through the whole banking system itself. In this case, it should be said that money laundering is committed against the bank and so not especially against the electronic money transferral system.

In this context, "money laundering in cyberspace" should mean an offence committed, particularly by the abuse of cyberspace advantages. In addition, it is necessary that a launderer has the intention of taking advantage of cyberspace. Considering these two conditions, there are two main streams in regard to cyberspace money laundering at present. First, to launder money using electronically issued money (electronic money). This is often called "e-money laundering". The other is any money laundering offence in cyberspace, such as abusing an Internet

[728] See 'Definition of Cyberspace', <http://www.education.miami.edu/ep/michigan/sld011.htm> and 'Identity and the Internet: A symbolic interactionist perspective on computer-mediated social networks', <http://www.buffalo.edu/~reymers/identity.html#intro> (print out on file with author).

banking system or Internet gambling operation, but without digital cash involved. The phrase "cyber money laundering" is sometimes used as a blanket term for all offences.

3.1 E-money laundering

The principal factor used to differentiate e-money laundering from other types of money laundering is the involvement of electronic money (hereinafter "e-money"). E-money has been defined in the European Parliament and Council Directive 2000/46/EC as:

> "Electronic money shall mean monetary value as represented by a claim on the issuer which is: (i) stored on an electronic device; (ii) issued on receipt of funds of an amount not less in value than the monetary value issued; (iii) accepted as means of payment by undertakings other than the issuer.[729] "

In short, e-money is composed of digital signals that have financial values equivalent to paper money, being issued under a certain authorisation. There are technically three types of e-money: the card-based scheme, the network-based scheme and the hybrid scheme between the two. The card-based scheme generally branches out into two different types: an integrated circuit (hereinafter "IC") card type and a stored valued card type. Some famous examples of IC card types, stored valued card types and network-based schemes are, respectively, Mondex and Visa cash, BitCash, and e-cash. An IC card type of e-money literally contains an IC chip which has huge storage capacity. This means that this type of e-money allows big business transactions. It is helpful to understand that it is roughly applicable to debit cards. The differences from using a debit card are, to begin with, money kept in an IC card is transferable from one person to the other, like paper money, by using a specific tool, such as a reader, scanner or Mondex telephone. Then money is withdrawn from a bank account with a debit card whereas an IC card has money on itself. On the other hand, the purpose of a stored valued card type of e-money is for online clearing. One can purchase a stored valued card from a shop and type a printed unique number when one wants to pay for a product or service online. The network-based scheme is solely motivated through online clearing where it is mostly necessary to transfer money from a bank by using specific computer software which has been installed in advance[730].

---

[729] See 'Electronic money directive, Directive 2000/46/EC of the European Parliament and of the Council', <http://141.211.44.49/faculty/rmann/Statutes/ElectronicMoneyDirective.pdf> (print out on file with author).

[730] Mondex has been developed by Mondex International (the UK) and Visa cash has been developed by Visa International (USA). DigiCash Inc. (Netherlands), which had developed e-cash, went bankrupt and Cybercash (USA) has been taken over. Thus it is said that Network-based e-money schemes have not been expanded compared to other schemes. See '*Dai-8-kai Densi-syoutoruhiki to kessai* (Vol.8

Some of the distinct differences between e-money and paper money are, firstly, it does not physically exist and thus is invisible; a receptacle card, to charge and keep e-money on, is visible[731]. Secondly, it is unavailable to spend without the assistance of computers in cyberspace or a specific tool to recognise and/or decipher its signals. That is to say that e-money is not always exchangeable everywhere. Indeed, e-money is not a perfect vehicle at present for the majority of people, although it is very likely to appeal to certain people who may exploit its privileges.

To concentrate on the feasibility of e-money laundering, there are two major advantages to attract launderers to abuse e-money: untraceability and mobility[732]. Most e-money remains anonymous, so it is impossible to trace an initial owner. In regard to its mobility, it obviously has no weight. Nobody would notice if one has only a few pounds or £1 million on one's receptacle card. These advantages save them time and cost in the process of laundering money. Furthermore, it could make it as easy for someone (who is well acquainted with computer technology) to counterfeit e-money as traditionally preparing sophisticated machinery and materials to counterfeit paper money. Since it does not physically exist, the words 'counterfeit' or 'forge' would not be technically correct. All that must be done is to take authorisation from an issuing agency or authority so that it looks as if it is authentic e-money. As an extreme example, hacking through a computer network and altering records in an issuing agency of e-money could work to get real authorisation.

The *Daily News* reported in December 1999 that the Thailand Development Research Institute had alerted its government to e-money transactions being abused as a new channel of laundering[733]. FATF has conducted research on e-money since 1997[734]. Has there been any case of e-money laundering committed in reality? Although DigiCash Inc. published that it had been contacted by individuals in 1997 requesting suspicious transactions such as converting offshore bank accounts to anonymous e-money, it seemed to have rejected the proposal[735]. The

---

E-commerce and clearing systems)', <http://www.zdnet.co.jp/help/ebusiness/08/> and '*Denshi-manê no genjô* (The present situation of e-money)', <http://members.tripod.com/tsurut/rep/e_money.html> (print out on file with author).

[731] See '*Mondex-jikken no nihon ni-okeru jôkyô* (The situation of Mondex test in Japan)', <http://law.rikkyo.ac.jp/98zemi/mondex4.HTM> (print out on file with author).

[732] See 'Electronic Money Laundering: An Environmental Scan' published by Department of Justice Canada, <http://www.sgc.gc.ca/WhoWeAre/PPC/eScan/emoney/emoney.htm> (print out on file with author).

[733] See 'Daily News, E-Money Laundering', <http://www.fitug.de/debate/9912/msg00015.html> (print out on file with author).

[734] See '1996-1997 Report on Money Laundering Typologies', <http://www1.oecd.org/fatf/pdf/TY1997_en.pdf> (print out on file with author).

[735] *The Wall Street Journal* dated 17th March 1997. It is also available online, 'Nations Worry About a Rise In On-Line Money-Laundering', <http://www.monkey.org/geeks/archive/9703/msg00008.html> (print out on file with author).

majority of types of traditional money laundering would be able to be committed in cyberspace through banking systems, international trading, purchasing foreign currency or valuable articles and so on. There is no strong suggestion that paper money is able to be laundered whereas e-money is not.

It is worthwhile examining the specific characteristics of e-money as to whether they have a greater impact upon laundering processes compared to paper money laundering. The anonymity of e-money is one aspect that encourages launderers to abuse e-money payments. Technically speaking, e-money is classified into two categories: whether it is or is not transferable amongst consumers. If it is transferable, the circulation of e-money is very similar to paper money, and it would be circulated amongst more than four different parties; an issuer, an owner, a receiver of e-money, and a third party/parties. An example is an IC card type of e-money as mentioned above. If not, it remains inside a closed network involving the first three parties[736]. In the latter case, it seems possible to trace e-money to discover who the owner is, since only three parties are involved. In terms of laundering money, transferable e-money would make the laundering processes easier. While being transferred amongst several parties, tainted money is turned into legitimate money. It is not, however, that simple to launder e-money because computer security detects suspicious transactions whether e-money itself is transferable or not. In regard to e-money's anonymity, it is explained by the word "privacy". Unlike paper money, it is technically possible to make ownership of e-money clearly identifiable and traceable. E-money would be helpful (for anti-money laundering purposes) to trace and arrest launderers if it were required to show its identity. But, it is against the principles of e-money to do so[737]. To ensure the privacy of a citizen and the integrity of e-money, it must be anonymous and secured.

On the other hand, paper money also remains anonymous. Although it has sequential numbers printed, it is impossible to identify a launderer from paper money being laundered unless an investigatory agency knows exactly which sequential numbers are laundered. Thus, it is not practical to compare the risk factors or e-money carries more risk.

However, there are methods of settlement for e-money which make it secure. It is to encrypt by encoding methods[738]. One of the methods

---

[736] *Nihonkeizai Shimbum* dated 28th April 2002.

[737] It is said that six principles exist for e-money to be kept: independence, security, privacy, off-line payment environment, transferability and ability to be added up or exchanged. See '*Denshimanē no genjyō to mondaiten* (The present situation of e-money and its problems)', <http://www.glocom.ac.jp/users/taiyo/emoney/emoney.html> (print out on file with author).

[738] To explain how big £1 million e-money would be, it is useful to cite a well-explained example introduced in the website entitled electronic money laundering. Suppose there is e-money being encrypted using a blind signature, of which a single monetary unit is £100. Suppose a single unit weighs 100 bytes. If

uses two different keys to encrypt: a public key and a private (or secret) key. A public key, literally being disclosed in public, is used to encrypt and a private key, being kept in secret, is to decrypt it. In short, when being encrypted by the method called fair-blind signature protocol, by using a public and a private key, it makes it possible to track down a launderer who abuses e-money. Under the supervision of a court, a trustee is asked to reveal and break the anonymity of an initial owner of e-money. This method, however, remains imperfect and there are loopholes for offenders[739]. So it is possible to conclude that e-money is potentially more efficient to combat money laundering or any other type of electronic crime. Although the global tendency of e-money is more likely to remain faithful to the said six principles, the issue of the anonymity of e-money remains to be judged, depending on each government's policy.

In regard to the mobility of e-money, this is more problematic than its anonymity. As the earlier example shows, £1 million could be saved in just a single floppy disk. Moreover, nobody could guess a disk contains such a huge amount of money at a glance. Even with the assistance of a computer, it would be indecipherable to identify as money if it were not decrypted. In addition to this, any transaction in cyberspace is in general done in a few seconds, and it would be possible to erase or not to leave a sign of the transaction being done with very advanced computer skills. E-money is very likely to be borderless: it should be exchangeable in any currency unit, particularly in cyberspace. Thus it causes difficulty and drawbacks to investigatory agencies and law enforcement authorities when mobility works with anonymity. This e-money mobility is a remarkable obstacle (compared to paper money) in combating money laundering.

What is the role of financial institutions in e-money business? Financial institutions, particularly banks, are very likely to be involved as issuers of e-money. This is because e-money is always founded on the existence of paper money: For instance, network-based e-money always refers to a deposit in a bank account since e-money is merely a method of payment.

As Hagen interpreted, in terms of the use of a stored value card, it would be unlimitedly transferable in theory whereas, in practice, it is restricted to transfer value either consumers against merchants or merchants against their acquiring banks[740]. Furthermore, the amount on a

---

an offender needs to launder a million pounds, ten thousand units are needed and it weighs about 1 MB. It means only one floppy disk contains £1 million! See '*Denshi manê rondaringu* (electronic money laundering)', <http://member.nifty.ne.jp/psyche/soj/ips09.html> (print out on file with author).

[739] *Ibid.* A trustee is called a judge in the original contexts. See 'Blind Signatures and Fair Blind Signatures', <http://www.csh.rit.edu/~spraguep/crypto/> (print out on file with author).

[740] See 'E-money activities and E-banking: Consequences of e-money for the prudential supervision of financial institutions', <http://www.ee/epbe/en/release/hagen.pdf> (print out on file with author).

stored value card is very likely to be limited mostly to a small amount. However, from the financial institutions' point of view, it is not necessary to limit the maximum amount either on a stored value card or an IC card. After deducting money from one's bank account and transferring value onto the card, if the bank is not the issuer of the card, there is no business concern for the bank if the transferred value is large or small. If a card is lost, stolen or broken, it is solely the responsibility of the card's owner[741]. However, it is a major concern for businesses if an institution is an issuer of e-money. It is not difficult to foresee that the more communication intermediaries are involved in money transactions, the less financial institutions would be required, as a result of increased liquidity. Even if e-money being circulated inside the closed circle (as mentioned earlier, such as a stored value card or network type e-money) and banks remain as issuers, the rise of e-money would change financial systems to a greater or lesser extent unless financial institutions are allowed to issue business exclusively.

On the contrary to all the above discussions, e-money laundering was considered negligible in 1997 by the Group of Ten, and this has hardly changed much since then. The reason was given as:

> "To date, G-10 countries have not seen evidence of [e-money laundering] in connection with electronic money products; if such products come to be used on a large scale, it is conceivable that criminals may seek to explore their potential for transferring illicit funds. (Group of Ten, 1997)[742]"

E-money itself holds other issues which will probably make it an unpopular vehicle of payments. For instance, there is the issue of how certain e-money should be dealt with in cases where the issuing bank goes bankrupt[743]. It is likely to be some time before e-money becomes familiar to the public.

3.2 Other types of money laundering offences being committed in cyberspace

Money laundering offences in regard to e-money were initially discussed in a 1996-1997 report published by FATF. Other possibilities of laundering in cyberspace were explained in detail in the 1997-1998 FATF report. FATF considers three specific characteristics of the Internet as likely to aggravate conventional money laundering:

---

[741] If a bank is an issuer of a stored value or an IC card, it would be responsible to prevent embezzlement of the stored value by someone, or reissue a card for the authentic owner if one's usage of stored value is surely recorded.

[742] See 'Electronic Money Laundering: An Environmental Scan' published by Solicitor General Canada, Department of Justice Canada in 1998, *supra* n.717.

[743] See '*Denshi-manê no genjô* (The present situation of e-money)', *supra* n.715.

(1) the ease of access through the Internet;
(2) the depersonalisation of contact between the customer and the institution, and;
(3) the rapidity of electronic transactions[744].

These characteristics could be both advantages and disadvantages as evident from the previous section. On one hand, they could work as indispensable factors to make worldwide commerce prosper further; on the other hand, they could bring chaos and problems from being abused. Hence, it is necessary to identify weak spots and have countermeasures in the event of an offence being committed. To begin with, it is crucial to establish what types of laundering offences could be committed in cyberspace other than those involving e-money.

The first possible type of offence is the abuse of online banking[745]. The majority of large banks worldwide offer such banking services for their customers at present and, moreover, there are some online-based banks which offer banking services entirely online. The conventional banks offer their online services to their own customers; this means a customer has a bank account before receiving online services. In regard to banks which offer online services only, business is started with a new customer from scratch, without face to face contact. Services offered online are generally more limited than offline services. No brand-new service particular to cyberspace is generally offered; only the method of access differs from the conventional way. So there is no doubt that all traditional types of money laundering offences are possible to be committed in cyberspace. The possibility of an offence being committed against "brick and mortar" banking systems is the same as against online banking systems. However, the frequency of an offence being committed would increase since abusing an online banking system is much easier and quicker than abusing the "brick and mortar" banking system. With online banking, one does not have to go to the bank physically and one can transfer money from one account to another in a minute. This saves time and money[746] and furthermore, considering the characteristics of the Internet, it is impossible to trace signs of a laundering process[747]. If transferring money online to a different jurisdiction, there is politically no

[744] See '2000-2001 Report on Money Laundering Typologies', <http://www1.oecd.org/fatf/pdf/TY2001_en.pdf> (print out on file with author).
[745] See '1997-1998 Report on Money Laundering Typologies', <http://www1.oecd.org/fatf/pdf/TY1998_en.pdf> (print out on file with author).
[746] In Japan all financial transactions charges a fee and one of the advantages of online banking is that a fee is mostly fixed cheaper than doing the same transaction at a bank.
[747] There are technical methods to trace the origin of the computer being used for an offence, for example using 'log files' which record the operation of a computer. But not all servers keep log files, and furthermore, obliging financial institutions to keep log files of all transactions for certain periods would be a huge burden of cost and business operations. See 'Cyberlaundering threats should put all bankers on alert, FATF warns', <http://www.moneylaundering.com/MLAarticles/01Apr5.htm> (print out on file with author).

way to investigate further.

The biggest difference between an online bank and a "brick and mortar" bank is that it is hardly possible to accomplish "Know Your Customer" (hereinafter "KYC") policies. This is a basic policy for financial institutions worldwide to carry out the identification of a customer before actually opening a bank account. All documentation must be checked carefully without exception when opening an online banking account. For instance, in the Japan Net Bank (hereinafter "JNB") — the first online-service-only bank in Japan — a potential customer fills in an online application form and a confirmation letter is sent to them within a few days. JNB has its own computer system, which automatically analyses all online applications to evict any suspicious applicants. If any suspicious applicant names are found, a confirmation letter is not sent. The letter, with a personal seal as well as a proof of identity, must be returned to JNB to be checked manually. If there are no irregularities, a cash card is sent to the customer. For checking online transactions, the said computer system automatically checks, with no manpower involved[748]. Introducing a computer checking system is, in reality, not a trump card for JNB only; many financial institutions have installed a similar or the same system. Although Sumitomo Mitsui Bank has a similar system for checking suspicious transactions, automatically referring to its own database, it remarked that the check is not done on a real time basis[749]. Computer checking systems could be more accurate and correct than manpower only if a database has been updated. Furthermore, a computer does not have the ability to judge whereas a human being has. Therefore, it is critical to be checked manually. FATF remarked:

> "...if an account is accessed through the Internet, there is no human intervention that might help to detect suspicious or unusual activity[750]..."

Many institutes and authorities involved have started to suggest strongly implementing "Know Your Cyber-Customer" policies[751]. There is no doubt that implementing those policies is not a straightforward process.

Any activity that involves a huge sum of money could be a good vehicle for launderers. The second possible offence type is using Internet casino and gambling as well as Internet auctions. The third offence type is infringing intellectual property rights. These are, however, very unlikely

---

[748] The author is grateful to Mr Y. Miyai, President, Mr T. Yoshida, Managing Director, Mr M. Komura, Director of Planning Division, Mr H. Doumen, Group Chief and Mr T. Miyagawa of Planning Devision, Japan Net Bank, for their invaluable comments and advice.

[749] The author is grateful to Mr M. Inoue, Group Chief and Mr S. Yanagi, Vice president of IT Planning Department, Sumitomo Mitsui Banking Corporation, for their invaluable comments and advice.

[750] See '2000-2001 Report on Money Laundering Typologies', *supra* n.729.

[751] See 'FATF experts espouse strict laundering controls for cyberbanking', <http://www.moneylaundering.com/MLAarticles/00Apr2.htm> (print out on file with author).

to involve financial institutions as the initial laundering vehicle.

In terms of casino and gambling, there is no doubt that many casino businesses in their early days were established by gangsters in the USA to launder illicit profits[752]. As anyone can enjoy gambling in an Internet casino with access from anywhere in the world, the gambling business could have a site anywhere, and many casinos are mostly located offshore. According to research published in the report of the National Cybercrime Training Partnership in the USA, there were 300 Internet gambling sites with an estimated revenue between 1997 and 1998 of 651 million dollars[753]. The report also suggested that there were "unscrupulous gambling operators", who were able to steal guests' credit card numbers, alter or move data, or even remove the whole site within minutes to avoid being uncovered or arrested. It is no wonder that both the operators and the authorities concerned get caught up in this vicious circle. Internet auctions are likely to incur the same problems as Internet casinos. As it is clearly mentioned earlier, neither gambling nor running an auction business needs to involve financial institutions since they have offshore bank accounts. However, they use reputable U.S. correspondent banks afterwards[754]. Therefore, it is unavoidable for financial institutions to be influenced by Internet casinos or auctions.

Regarding the infringement of intellectual property rights, illegal profits are laundered while pirated edition of computer software and/or entertainment articles such as compact disks are sold[755]. It sounds odd since selling a pirated article itself is an illegal activity. It is presumably a matter of choice as to in which count a criminal is detected by an investigatory authority. In other words, the choice is which offence would be given a lighter punishment: selling a pirated article or drug trafficking. So a pirated article could be replaced by others, e.g. alcohol, pornography (including child pornography), firearms, psychotropic substances and so on. The critical issue is, as it was discussed in an earlier section, whether an offence is under a certain range of offences or defined as a serious offence controlled by the relevant money laundering regulations. Each country has a different view of regulating offences: in short, selling firearms online is a serious offence in many countries whereas infringing intellectual property rights might hardly be defined as such. If it is not identified as a predicate offence of money laundering, it is not possible to criminalise money laundering as infringement of intellectual property rights.

Analysing all the types of possible online laundering offences

---

[752] See 'Tracking money trails with technology', <http://news.com.com/2008-1082-276078.html> (print out on file with author).
[753] See 'The Electronic Frontier: the challenge of unlawful conduct involving the use of the Internet', <http://www.nctp.org/unlawful1.html> (print out on file with author).
[754] See 'Cyberlaundering threats should put all bankers on alert, FATF warns', *supra* n.732.
[755] See 'The Electronic Frontier: the challenge of unlawful conduct involving the use of the Internet', *supra* n.738.

mentioned above, it is possible to say that almost all of the offences show no drastic difference from traditional types of laundering offences thus far. The fact is that the Internet and its technologies are very likely to be taken advantage of by launderers.

4. What is at risk for financial institutions?

It is very likely to be perceived that the offence of money laundering is one committed against banks. It could also be said that it has, to date, been committed mainly against banks . Investing in stocks or purchasing life insurance could also be a major vehicle of laundering money. For instance, the Japan Securities Dealers Association has its rule against money laundering in its Articles of Association and Fair Business Practice Regulation which propose that its members appoint a person to be responsible for controlling internal administration as well as notifying a relevant authority of suspicious transactions [756] . Moreover, it has appointed the Members Firms Department to deal with money laundering schemes[757]. In terms of the Japanese insurance market, a risk of money laundering being committed against it is likely to be perceived to some degree. JISA Business Support clearly pointed out that a policy which stores premiums is at risk[758]. Then, what type of risk do financial institutions have to fight against in cases of money laundering being committed? The possibilities are said to be classified into reputational and compliance risks[759]. In this context, it is appropriate to apply two categories: operational and reputational risks on the grounds of applying the definition of the Basel Committee on Banking Supervision[760].

There is no doubt that the good reputation of financial institutions is essential and indispensable. Both general public and corporate bodies have keen sensitivity to their business integrity to a greater or lesser extent. A good reputation as a result of keeping a high level of integrity makes running a business easier for financial institutions. However, its nature causes wild fluctuations in response to any social phenomenon and

[756] See Japan Securities Dealers Association, 'The Articles of Association and Fair Business Practice Regulation' (2001) Japan Securities Dealers Association, Tokyo, at 321and 329.
[757] The author is grateful to Mr T. Okada, General Manager and Mr M. Matsumoto, Member Firms Department, Japan Securities Dealers Association for their invaluable comments and advice.
[758] The author is grateful to Mr A. Morikawa, Managing Director, JISA Business Support Co., Ltd. for their invaluable comments and advice.
[759] See 'There is an old saying that "what you don't know cannot hurt you." When it comes to money laundering, nothing could be further from the truth', <http://www.aciworldwide.com/trends/loss_prevention.asp> (print out on file with author).
[760] According to the Consultative Document on The New Basel Capital Accord published in 2001, operational risk is defined as 'the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events' but excluding strategic and reputational risk. Thus, compliance issues could be included in operational risk. See 'Consultative Document on The New Basel Capital Accord', <http://www.bis.org/publ/bcbsca03.pdf> (print out on file with author).

it is difficult and, once lost, it is costly to rebuild credibility. The potential causes of loss of reputation are as follows:

(1) A financial institution fails to detect involvement in money laundering;
(2) an employee is a complicit or principal offender in the laundering process, or
(3) an executive is a complicit or principal offender in the laundering process.

Degrees of impact on each case show differences. The impact on business increases in numerical order. All three of them connect considerably with the matter of compliance, and the two latter cases involve criminality. The more active the involvement in a criminal network is found, the more critically and rapidly reputations are lost[761]. A financial institution is very likely to be involved in litigations. Being involved in litigation gives a financial institution adverse publicity, loss of credibility and incurs criminal and/or civil penalties and results in a weakening of its strength. On top of legal risk, it would face systemic risk[762] if a computer system is abused. Simply put, a financial institution would be likely to be forced to rebuild a more appropriate compliance system and be fined as a consequence of violating the regulations concerned, depending on each jurisdiction. Issues of compliance, legal or system risks are categorised as operational risk. However, reputational risk, especially with this background, cannot be entirely independent from operational risk due to the reason mentioned earlier.

Examining the factual cases, the Bank of Boston was criminally convicted in February 1985. Civil fines of US$2.25 million for the Crocker National Bank as well as $4.75 million for the Bank of America were imposed for failing to report suspicious transactions against the Bank Secrecy Act[763]. To take a recent case, the Bank of New York was deeply involved in committing nine money laundering offences in February 2000. In this case, a former vice president and her husband knowingly committed the offences and it is said that more than $7 million were laundered[764]. The couple pleaded guilty to received $1.8 million in commission although the bank itself avoided having criminal charges filed[765]. The culprits

---

[761] See 'There is an old saying that "what you don't know cannot hurt you." When it comes to money laundering, nothing could be further from the truth', *supra* n.744.
[762] System risk means a loss incurred as a result of failure, suspension, inadequacy or abuse of computer systems internally or externally. So it is different from systemic risk. See '*Yôgosyû* (a glossary)', <http://www.dandi.co.jp/yougo.html> (print out on file with author).
[763] See W. Adams, 'The Practical Impact on United States Criminal Money Laundering Lawson Financial Institutions' in B. Fisse, D. Fraser and G. Coss (eds) *The Money Trail* (1992) The Law Book Company Limited, London, at 374.
[764] See 'There is an old saying that "what you don't know cannot hurt you." When it comes to money laundering, nothing could be further from the truth', *supra* n.744.
[765] See 'Russian money launderers plead guilty', <http://news.bbc.co.uk/hi/english/world/americas/newsid_645000/645717.stm> and

agreed to have $1 million confiscated by paying $500,000 each to be released, and the Bank of New York agreed to have more than $6 million seized from the culprits' bank accounts[766].

In the UK, 23 banks in London (15 British and branches of foreign banks making up the remainder) were shockingly found to be involved in money laundering offences relating to the former Nigerian president, General Sani Abacha, in March 2001. Although the Financial Services Authority (FSA) refused to disclose the name of the banks, it was not impossible for a determined mass media to unveil them[767]. Naturally, no financial institution is confident to disclose any type of penalty being imposed, hence neither the exact penalties nor the admonition are public knowledge. It is, however, possible to infer from the UK regulations what type of penalty could be imposed on financial institutions involved in this disgraceful money laundering case. Apart from the general criminal law, there are specific regulations particularly supplementing the UK financial market, that is to say, the Money Laundering Regulations 1993 and 2001, and the Anti-Terrorism, Crime and Security Act 2001[768]. According to the Money Laundering Regulations, any contravention of the requirements carries a penalty on conviction of up to two years imprisonment or a fine or both as Regulation 5 of the Money Laundering Regulations 1993 (the Regs) requires[769]. Taking another case, a former employee of a bank, Arkin Izzigil was convicted and received two years imprisonment as a consequence of knowingly failing to disclose suspicious transactions in 1998[770]. Penalties vary between each offender depending on how and which regulation they violate. If this is the case, surely one would imagine these penalties have worked as a deterrent to money laundering.

5. The Strengths and Weaknesses of Being Involved in Crime

The draft of the Proceeds of Crime bill remarked that employees in the regulated sector (by the FSA) are expected to exercise a higher level of diligence in daily business than those in other businesses[771]. However, it

---

'Montesinos had accounts at BONY that facilitated his money laundering' <http://www.moneylaundering.com/index.htm> (print out on file with author).

[766] See 'Bank Exec, Husband Admit Laundering Billions', <http://www.apbnews.com/safetycenter/business/2000/02/16/pleas0216_01.html> (print out on file with author).

[767] See 'Banks guilty of laundering', <http://www.marcosbillions.com/marcos/Dictators%20Abacha%20British%20banks_guilty_of_laundering.htm> (print out on file with author).

[768] The general criminal law is intended for all UK citizens, such as the Criminal Justice Act 1988 (supplemented in 1993), the Drug Trafficking Act 1994, the Terrorism Act 2000 and the Proceeds of Crime Bill 2000.

[769] The author is grateful to be given an opportunity to pilot a training programme on money laundering organised by the British Banker's Association. Due to the nature of the programme the details remain anonymous.

[770] See Cabinet Office, 'Recovering the Proceeds of Crime, a Performance and Innovation Unit report' (2000) Cabinet Office, London.

[771] See H.M.S.O., 'Proceeds of Crime Bill: Publication of Draft Clauses' (2001) H.M.S.O., London, at 301.

is still doubtful whether each level of employees in the financial institutions have developed satisfactory knowledge of the prevention of money laundering. Even though employees are well aware of money laundering, if the reporting system is not established, a financial institution is very likely to have a heavy fine or penalty imposed. It is necessary for the financial institutions to catch up to this level of complying with the regulations concerned.

This raises another question. Is the good reputation of a financial institution fatally damaged by being involved in or committing money laundering? Generally speaking, there have been some disgraceful cases in the global financial market. The familiar examples are the BCCI and Daiwa Bank (New York branch) cases; the former bank closed down in 1991 as a result of being involved in significant fraud and money laundering offences. The latter was disqualified from conducting business and withdrew completely from the USA in 1996 as a consequence of illegal off-the-books dealings[772]. However, financial business resulting in such devastating outcomes does not happen very frequently, since the authorities concerned supervise the market and financial institutions. In reality, even a minor misdeed, such as embezzlement, is scarcely reported publicly. A misdeed is more likely to be suppressed and discreetly settled internally. It is difficult to know if the relevant authorities are informed of such cases by the institutions involved. It is said that there is a tendency for financial institutions, particularly in Japan, to choose to settle an insider offence internally (by funds pooled for offsetting in case any risk emerges) rather than purchase an insurance policy to cover the potential loss[773]. No institution would admit this; nevertheless, it seems to be, to some degree, a common attitude worldwide towards the problem.

Contrary to the above discussion, there is a question as to what extent a financial institution would in fact engage itself in retrieving a good reputation once a misdeed is made public. A good reputation can be lost overnight. However, it does not mean hosts of customers would close their bank accounts the next morning. The general public may not bother to close their bank accounts in Bank X and open new bank accounts in Bank Y because Bank X is involved in money laundering, unless they are convinced by fact or rumour that Bank X is about to go bankrupt or be forced to close down by a relevant authority. A corporate body may react very cautiously to protect its public image and reputation. Due to the fear of giving a false image of the firm, it would withdraw the business with Bank X in order not to be seen to be conducting business with the

---

[772] See 'Money laundering: The International And Regional Response' published by Asia/Pacific Group on Money Laundering Secretariat, <http://www1.oecd.org/fatf/pdf/APGBack-1998_en.pdf> and 'Daiwa Bank shareholders' lawsuit a wake-up call for company execs', *supra* n.407, and '*Kabunushi-Daihyō-Sosyō* (The shareholder derivative action)', <http://www.eiko.gr.jp/topics019.htm> (print out on file with author).

[773] The author is grateful to Mr Y. Fujita, Manager of Production & Underwriting Department, Lloyd's Japan for his invaluable comments and advice.

convicted bank or, worse, that it has participated in an offence. This depends on the seriousness of the offence; the less serious it is, the less risk of losing customers. Although there is no strong proof, the 23 banks involved in the Nigerian money laundering case mentioned above were unlikely to permit customer loss. The grounds are that, firstly, no name was officially announced and secondly, most major banks were involved, so there would have been very limited choice available if a customer had wanted to change banks.

An analysis of the transition of the share price of the Bank of New York reveals an astonishing fact. Since, a series of misconducts initially became public, it has fluctuated to a greater or lesser extent, although on the whole, it continued to rise. (Figure 8.1) This case was surely one of the most serious money laundering cases. Even if it had not made a big impact upon the bank's share price, does it mean committing or being involved in money laundering offences harm neither the good reputation nor share price of the bank? In spite of the facts, it is hardly possible to judge that the said offences did not harm either of them. This is because share prices generally fluctuate according to all types of information, involving the speculations of the people concerned. The series of fluctuations might have happened because the bank's compliance would certainly have improved under the supervision of a relevant authority. The fact is that a firm's criminality is merely one factor, and not the only factor to sway a share price.

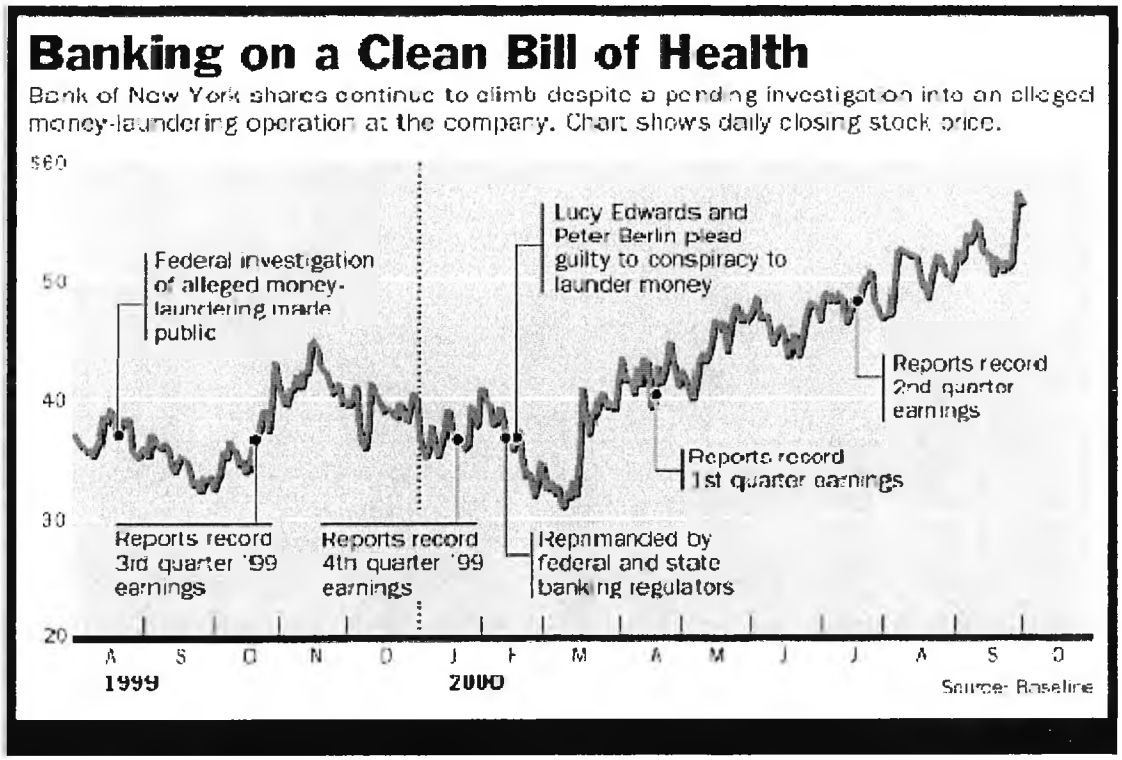


Figure 8.1: The transition of Bank of New York's share price

(Reference: Copyright (c) 2000, Dow Jones & Company, Inc.[774])

Financial institutions are usually reluctant to disclose any misdeed internally or externally. However, once it is public, all types of fears (losing a good reputation and customers, drop in share price) are somehow overcome to some degree. Do they not make efforts to prevent money laundering or other offences? The answer must be negative. Now that Bank X overcomes a fear of losing indispensable things, it should keep up its appearance. In short, Bank X has to show its positive will and steadfast attitudes to prevent money laundering to the general public. Those efforts would work to minimize the loss. For example, the Nigerian dictator's money laundering case mentioned earlier accelerated the finalizing of Wolfsberg principles, wherein 11 worldwide private banks took the initiative to prevent abuse[775]. They are the best practice principles for uncovering money laundering, having progressed for two years since being

[774] The Wall Street Journal dated March 10, 2000. See 'Investors Are Betting That Bank of New York Will Emerge Unscathed From Investigation', <http://www.russianlaw.org/wsi100300.htm> (print out on file with author).

[775] See 'Banks face loyalty dilemma', <http://news.bbc.co.uk/hi/english/business/newsid_1876000/1876126.stm> and 'Are Recent Developments in International Co-operation incompatible with Swiss Banking Secrecy?', <http://www.secretantroyanov.com/Publication/Swiss%20banking%20secrecy.htm> (print out on file with author).

published in October 2000.

Taking all discussions into consideration, it is possible to conclude that no positive reason exists to drive financial institutions to devote themselves to fighting against money laundering. Only the risk of being forced by a relevant authority to close down the business as a result of violating regulations could stop financial institutions' moral hazard. There is, however, a crucial issue for them to deliberate. This is the issue of the proceeds of crime.

6. The Proceeds of Crime and its whereabouts

Suppose Bank X has a customer called Y, who has £10 million deposited in his or her account. If Y is convicted of drug trafficking or money laundering, his or her deposit is doomed to be frozen and confiscated. Aside from whether or not Bank X has noticed it was proceeds of crime, what does this huge sum of money mean to Bank X? The fact is that Bank X is not the owner. It would have been utilised practically and effectively for Bank X's business if it had not been forfeited or if it were legitimate money. Therefore, it is possible to say that Bank X lost the possibility to invest £10 million and make a profit from this investment. This confiscated money is generally supposed to go to the National Treasury after the court gives the confiscation order. It goes, for instance, to Bank of Japan[776]. In the UK, a new agency called the Assets Recovery Agency will be responsible for a series of proceedings when the Crown Court makes a confiscation order (clause 6) if the Proceeds of Crime Bill is approved[777]. As long as £10 million does not belong to Bank X, it has no right to claim to recover its loss. It is technically dubious to use the word "loss", although it could be ideal to express it as "an opportunity loss". It is very unlikely for relief measures to be found for Bank X if it is involved in such a case.

Indeed, the Proceeds of Crime Bill introduces a brand-new negligence offence, which financial institutions would face when failing to report suspicious transactions (clause 329)[778]. If an employee, whether one is an appointed Money Laundering Reporting Officer or not, commits this negligent offence, they would be imprisoned, fined or both, as follows:

---

[776] Here the company remains anonymous by the company's request. The author would like to thank the company for its frankness.

[777] Proceeds of Crime Bill brought from the House of Commons to the House of Lords on 28th February 2002 and continues deliberation. If it is approved, a new agency called the Assets Recovery Agency will exercise control to reduce crime in the UK. It makes the said agency able to confiscate or tax a criminal's assets even if one is not convicted. See 'Proceeds of Crime Bill (HL Bill85)', <http://www.publications.parliament.uk/pa/ld200102/ldbills/085/2002085.pdf> and its explanatory notes <http://www.publications.parliament.uk/pa/ld200102/ldbills/057/en/02057x> (print out on file with author).

[778] *Ibid.*

"329 Penalties
(1) ...

(2) A person guilty of an offence under section 325, 326, 327 or 328 is liable-
(a) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both, or
(b) on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both.[779]"

In addition to this, if a bank or building society fails to comply with the magistrates' court when it orders them to pay the justices' chief executive under a confiscation order, the financial institution involved is likely to pay a fine not exceeding £5,000 as adjudged to be paid by a conviction of the court (clause 67).

In Japan, a person who knowingly receives proceeds of a crime is imprisoned for a term not exceeding three years with labour, or fined a sum not exceeding one million yen (equivalent to £5,882), or both by Article 11 of the existing legislation called the Law for Punishment of Organized Crimes, Control of Crime Proceeds and other matters[780]. The brand-new law, approved on 22nd April 2002, has obliged financial institutions to identify their customers as well as to keep all records for seven years after closing an account (Articles 3 to 5). It imposes imprisonment of terms not exceeding two years or fines not exceeding three million yen (equivalent to £17,647) or both as well as a fine against the corporate body for a sum not exceeding three hundred million yen (equivalent to £1.76 million) (Articles 15 to 18)[781].

Neither paying brand-new type fines nor enduring an opportunity loss for a financial institution must be unfavourably received. Having a fine imposed evidently costs in terms of good reputation besides losing irretrievable business opportunities; thus indicating the critical importance of strengthening countermeasures to prevent money laundering.

7. Countermeasures to prevent money laundering in the financial market

---

[779] The details from 325 to 327 are;
325 Failure to disclose: regulated sector
326 Failure to disclose: nominated officers in the regulated sector
327 Failure to disclose: other nominated officers
328 Tipping off.
See 'Proceeds of Crime Bill (HL Bill85)', *supra* n.762.

[780] See 'Regulations and Documents related to Anti-Money Laundering', <http://www.fsa.go.jp/fiu/fiue/fhe001.html> (print out on file with author).

[781] The exchange rate: One pound sterling equivalent to approximately 170 yen. See '*Kinyû-kikan-nado niyoru kokyaku-nado no honnin-kakunin-nado ni kansuru houritu* (The Law for Financial Institutions Identifying the Customers)', <http://www.fsa.go.jp/houan/154/hou154.html#01> (print out on file with author).

The UK government published that the total cost of crime nationally was approximately £50 billion per annum per annum; nevertheless it is hardly possible to break this down into each type of crime[782]. It goes without saying that the more the cost of is crime reduced, the more the surplus would be beneficially spent, for example, on social welfare and education. Financial institutions are also delighted by not only reducing crime but also taking the opportunity to be involved in legitimate businesses. What type of solutions are available to reduce risks of being involved in money laundering offences? To avoid having a fine imposed, all the institutions have to do is comply with the relevant regulations. It is, however, not simple to comply with the law. Logical and practical reporting systems must be established, as well as known and understood by employees. Clearly a corporate body is responsible for the education and training of its employees to broaden their outlook on money laundering. Different types of knowledge and skills would be required, depending on the level or department to which an employee belongs. As a result, a strengthened sense of responsibility to prevent involvement in an offence and emphasis of the moral aspect should be seen. Having an internal disciplinary panel (in case an employee is involved in an offence) or an incentive system (to appeal to employees' morals and initiatives) could work to reduce risks.

In practice, pursuing a thoroughgoing "Know-Your-Customers" rule (including online customers) is required. The former Dai-Ichi Kangyo Bank (hereinafter "DKB") mentioned that it supports and follows the Charter of Ethics established by the Japanese Bankers' Association, based on enforcing the "Know-Your-Customers" rule[783]. There is no doubt that all private banks in Japan follow the Charter. As DKB stated, it is widely understood that involvement in money laundering offences results in the loss of good reputation, although it is hardly possible to quantify to what extent reputation could be lost. Quantifying a risk would surely motivate financial institutions to fight against money laundering. Nevertheless, it is hardly possible to estimate risks in figures. It is rather more practical for financial institutions to establish effective internal controls systematically. This also includes building up-to-date computer databases which automatically check suspicious transactions. Moreover, considering the possibilities of cyber money laundering, updating technology should command prime importance in the prevention of such offences. The establishment of global standards of Internet banking would help this. Indeed, it is indispensable in order to communicate and cooperate with other jurisdictions since cyberspace is borderless.

---

[782] See Cabinet Office (2000), *supra* n.755.

[783] The author is grateful to Y. Yamaka, General Manager of Global Transaction Services Planning Division and M. Yamaguchi, Assistant to the General Manager of IT Planning Office, The Dai-Ichi Kangyo Bank, Limited (current Mizuho Financial Group), for their invaluable comments and advice. For the Charter of Ethics, see '*Zenginkyô*', <http://www.zenginkyo.or.jp/abstract/katsudou/abstract0406.html> (print out on file with author).

As for the employment of external countermeasures, the purchase of insurance policies could be a measure to reduce the losses of a financial institution involved in criminal offences. However, this type of insurance policy is very likely to be costly. In addition to this, whether a loss is huge or not, it is necessary to report an offence being committed against an institution to both the police and the insurance company if the institution wants to recover the loss. It must be prepared to go public. Pooling money apparently has similar properties to purchasing an insurance policy. However, it is likely to be an imperfect solution as losses increase.

8. Conclusion

To date there is no reported case on cyber money laundering. As previously discussed, its impact is likely to differ from that of conventional money laundering whereas both types are remarkably similar. Money laundering seems to be a significant peril for financial institutions. Although their employees could participate in any criminal activity, the regulations concerned cannot punish corporate bodies. Money laundering regulations have been tightened on a global level and moreover, cyber money laundering certainly suggests it is borderless. It is essential for law enforcement agencies and the relevant authorities in various countries to cooperate with each other as well as to harmonize their legislation.

The relevant authorities do not scrutinize for a chance to take advantage of imposing a heavy fine on financial institutions. But they cannot be negligent in their business in the event of money laundering being committed. It is no longer a fantastic offence: it is a real offence that could happen any time against any financial institution. As mentioned earlier, many a financial institution has already worked issues on money laundering into their basic training for employees. Nevertheless, depending on each employee's place in the hierarchy, the training is very likely to impart minimum knowledge. If importance were placed on keeping a good reputation, it would be practical to raise the level of training up to an advanced level rather than depending on the rank of each employee. Possible penalties and obligatory duties should be fully taught. These would help each employee's understanding of money laundering to be clear so that losing a business opportunity and paying a heavy fine would be avoidable. Moreover, the establishment of a strict reporting system against suspicious transactions is undoubtedly required for financial institutions. The system must not be a halfway measure which could interrupt or stop reporting, intentionally or unintentionally.

Nothing fully protects financial institutions from involvement in money laundering. Even if all employees are good men and women, who do not have the slightest intention of deceiving their employer, a villain from outside a financial institution could target it to launder his tainted money. Constant vigilance is the only way to reduce the risk of financial market abuse by money laundering.

Chapter X: A Recommended Framework of Cyber Risk Management

1. Cyber risk: its worth for financial institutions

For the last couple of years, it is as if the relevant authorities, companies and academics have groped through the fog in search of cyber risk and its solutions. Cyber risk is yet at its dawn. Risks examined thus far are likely to be just the tip of the iceberg. Unfortunately, there are possibilities that a new type of offence or incident would emerge all of a sudden. It might be an entirely brand-new type of risk or offence that nobody has ever imagined. The existing countermeasures and solutions against the existing cyber risk are still under development. Indeed, it is doubtful whether the existing solutions are applicable to a brand-new type of incident or risk.

There is a question: does cyber risk really cause disastrous loss or damage upon financial institutions? "Cyber risk" has been a buzzword and it gives the impression of a serious danger to a business. If materialised cyber risk is not likely to cause any grave loss, it is not worth examining in depth. One of the methods to find out is the dependence on figures. To show the size of potential cyber risk by figures, it proves whether it is worth examining or not. However, it is hardly possible to measure the size of unrealised risk precisely. Even if it is possible to measure it by estimating from a simulation case, the outcome is satisfying only to the researchers. If cyber risk really is materialised, the reality can easily fail to prove the figures submitted by the simulation case. This is because the relevant factors, such as the levels of precaution taken by the parties concerned and the like, vary according to each case. It is dubious that such figures sound convincing. Take the case of Mizuho Financial Group (hereinafter "MFG") as an example. Damages were brought against it due to its serious computer system error; and damages for only four companies reached £59.33 million[784]. Although the MFG has not published the total amount of damages being claimed, it is not difficult to perceive it reaching an enormous amount, including the claims of all companies and institutions who suffered from this critical error.

On the other hand, a year prior to the integration of the MFG in April 2002, the Sumitomo Bank and the Sakura Bank were integrated into the Sumitomo-Mitsui Banking Corporation (hereinafter "SMBC"). Although some system errors have been reported, none of the cases has aggravated the SMBC[785]. Technically speaking, the MFG consists of the Fuji Bank, the Dai-ichi Kangyô Bank (hereinafter "Kangin") and Nihon Kôgyô Bank (the

[784] For details, see Chapter III.

[785] It is reported that the SMBC's automated-teller machines (ATM) had been down for two days in July 2002. Prior to these incidents, the *shinkin-net*, which connects the SMBC with nationwide credit unions, became disabled in May. Both cases were successfully restored at an early stage. See '*Mitsui-Sumitomo toraburu; Seishiki-happyô okureru, jôhô-kôkai ni kadai* (A system error at Sumitomo-Mitsui; the official announcement delayed, the problem of disclosure)', <http://www12.mainichi.co.jp/news/search-news/861311/8eO88e48fZ97F-0-12.html> (print out on file with author).

Industrial Bank of Japan, hereinafter "IBJ"). So, the MFG had to integrate three different types of computer systems whereas the SMBC had two computer systems to integrate. Nonetheless, the MFG case analysis revealed that the series of incidents were caused due to haste of integration without a well-prepared process and procedure. Comparing the size of assets between the two groups, the MFG (150.9 trillion yen, approximately £0.89 trillion) is superior to the SMBC (107.3 trillion yen, approximately £0.63 trillion)[786].

Thus, it is hardly possible to say that the cause was due to financial resources. This shows that the decisions over the whole procedure on system integration decided the outcome. That is to say that it is certain that cyber risk could cause critical losses or damages when being materialised. However, it is possible to avoid, minimise or reduce by taking sufficient precautions, even after the fact. In reality, any risk exists behind a business opportunity. It is a common notion that businesses cannot thrive without taking risk. Indeed, "risk" is just a different name for a 'business opportunity'. Therefore, it is not important to know to what extent cyber risk affects businesses by the exact figures. The essential points are;

(1) to search for all potential cyber risks for examination; and
(2) to take adequate levels of countermeasures to avoid, reduce, and/or minimise the materialised cyber risk.

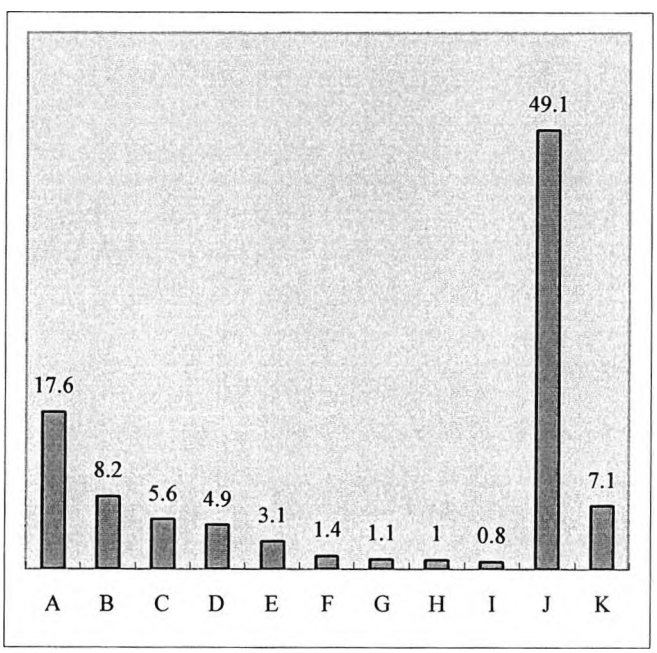
The relevant authorities are also aware of cyber risk. So, financial institutions establishing precautions against cyber risk is favourably received. This is because their concern is the stability of the financial market. It is hardly necessary to explain the gravity of maintaining the financial market's stability. Cyber risk is likely to give rise to system risk[787]. Due to the nature of borderless cyberspace, system risk being incurred by cyber risk may involve foreign factors. Considered from these viewpoints, it is the responsibility of financial institutions to take countermeasures against cyber risk, as good members of society, for the stabilization of financial market. They are, at least, obliged to their shareholders to perform sound business management, as well as to their customers in offering secure services.

It is, of course, the best if cyber risk does not materialise. But if it does, the consequences would be far less for financial institutions if their

[786] Each institution of the MFG had different types of computers and network systems: IBM (Fuji), Hitachi (IBJ) and Fujitsu (Kangin). The situation of the SMBC was almost the same: NEC (Sumitomo) and Fujitsu (Sakura). Each computer system has technically different structures and concepts. Thus, the integration procedure cannot be done easily in a short period. The exchange rate: £1 equivalent to approximately 170 yen.
See '*Biggu 4 Tanjô* (the birth of Big 4 financial groups)', <http://www.rinku.zaq.ne.jp/kazu_san/ginko4.htm> (print out on file with author).
[787] In regard to system risk and systemic risk, see Chapter VIII.

countermeasures successfully protect against losses or damages from such materialised cyber risk. Like the case of the MFG above-mentioned, cyber risk principally devours business funds: it may cause extra expense to fix the failure of computers and the networks, or perhaps damages and legal cost as a result of a client lawsuit. Cyber risk also causes the deterioration of an institution's reputation. Keeping up a good reputation is critical for financial institutions' business. As was discussed particularly in Chapter VIII, it is not always necessary for clients to completely terminate contracts with a certain financial institution that caused a deplorable consequence. This could be because clients do not want to be bothered with changing. It is also possible to say that the good historical reputation, which an institution has built prior to the scandal, could save it from a real danger to a greater or lesser extent. However, it probably works once only. There will be no second chance. In relation to the MFG affair, the online survey of 11,597 ordinary individual Internet users was conducted by the end of April 2002. 40% of the total respondents had a bank account at MFG and only 3% suffered from the MFG affair. Table 9.1 shows what type of action these 3% had taken after the affair. Approximately 10% only took a negative action against the MFG whereas approximately 75% did not take an immediate action.

Table 9.1: What action have you taken since the Mizuho affair?



(A) I did not take any action.
(B) I do not like troubles changing accounts.
(C) An unchangeable account for salary.
(D) I withdrew a part of the deposit.
(E) An unchangeable account for mortgage.
(F) I changed an account to other banks.
(G) I closed all bank accounts.
(H) I closed an ordinary deposit.
(I) I closed a fixed deposit.
(J) Wait and see.
(K) Other.

(Reference: See '*MyVoice: Ginkō no sisutemu syōgai* (MyVoice: computer systems disorder in banks)', <http://www.myvoice.co.jp/voice/enquete/4604/> (print out on file with author).

Furthermore, it is an important clincher for a financial institution how quickly it could take effective actions for both repairing work and retrieving reputation. After it is involved in a scandal, it is very likely to spend huge amounts of money for a reform measure. The quicker the institution takes actions, the more effective it achieves its result.

Regarding the number of users engaged in Internet banking services, it has already observed in Chapter VII that, contrary to the majority of general expectations, the number of users has stagnated. Even if financial institutions appeal by their convenient services, a certain obstacle is too intractable for potential customers and the existing clients who refuse to use the said services. It is security that is always a central issue of cyberspace. Unless the general public is convinced of the services' security, the customer base will not grow rapidly. Although what the Internet banking services can do is restricted compared to the traditional services, it will potentially bring customers closer to the banking services than ever if only it extends the availability. By establishing secure services at present, it will increase customers. This will result in customers being more active in utilising financial services when online services broaden the scope in the near future.

To enjoy successful online businesses, how should financial institutions react against cyber risk? As has been discussed, there are mainly three different types of steps to control it: avoid, minimise the losses of, and transfer cyber risk. This is a threefold protection. By having two contingency plans in reserve to cover all possibilities, cyber risk virtually seems to be controllable.

2. The first bulwark: to avoid cyber risk

Preventing cyber risk from materialising and avoiding materialised cyber risk are two different matters. To pursue the former purpose, implementing compliance programme and thoroughgoing security policies are effective. In addition to these, establishing corporate governance is essential. As noted in Chapter VI, it is crucial to establish reliable compliance programmes and corporate governance. As was previously observed, they are relatively new in businesses. However, it goes without saying that their basic premises are rooted in ethics. In other words, it is global common sense that any behaviour, which is contrary to accepted standards of morality, should be refrained and abstained from in businesses. So, it was, in a way, too late for companies and institutions to perceive the importance of business morality. In a way, it is lamentable that companies and institutions are unable to maintain high business morality without specific compliance or corporate governance guidance from industry regulators or government. It seems an imperative that in order for programmes to be introduced, a framework for compliance and corporate governance must be enforced: otherwise, the private sector either appear at a loss as to the extent of the programs that they should be

introducing, or where they are not at loss, the projects they undertake are designed to conform to minimum or basic standards. Although their principal aim is to avoid risk being materialised, they are also effective to minimise risk after it has materialised. For instance, by establishing the internal reporting systems (directly to the management class) or employing audit systems, it is possible to discover an error or a dishonest act before it gets serious and causes grave losses and damages.

A successful compliance and corporate governance system is, however, mostly effective for internal risk, such as an employee's dishonest act or error and computer failure. They have mere secondary effects on external risk to some degree. To fill this gap, it is of necessity to implement the appropriate level of computer security. This is also to pursue the latter purpose of avoiding materialised cyber risk. Implementing computer security means the policy for the entire organisation involving both administrative and advanced technical means. It is no use without the management of employees and the physical site even if the most advanced technology and equipment is implemented. The difficulty depends on the rapid progress of technology. The relevant steps to implement computer security cost a considerable amount. Due to ever-progressing technology, a brand-new product is constantly lined up on the market and it is not easy, even for a resourceful company, to stay abreast of the latest technology on the market. Moreover, the administration of both employees and the physical site is likely to vary depending on the dogmatic decisions of a person involved in making a policy.

Thus, it is helpful to follow any standard that the relevant authorities or international organisations have published. The most popular standards are the ones published by the International Organisation for Standardization (ISO)[788]. Although there are various types of standards available both domestically and internationally, it is commonly better to employ the standard that the relevant authority or industrial association recommends. The standards published by the relevant domestic authorities are not always updated, whereas the international standards are frequently updated. Furthermore, some of those standards require periodical inspections of the acquired institutions. Thus, rigorous post-acquisition supervision is ensured. In so doing, the whole industry is provided with the same minimum standard. To date, self-responsibility seems to be regarded as common knowledge in cyberspace. This means an individual or institution is responsible for its own Internet transactions. In other words, it is of necessity to implement the minimum level of precautions on computer security (without causing inconvenience for the neighbours), considering the unbounded nature of cyberspace[789].

---

[788] For details, see Chapter VI.

[789] For example, installing anti-virus software is nowadays the minimum precaution for the Internet users.

In theory, having appropriate cyber law is also effective to avoid, to some degree, cyber risk being materialised. The deterrence only works when enforceable punishment is severe. However, even if it is very severe, it remains doubtful whether it deters conceited cyber criminals. Due to the nature of such cyber criminals, even severe punishment could be mere spice to add excitement to committing an offence[790]. Regarding this issue, the problem is, however, not the state of legislation. It is the police and authorities concerned — whether they can discover and arrest an offender.

3. The second bulwark: to minimise the losses of cyber risk

Once cyber risk has materialised, it is crucial to minimise the losses and damages. The most essential and urgent step is to assail the origins of an incident completely. In other words, if the incident has been continuing, it must be stopped immediately. In addition to this, it is essential to take countermeasures to avoid the recurrence of similar incidents. The longer the incident continues to be unsolved, the more it costs an institution, both financially and in terms of reputation. It would not be difficult, in general, to resume the cases caused by computer failures or human errors. If the incident is a criminal offence, legislation criminalizes the offences or wrongful conduct and seeks legal remedy. There are two different legal approaches: by criminal law and civil law.

Criminal law is universally an ex post facto law. It is an outcome of natural consequence that a new type of offence tends to be unpredictable. When a new offence is committed and it is outside the remit of the existing legislation, criminal law comes to be revised or a new independent law is established[791]. So, generally speaking, the revised sections of, or a newly established criminal law is very unlikely to be retrospective to an offence having already been committed. This means that there are difficulties for cracking down on a brand-new type of cyber risk until the relevant legislation criminalizes the act under existing (or new) law. The majority of vulnerable objects of businesses in cyberspace are intangible property. If criminal law expands to protect "integrity" and "availability" of intangible business property even without physical damage, it would be far more effective against cyber crime[792]. This remains to be seen in future legal development.

To globally accelerate the prompt establishment of appropriate legislation up to a certain level, the various international organisations publish conventions and treaties to be ratified by each nation. The problem is that most private enterprises are reluctant to report such incidents to the relevant authorities. This is mainly due to serious concern over loss of reputation by the consequent negative publicity

[790] For details, see Chapter I.
[791] For details, see Chapter II.
[792] *Ibid.*

generated by such incidents. Moreover, the time consuming nature of a criminal case is not attractive for them since there cannot be any commercial merit from pursuing the case. If companies and institutions do not report an offence and conceal the evidence of the crime, cyber criminals will return to attack those who have shown themselves unlikely to report the crime. In addition to this, companies themselves misunderstand cyber risk as being low from the number of incidents reported, which does not reflect the number of hidden incidents and impacts. That would lead companies to negligence regarding cyber risk. It is possible to call this a vicious circle. Companies and institutions must realise that knowingly not reporting a crime is an offence in itself.

One of the means to encourage reporting such crimes is to seek relief measures from civil law. Technically speaking, it is not necessary to seek damages by civil law whether or not an act or behaviour is defined as a crime. It is only necessary that a party incurs losses from another party. Financial institutions are likely to be both a victim and an offender (or an accomplice at least) at the same time[793]. To give an extreme illustration, it is possible for a financial institution to claim damages from an offender, who used that institution as a stepping-stone towards committing a crime, when a third party claimed damages to the institution. Although it claims damages from the offender, the claim is highly unlikely not to succeed, especially when the extent of damage from the crime is enormous. What's more, there are many cases where a cyber criminal is at large. Largely due to the nature of cyber crime, it is unfortunately true that cyber criminals are outside the law's reach to some degree. To reform this tendency, it is of essence to get support from other industries. Tracing electrically left evidence enables the police and the relevant authorities to detect a cyber criminal. For instance, if other industries, such as the Internet Service Providers ("ISP"), cooperate to keep logs for a certain period, it will help detection. Financial institutions themselves also have to do so. Financial institutions are not the only industry that is the target of cyber crime. The cooperation with other industries and the relevant authorities will change the present situation.

When a financial institution is being sued by another party, it is also possible to reduce the potential legal cost and time by using Alternative Dispute Resolution ("ADR")[794]. Furthermore, the decision is basically kept confidential[795]. Indeed, it helps control reputation loss to a greater or lesser extent.

After a financial institution is involved in a lawsuit, it must spend extra funds on clearing its name. Surely it is indispensable to have a contingency plan in case something happens. Prompt responses are crucial for future business, although it is hardly possible to take any action

---

[793] For details, see Chapter III.
[794] For details, see Chapter VI.
[795] Unless both parties agree to disclose the decision, it remains to be confidential.

in a state of confusion without a prepared scenario. Establishing a contingency plan must be included in computer security policy.

4. The third bulwark: to transfer cyber risk to others

The third bulwark, in reality, is positioned between the first and the second bulwark and at the end. This is because cyber risk transferring is able to be included in reducing cyber risk. The countermeasures to reduce risk become effective after cyber risk has materialised. It is not necessary for financial institutions to be aware of cyber risk in advance. Albeit, the countermeasures for risk transferring need to understand cyber risk potential, due to the cost to an institution.

The first countermeasure is to employ insurance products. They are available on the market. Insurance products enable financial institutions to transfer their cyber risk to the insurance market. Using Alternative Risk Transfer ("ART") is, more or less, the same idea[796]. Neither of them is yet a major solution to manage cyber risk. The insurance market expected that liability insurance products would be successful whereas, in reality, they had not yet done so at the time of their market début. On the one hand, it is said that financial institutions have considerable interests in the relevant insurance products. On the other hand, they are highly likely to perceive that the premiums for cyber insurance products are not commensurate with the potential size of cyber risk. In other words, such products are considered to be expensive. There are, financial institutions believe, shortcomings in those insurance products, as was mentioned in Chapters IV and V. Considering this, purchasers judge them as costly. The possibilities to make them purchase are: a serious cyber case happening or any change of or new legislation that inspires them to do so. The former is self-explanatory, while in regard to the latter case, legislation does not have to have a specific section to impose legal obligation on purchasing insurance. It is enough to inspire financial institutions to purchase them if only legislation stipulates responsibility to the institutions for taking precautionary management of cyber risk[797]. This is because if a certain responsibility is set in law, there is also punishment prepared in case of a violation. It is shameful to violate the relevant legislation and this leads to loss of reputation. Thus, this will have an impact on the sales of cyber insurance products.

Employing new technologies (for instance, honeypot) and outsourcing are also effective to transfer cyber risk to others. Albeit, both solutions are likely to produce different type of risks. New technology might not be well examined before being available at the market. Outsourcing can be an efficient solution from the business efficacy and

[796] For details, see Chapter IV, V, and VI.

[797] The author is grateful to Mr T. Matsumura, Regional Manager of Japanese Business Division, AIG Europe (UK) Limited for his invaluable comments and advice.

cost benefit point of views. But it only shifts risk from the institution to another affiliated company.

5. The future of cyber risk: the totalitarian cyber risk management

To enjoy running businesses in cyberspace, it is unavoidable to face cyber risk whether it has materialised or not. Hence, it is of the essence to be aware of cyber risk. It is not enough to perceive cyber risk: financial institutions need to realise that their very own institution is at risk, not other institutions. In addition to this, it is indispensable for combating cyber risk to have an understanding from the whole institution since cyber risk is ubiquitous.

When a third party suffers from any type of cyber incident, it is natural that the party seeks damages from the service providers, in this context, financial institutions. This is a liability issue. If a professional negligence is found in financial institutions, they are very likely to be obliged to compensate the losses of their customers. Even if they have an exemption clause in the contract form and it is in force, if the relevant court judges that it is unfair to follow the clause, the exemption clause becomes invalid. If a financial institution is a pure victim of cyber incidents, the real enemy, who cuts off all relief measures except those dependent on self-financing, is the financial institution itself. By doing this, reputation would be saved once. But if a second incident happens and it becomes public knowledge, the financial institution could be finished or sustain serious loss or damage. Unless criminal law or the relevant regulations impose a penalty on an institution which conceals cyber crime and the like, there is no way but being content with the status quo. After all, it is the decision of financial institutions whether they prefer to accept or reduce cyber risk.

It has been said that boundlessness is one of the peculiar issues of cyberspace. Thus, when an incident happens, it is not always necessary for the parties concerned to have the physical location in the same jurisdiction. To date, cyber court has not established once an incident happens, and when the solution is sought in court, both parties (or their attorneys-in-fact) have to appear in court of the chosen jurisdiction. Unless an appropriate insurance product is purchased, all legal costs are charged to them.

The Basel Committee on Banking Supervision of Bank for International Settlement has not yet finalised its project on revising the Capital Accord[798]. When it is completely finalised, its impact may be likely to promote financial institutions' understanding the potentiality of cyber risk and encouraging precautionary countermeasures. The consequence remains to be seen.

---

[798] For details, see Chapter VI.

The successful risk management methods against cyber risk are like a patchwork of all the different types of methods mentioned thus far. Their combinations vary depending on what type of cyber risk an institution particularly prefers to deal with. Yet the essential issue at this stage is more the perception of cyber risk than the risk management methodologies.

It need hardly be said that there are tremendous potential cyber risks but that these risks are in a sense intangible. This explains why the security of firms and institutions across the world lapse due to misunderstanding of cyber risk or employing defective management methods. Such halfway measures pose the highest threat to cyber risk management. As was proved in several case studies, the majority of cyber risk is caused by an internal outbreak. In the case of MFG above-mentioned, it is possible to say that critical errors could have been avoided if it had made the decision to assign more time and resources to risk management. This is a good example of what happens when the risks are disregarded. It is a grave misjudgement on the part of any firm who perceives cyber risk management as negligible. Cyber risk is something of the joker in the pack; if it materialised, a firm would suffer severe damage. If not, a firm might perceive resources spent to combat cyber risk as wasted. All the proof points to the fact that cyber risk management must be implemented to comply with social duty and corporate responsibility. That being so, some technical management methods (such as strengthening computer security, purchasing insurance) are less prior to reforming and raising management's consciousness about cyber risk. Whether risk materialises internally or externally, without the "green light" and backing of the management, cyber risk management cannot proceed. To survive in these business circumstances, it would be the most critical for a firm to train the management who understands a brand-new type of risk and knows the importance of complying with social duty. It is increasingly critical for firms to have a management that understands this new type of risk to business in order to help ensure their survival.

Chapter XI: Conclusion

Various factors could result in grave losses for people running businesses. This thesis has identified those factors as risks. Once discovered, some risks should be taken very seriously. For example, if a computer on the Intranet has not been updating its computer virus files, suitable action should be taken immediately. Some risks do not particularly lead to a loss or bad reputation for a company. For example, an employee spending time browsing pornographic websites during office hours. Risks are similar to pathogenic bacteria. There are various types of bacteria and it is practically impossible to know if you have caught one. If the bacteria are a newly discovered species and no vaccine is available, serious illness or even death may occur. Computer risks are various and complicated and a factor that poses no risk today may become a serious risk tomorrow. This is usually in relation to a change such as the enforcement of new legislation.

The potential business risks and risk management methods have been thoroughly analyzed. As mentioned in previous chapters, there is no single solution to cover all types of risks: risk management is a patchwork of various types of methods. Therefore, it is necessary for companies to be discerning. Technically speaking, the first step is to investigate the risks that already exist in a company. Secondly, each risk is ranked in order of importance. The company can then decide which methods to apply to their targeted risks by consulting the available budget.

In the business world, the individual risks examined in this thesis are, to some degree, known. However, the risks are not always understood and proper action to avoid or minimize risks is not always taken. Some companies continue to neglect risks even after a full inspection by a professional or internal staff member who has estimated potential losses. It is critical to understand the existence of risks and that risk can cause serious losses, but equally important to know there are methods to minimize such losses. If companies neglect risks without well-grounded reason, they may experience critical losses.

This thesis has examined that financial institutions run businesses full of risks. In particular, providing detailed legal analysis on the risks in business is unique. In relation to the analysis of criminal law, it is practical to understand the legal trend of Britain and Japan by referring to international movements. This leads to an understanding of the legal limitations. Knowing the extent of legal remedy available, helps encourage the private sector to be proactive in protecting their business independently. In the analysis of civil law, all risks have been classified into several types of property. This is an epoch-making analysis for business people, who are not law professionals, to tidy up legal issues. The analysis makes it easy to understand what the problems and legal limitations are. There is, of course, often a legal department in large enterprises. If a company is sued, it is time to work in collaboration with professional lawyers. Staff members with any doubts should be able to

consult the legal department. Even so, it helps ordinary staff to avoid risks before engaging in a new business project if they have some legal knowledge in relation to their own business task.

Although insurance has been the traditional risk management method, research on insurance products spotlights the relatively new and obscure part. When the CCI and its family insurance products were introduced, the product line was considered mainstream. In reality, it is attractive to the market, but there are obstacles to major products. By examining the possibility of the said product line, it would become known to the market. Its popularity would help insurance companies discover solutions to the obstacles that the products hold.

While risk management is a research topic, it is impossible to ignore Information Technology (IT) completely. Strengthening IT security may be the easiest policy, but is also the most adequate method. These days, many financial institutions provide a system audit as part of the standard auditing process. As mentioned earlier, the IT issue has not been analyzed in depth. Amongst the various risk management methods, this issue is the quickest to become outdated: today's technology could be useless tomorrow. Monthly magazines may contain some useful information about the latest technology or facilities available "now", yet constructing a security policy and implementing it is essential. It is highly likely that most companies have very similar policies. The critical issues of the wording are fixed: there is not much room for uniqueness. Moreover, companies are likely to use the same draft policy, published by the related governmental authority, as a guideline.

There are other effective risk management methods being examined. With or without the legal remedy and insurance products, it is possible to choose risk management methods in compliance with the type of risks and financial resources. It is possible to avoid most risks, or at least minimize their impact, by applying appropriate methods. Consequently, this thesis has indicated a framework of risk management methods for financial institutions. Various risk management methods to build the bulwark from risks have also been carefully examined and provided. The only step an individual company has to take to apply this analysis is to decide which method works most effectively for building up the strong barricade against risks.

There is another issue. Technological innovation is unstoppable and in accordance with innovation, the characteristics of risks changes. Moreover, a new type of risk can emerge from out of the blue. The potential loss of a new risk today can be twice as large the next day. Therefore, it is essential to constantly observe risks and be vigilant. This requires companies to have stamina. In other words, to manage risks, a company must have full support and understanding from management. Without this, it is difficult for a company to operate. Nevertheless, this

remains idealistic because there is always a cost to manage risks in the most adequate way. Risk management is not a profitable service since it controls quality of the company itself. It is not realistic to allocate an abundant budget to a non-profitable department (or section) of the company. Financial resources for risk management are generally limited. In small and medium-sized enterprises, it might be impossible to spend enough financial resources against risks, even if the potential risks are critical. In this case, small and medium-sized enterprises have to hope that any risk is not actually realized!

The more business becomes globalized; the impact of risk is widened. Large companies may suffer damages from the realized risks of small and medium-sized enterprises. The reverse case would be disastrous, but risks can never be diminished completely. Thus, it is desirable to develop inexpensive risk management methods.

There is a proper order for implementing risk management into business: to plan, to do, to check and to act. First, it is necessary to examine the status quo of the problems. Knowing the nature of the target makes it possible to make a combat plan. Initially, risk management methods should be implemented in compliance with a trial plan. After the trial, a review is necessary: if the methods used are unsuitable, the plan needs to be revised. At the end of the trial period, the most appropriate methods should be implemented. To date, analysis of existing potential risks has been undertaken, and diverse methods to deal with the risks have been introduced. This means that it is currently between the stages of "plan" and "do". Some risks have existed for ages and others have only been recently recognized. Generally, the style of business operation has recently changed due to computers and the Internet. Managing such risks is still a brand new task for companies. Some companies have started risk management procedures and thus far, they have been through trials and errors seeking the most effective methods to reduce risks. Therefore, it is important to continually review and improve the trial implementation of risk management, and it is worth conducting further research into these areas. It would be particularly useful if the research involved cooperative fieldwork with companies on the reviewing process and developing the most effective risk management methods. A case study of factual risk management within a specific company would be most attractive, not only for researchers but also for the private sector. Any case model would be a good example for other companies.

Risk management should be continuous and vigilant. By repeating the cycle of the aforementioned four phases, the realization of risks would reduce and a sound economy would be accomplished. This research ends with a recommendation to companies or institutions to be proactive against risks, and not to quail before or be ignorant to risks.

End

Appendix

1. On-the-spot survey of CCI products in the Japanese market

1 Questions regarding the development of CCI products
- 1.1 On what size of enterprise did your company focus for the CCI products?
- 1.2 Did your company focus on a specific industry for the CCI product?
- 1.3 What does your company think is the most important issue for CCI products?
- 1.4 On what does your company place the greatest importance, regarding selling the CCI products — property damage or liability for a third party?
- 1.5 Who was involved in measuring the new risks from cyberspace and developing the CCI products?

2 Questions regarding selling CCI products
- 2.1 What types of skills do sales staff need? (I.e. special/technical knowledge?)
- 2.2 Does your company think that the risks in cyberspace are counted as a catastrophe risk?
- 2.3 Does your company think re-insurance is necessary for CCI products? If so, what insurance companies does your company ask to re-insure? (I.e. domestic or international?)
- 2.4 To what extent do the risks increase in a one-year span? How often does your company have to reassess products?
- 2.5 Do you differentiate on pricing by geographic area?
- 2.6 To what extent is it possible to cover losses regarding computer crime?
- 2.7 To what extent is it possible for an insurance product to cover losses caused by employees' dishonesty?

3 Questions regarding the future of the CCI products
- 3.1 How much revenue does your company expect in FY2000 from CCI products?
- 3.2 Is it possible to cover any loss occurred overseas at present and in the future?

4 Others
- 4.1 To what extent does your company compare between its own CCI products and the others?
- 4.2 What does your company think of Internal Controls?

2. Survey topics in the British market

1. History of the British market
2. Traditional insurance products
3. Perceived cyber risks
4. Products line in relation to cyber risks
5. Coverage of those insurance products

6. Limitation of those insurance products
7. Existing British market
8. Sales methods/advertisement
9. Ideological gap between carriers and clients
10. Jurisdictional issues
11. Foreign markets' analysis
12. Other

Reference

BOOKS

Arthur Andersen (ed.), 'Operational Risk' (2001) Kinzai, Tokyo.

T. Atsumi (ed.), '*Soshiki, kigyô-hanzai wo kangaeru* (The consideration on organised crime and corporate crime)' (1998) Chûô-daigaku Syuppankai, Tokyo.

Attorney General's Department, 'Review of Commonwealth Criminal Law: Interim Report on Computer Crime' (1988) Australia Government Publishing Service, Canberra.

Audit Commission for Local Authorities in England and Wales, 'Computer Fraud Survey' (1985) H.M.S.O., London.

Audit Commission for Local Authorities in England and Wales, 'Survey of Computer Fraud and Abuse' (1987) H.M.S.O., London.

Audit Commission for Local Authorities and the National Health Service in England and Wales, 'Opportunity makes a thief: an analysis of computer abuse' (1994) H.M.S.O., London.

J.Beatson, 'Anson's Law of Contract' (2002) Oxford University Press, Oxford.

D. Bender, 'Computer law, vol.4' (1997) Matthew Bender, New York.

Cabinet Office, 'Recovering the Proceeds of Crime, a Performance and Innovation Unit report' (2000) Cabinet Office, London.

D. Campbell, R. Halson and D. Harris, 'Remedies in contract and tort' (2002) Butterworths, London.

J.M. Carroll, 'Portrait of the Computer Criminal', in J.H.P. Eloff & S.H. Solms, 'Information Security - the next decade' (1995) Chapman & Hall, London.

R.D. Clifford (ed), 'Cybercrime: the Investigation, Prosecurtion and Defense of a Computer-Related Crime', Carolina Academic Press, Durham.

P.A. Collier & B.J. Spaul, 'A Forensic Methodology for Countering Computer Crime', in I. Carr, 'Computers and the Law' (1994) Intellect, Oxford.

Council of Europe, European Committee on Crime Problems, 'Economic crime' (1981) Strasbourg.

H. Croall, 'White collar crime : criminal justice and criminology' (1992) Open University Press, Buckingham.

R. Dembo and A. Freeman, 'Seeing Tomorrow: Rewriting the rules of Risk' (1998) John Wiley & Sons, New York.

A.M., Dugdale (ed.) 'Clerk and Lindsell on Torts' (2000) Sweet & Maxwell, London.

Department of Trade and Industry, 'Dealing with computer misuse: review of the application of the Computer Misuse Act and the associated market for information and expert advice', (1992) Department of Trade and Industry, London.

K. Ebata, 'Information War' (1997) Far East Economics, Tokyo.

T. Elbra, 'A Practical Guide to the Computer Misuse Act 1990' (1990) Blackwell, Oxford.

European Commission Joint Research Centre, 'Cyber Crime in E-Business Processes: Report of an exploratory study' (2001) European Commission.

European Committee on Crime Problems, Council of Europe, 'Computer-related crime: Final report: Recommendation No. R (89) 9' (1990) Council of Europe, Strasbourg.

D. Friedrichs, '*Howaito karâ hanzai no houritsugaku* (Trusted Criminals)' (1999) Springer-Verlag, Tokyo.

V. Harpwood, 'Principles of Tort Law' (1998) Cavendish Publishing Limited, London.

B. Harvey and J. Marston, 'Cases & Commentary on Tort' (1994) Pitman Publishing, London.

K. Hirano & S. Makino, '*Hanrei Kokusai, Internet hô - cyberspace niokeru houritsu jousiki* (Cyberspace Law: ethics of cyberians and spirits of self-governance)' (1998) Prosper, Tokyo.

N. Hiyoshi, '*Daigaeteki risuku iten* (Alternative Risk Transfer)' (2000) Hoken Mainichi Shimbumsya, Tokyo.

H.M.S.O., 'Proceeds of Crime Bill: Publication of Draft Clauses' (2001) H.M.S.O.,, London.

Information Risk Management Dept. (ed) 'Information Security Survey 2000 Report' (2000) KPMG Business Assurance Japan, Tokyo.

ILC - Internet Lawyers Committee, 'Internet and the Law' (1998) Nihon Hyouron, Tokyo.

W. Ishikawa, T. Nara, S.Takakubo, & Y. Sato, '*Keihô* (Criminal Law)' (1983) Seirin, Tokyo.

Japan Securities Dealers Association, 'The Articles of Association and Fair Business Practice Regulation' (2001) Japan Securities Dealers Association, Tokyo.

M. Kamiyama (2000) '*Hoken no shikumi* (the Structure of Insurance)', Nihon Jitsugyô Syuppan, Tokyo.

Kanno, 'Tricks of Computer Crime' (1990) Corona, Tokyo.

C.E.A. Karnow, 'Future Codes: Essays in Advanced Computer Technology and the Law' (1997) Artech House, London.

H.W.K. Kaspersen, 'Standards for Computer Crime Legislation: A Comparative Analysis', in Vandenberghe, G.P.V.(eds) Advanced Topics of Law and Information Technology, (1989) Kluwer Law and Taxation, Boston.

K. Katayama, '*Beikoku ni-okeru akaunto agurigeisyon no sinten* (The Development of Account Aggregation in the USA)' (2001) Capital Market Quarterly Spring, Nomura Research Institute, at 35-49.

M. Kato, '*Jimukanri, Futouritoku, Fuhoukoui* (Misconduct of business, Unjust enrichment, and Tort)' (2002) Yûhikaku, Tokyo.

M. Kishida, '*Hô to keizai* (Law and Economics)' (1996) Sinseisya, Tokyo.

The Kightmare, 'Secret of Super Hackers', translated into Japanese by R. Matsufuji, (1995) Noritsu Management, Tokyo.

T. Kobayashi, '*Kenpô* (the Constitution)' (1989) Nihonhyouron, Tokyo.

S. Kumon, 'Y2K Trouble' (1999) NTT Publishing, Tokyo.

R.A. Kurz, 'Internet and the law' (1996) Government Institutes, Rockville.

The Law Commission, 'Criminal Law Computer Misuse Law Commission report No.186' (1989) H.M.S.O., London.

S. Le Doran & P. Rose, 'Cyber Thrillers' translated into Japanese by T. Kuwabara, (1996) Bungei-Syunjû, Tokyo.

D. Longley, 'Security and the Law', in W. Caelli, D. Longley, M. Shain,

'Information Security for Managers' (1989) Macmillan, Basingstoke.

The Marine and Fire Insurance Association of Japan (ed), 'Fact Book: Non-life insurance in Japan 1998-1999' (1999) The Marine and Fire Insurance Association of Japan, Tokyo.

The Marine & Fire Insurance Association of Japan (ed) 'Non-Life Insurance in Japan 1998-1999' (1999) Tokyo.

R. Matsufuji, '*Secrets of a Super Hacker: Anata no computer mo nerawareteiru* (The Nightmare. Secrets of a Super Hacker)' (1995) Noritsu Management Centre, Tokyo.

R.F. Meier & J.F. Short, Jr., 'The Consequences of White-Collar Crime' in G. Geis, R.F. Meier & L. Salinger (eds) 'White-Collar Crime: Classic and Contemporary Views' (1995) The Free Press, London.

K. Murayama, Y. Ôya & N. Takeuchi (1998) '*Legal Risk Management to Senryaku Houmu* (Legal risk management and strategy) ', Tax and Accounting Association, Tokyo.

T. Murobushi, '*Konpyûta hanzai sensou* (Computer Crime War)' (1987) Sunmark, Tokyo.

C. Nakajima, 'Conflicts of Interest and Duty' (1999) Kluwer Law International, London.

Y. Nakanome, '*Keiji Sosyô Hoû no kaisetsu* (An commentary to Japanese Criminal Procedure Code)' (1997) Hitotsubashi Syuppan, Tokyo.

The National Police Agency (ed) 'High-tech crime: the fact and the countermeasure' (1999) Tachibana Shobô, Tokyo.

NCIS, 'Project Trawler: crime on the information highways' (1999) London.

Non-life Insurance Research Centre (ed) 'New insurance product' (1999) Tokyo.

OECD 'Computer-related crime: analysis of legal policy: Being: Information, computer, communications policy: V.10' (1986) OECD, Paris.

D.B. Parker, 'Fighting computer crime', translated into Japanese by M. Uzawa, (1984) Syujunsya, Tokyo.

D.B. Parker, 'A new framework for information security to avoid information anarchy', in Eloff, J.H.P. & von Solms, S.H. Information Security-the next decade, (1995) Chapman & Hall, London.

W.V.H. Rogers, 'The Law of Tort' (1994) Sweet & Maxwell, London.

M.D. Rostoker and R.H. Rines, 'Computer Jurisprudence: Legal Reponses to the Information Revolution' (1986) Oceana, New York.

Scottish Law Commission, 'Computer Crime: Consultative Memorandum No.68' (1996).

Sieber, 'International Handbook on Computer Crime: computer related economic crime and the infringements of privacy' (1986) John Wiley & Sons, New York.

H. Sutherland, edited by K. Schuessler, 'On Analyzing Crime' (1973) The University of Chicago Press, Chicago.

C. Tapper, 'Computer Law' (1989) Bath Press, Harlow.

K. Tiedemann, '*Doitsu oyobi EC niokeru Keizai-hanzai to keizai-keihou* (Economic crime and economic law in the Federal Republic of Germany and EC countries, the translation of 'Wirtschaftskriminalitat und Wirtschaftsstrafrecht' by H. Nishihara & K. Miyazawa) (1990) Seibundo, Tokyo.

D.S. Wall, 'Cybercrimes and the Internet' in D.S. Wall (ed) 'Crime and the Internet' (2001) Routledge, London.

M. Wasik, 'Crime and the Computer' (1991) Clarendon, Oxford.

C. Williams, M.L. Smith and P. Young, 'Risk management and insurance: the eighth edition' (1998) McGraw-Hill, London.

JOURNALS

J. Backhouse & G. Dhillon, 'Managing computer crime: a research outlook', 14 Computer and Security 7 (1995).

L. Duff & S. Gardiner 'Computer Crime in the Global Village: Strategies for Control and Regulation - in Defence of the Hacker', in S. Savage & J. Carrie (eds) 24 International Journal of the Sociology of Law (1996) .

J. Gantz, 'A city of felons at T1 speeds', in 31 Computerworld 7 (1997).

K. Gotô, '*Kigyô-keiei no saidai-kadai to natta risuku manegimento* (Risk management, the crucial key factor of business management)' (2001) 4 Songai hoken kenkyû 62.

S. Heymann, 'Legislating Computer Crime', in 34 Harvard Journal on

Legislation 2, (1997).

Insurance Online, 'Study: E-Risk Coverage Stagnates' at 12 on 7 August 2000,

S. Levy, 'The Bug That Didn't Bite: Billions of dollars later, Y2K is on the run. The lessons of a millennial computer scare' in Newsweek, 10 January 2000.

K.J. Mills, 'FBI forms cyber squad', in 9 International Business 7, (1996).

M. Solomon, 'The CU crime that hurts most', in 63 Credit Union Magazine 2, 1997.

H.A. Wan, 'An Analysis of Chinese Laws against Computer Crimes', 5 Journal of Global Information Management 2, 1997.

J. Young, 'Spies like us', in *Forbes*, February 1996

NEWSPAPERS

The Daily News Mail online from Infostand dated 19th June 2002.

The Financial Times dated 20th February 2000.

The Financial Times dated 28th July 2001.

The Financial Times dated 5th March 2002.

Mainichi Shimbun dated 28th March 2001.

Nihonkeizai Shimbum dated 20th September 2000, 'The age of reform in the insurance industry'.

Nihonkeizai Shimbum dated 1st June 2001, at 5.

Nihonkeizai Shimbum dated 1st April 2001, at 1.

Nihonkeizai Shimbum dated 17th April 2002.

Nihonkeizai Shimbum dated 28th April 2002.

Nihonkeizai Shimbum dated 17th July and 2nd August 2002.

Nihonkeizai Shimbum dated 3rd August 2002.

Nihonkeizai Shimbum dated 23rd August 2002.

The Wall Street Journal dated 17th March 1997.

World Wide Web (print out on file with author)

'*15sai no kodomo demo kanou. FBIsousakanbu, net-syakainoyowasa wo siteki* (FBI investigators said teenagers can crash network) ', <http://www.mainichi.co.jp/digital/netfile/archive/200002/10-2.html>

'1996-1997 Report on Money Laundering Typologies', <http://www1.oecd.org/fatf/pdf/TY1997_en.pdf>

'1997-1998 Report on Money Laundering Typologies', <http://www1.oecd.org/fatf/pdf/TY1998_en.pdf>

'2000-2001 Report on Money Laundering Typologies', <http://www1.oecd.org/fatf/pdf/TY2001_en.pdf>

'*5 syô. Hidaitodoke, Sosyô, Sousa* (Chapter 5. An incident report, a lawsuit and investigation)', <http://www.web110.com/roppou/roppou4.html>

'*6-9tuke Jôhô-tsûshin network no anzen/sinraisei ni kansuru kenkyûkai-houkokusyo dai-1-hen dai-2-syô* (A report on a society for safety and confidentiality of information communication network dated June 9th)', <http://www.soumu.go.jp/joho_tsusin/pressrelease/japanese/denki/970609j602_3.html>

'*7. Saibâ hanzai* (7. Cybercrime)', <http://www.law.co.jp/okamura/jyouhou/cybercrime/crim7.htm>

'7799 History', <http://www.c-cure.org/7799history.htm>

'8th United Nations Congress Resolution on computer-related crimes', <http://www.io.com/~asrcs/un.html>

'*9. Owarini* (9. The conclusion)', <http://www.law.co.jp/okamura/jyouhou/cybercrime/crime.htm>

'18 September 2002, Websense Japan Inc.', <http://www.websense.com/company/news/pr/02/japan/091802.cfm>

'A Bill To facilitate the use of electronic records and signatures in interstate or foreign commerce', <http://www.isc.meiji.ac.jp/~sumwel_h/doc/code/bill-1999-k.htm>

'A New ID-Less ID System',

<http://www.wired.com/news/print/0,1294,34477,00.html>

A Specimen Policy of Tyser's Cyber Liability Insurance is available online from <http://www.tyseruk.co.uk/esurance.pdf>

'About the financial system reform (The Japanese version of the Big Bang)', <http://www.mof.go.jp/english/big-bang/ebb1.htm>

'Account aggregation', <http://www.fsa.gov.uk/consumer/whats_new/updates/e_commerce/mn_aggregation.html>

'Account Aggregation - Consumers' Questions Answered', <http://www.europathway.net/newsresult.asp?ID=53>

'Account Aggregation: Consolidate, or be Consolidated?' , <http://www.unisysfinancial.com/events_news/publications/articles/account_aggregation.asp>

'Account Aggregation - Consumers' Questions Answered', <http://www.europathway.net/newsresult.asp?ID=53>

'Aggregate to accumulate', <http://www.moneyextra.com/features/2001/f011004_investment_84.html>

'Aggregation: An Untouched Opportunity For Financial Institutions', <http://www.microbanker.com/artarchive02/hallcreditlendAggregationAnUntouchedOpportunityFor121501bts.html>

'Aggregation for the Little Guys', <http://www.banktechnews.com/btn/articles/btnaug01-4.shtml>

'Aggregation guidelines receive cautious welcome', <http://www.onwindows.com/news/2001/December/241201.htm>

'Aggregation Is The New Buzzword - Aggregation Will Allow', <http://globalarchive.ft.com/globalarchive/articles.html?id=010713016979&query=account+aggregation>

'*Akaunto agurigêsyon no kinou* (The functions of the account aggregation)', <http://www.sw.nec.co.jp/finance/Special/Aggregation/FSFair402.html>

'*Akaunto Agurigêsyon wo shitteimasuka?* (Do you know the account aggregation services?)', <http://itpro.nikkeibp.co.jp/free/ITPro/OPINION/20011220/1/>

'American Banker-The Financial Services Daily, While Others Quail At 'Screen Scraping,'Fleetboston Will Embrace It on New Site',

<http://www.yodlee.com/company/news/articles/amerbanker_services.html>

'APACS publishes best practice guidelines for account aggregation', <http://www.apacs.org.uk/downloads/aggregationpr2.pdf>

'The Association Of British Insurers', <http://www.abi.org.uk/Display/default.asp?Menu_ID=507&Menu_All=1,506,507>

'Anti-Hacking premiums 25% higher for Win NT', <http://www.theregister.co.uk/content/8/18324.html>

'Arbitration and Mediation Centre', <http://arbiter.wipo.int/arbitration/arbitration-guide/index.html>

'Are Recent Developments in International Co-operation incompatible with Swiss Banking Secrecy?', <http://www.secretantroyanov.com/Publication/Swiss%20banking%20secrecy.htm>

'*Autosôsingu* (Outsourcing)', <http://www.dtcg.tohmatsu.co.jp/serviceline/outs.html>

'*Beikoku denshisyomeihô sikoukara 1 nen, fukyû-kakudai wo habamu mondaiga sanseki* (A year has passed since Signatures in Global and National Commerce Act came into effect in the USA, innumerable problems to avoid popularised dated 1 November 2001)', <http://www.idg.co.jp/report/itreport/backnumber/200111/20011101_01_ebiz_report.html>

'Bank Exec, Husband Admit Laundering Billions', <http://www.apbnews.com/safetycenter/business/2000/02/16/pleas0216_01.html>

'Banks face loyalty dilemma', <http://news.bbc.co.uk/hi/english/business/newsid_1876000/1876126.stm>

'Banks guilty of laundering', <http://www.marcosbillions.com/marcos/Dictators%20Abacha%20British%20banks_guilty_of_laundering.htm>

'Basel Committee Publications - Electronic Banking Group Initiatives and White Papers - Nov 2000', <http://www.bis.org/publ/bcbs76.pdf#xml=http://search.atomz.com/search/pdfhelper.tk?sp-o=2,100000,0>

'Basel Committee reaches agreement on New Capital Accord issues', <http://www.bis.org/press/p020710.htm>

'*Beikoku akaunto Agurigêsyon sâbisu saishin doukô* (The latest trend of the account aggregation services in the USA)', <http://www.sw.nec.co.jp/finance/Special/Aggregation/FSFair401.html>

'*Beikoku ni okeru akaunto Agurigêsyon no shinten* (The latest progress of the account aggregation services in the USA)', <http://www.nri.co.jp/report/sihonsijo/01_spring/04-04_004s.htm>

'*Beikoku ni-okeru akaunto agurigêsyon sijô no kibo* (The size of the account aggregation market in the USA)', <http://www.sw.nec.co.jp/finance/Special/Aggregation/FSFair403.html>

'*Beikoku ni-okeru akaunto agurigêsyon sijô no kibo* (The size of the account aggregation market in the USA)', <http://www.sw.nec.co.jp/finance/Special/Aggregation/FSFair403.html>

'Best Practice Aggregation Guidelines', <www.apacs.org.uk>

'*Biggu 4 Tanjô* (the birth of Big 4 financial groups)', <http://www.rinku.zaq.ne.jp/kazu_san/ginko4.htm>

'THE BIRMINGHAM SUMMIT: FINAL COMMUNIQUE - Sunday 17 May 1998', <http://birmingham.g8summit.gov.uk/docs/final.shtml>

'BITS', <http://www.bitsinfo.org/aggregator.html>

'BIS History', <http://www.bis.org/about/history.htm>

'Blind Signatures and Fair Blind Signatures', <http://www.csh.rit.edu/~spraguep/crypto/>

'Bringing Order to Chaos Insurance Issues for E-Commerce Activities', <http://www.irmi.com/expert/articles/rossi001.asp>

'Brit Cops Tackle E-Thievery', <http://www.wired.com/news/business/0,1367,43171,00.html>

'BS ISO/IEC 17799:2000 - Overview', <http://www.c-cure.org/7799Overview.htm>

'c:cure', <http://www.c-cure.org/welcome.htm>

'Case: Cox vs. Riley (1986)', <http://www.cs.mdx.ac.uk/courses/foundation/modules/bis0015/lectures/bis0015_week11/tsld017.htm>

'Categorization Plus Syndication Does Not Necessarily Equal Viability',

<http://www4.gartner.com/DisplayDocument?id=334188&acsFlg=accessBought>

'CBA leads charge for all-in-one bank sites', <http://globalarchive.ft.com/globalarchive/articles.html?id=010809001851&query=account+aggregation>

'Changes in EU Financial and Insurance Markets and New Strategies of EU Financial Institutes and Insurers throughout the 1990's, especially in the UK, German and French Markets', <http://www.sj-ri.co.jp/quarterly/q32.html>

'Chapter One Crime and the Computer', <http://www.strath.ac.uk/Departments/Law/dept/diglib/book/criminal/crim16.html>

'*Chiyoda seimei: Kousei Tokureihou Tekiyou wo Shinsei. Sengo Saidaino Tousan* (The largest bankruptcy: Chiyoda Mutual Insurance) ', <http://www12.mainichi.co.jp/news/search-news/809459/90e791e393c90b696bd-0-5.html>

'*Chosakuken-singai ni taisuru songaibaisyô ya sasitomeseikyû* (Claims for damages and rights to demand the injunction on the infringement of copyrights)', <http://www.kyoto-archives.gr.jp/copyright/KOZA/koza08.html>

'*Chûsai no tokuchô* (The characteristics of arbitration)', <http://www.jcaa.or.jp/arbitration-j/kaiketsu/t-3.html>

'Citibank misses its deadline for online service', <http://news.ft.com/ft/gx.cgi/ftc?pagename=View&c=Article&cid=FT302R0E5RC&live=true&query=aggregation>

'The classification and the application of operational risk (*Operational risk no bunrui-taikei to katsuyôhô*)', <http://www.kinzai.jp/books/new_book/20010815/10128-2.pdf>

'CNET Japan', <http://japan.cnet.com/Help/manual/0911.html>

'Code Red Dormant--For Now', <http://www.internetweek.com/story/INW20010730S0002>

'COMMUNIQUÉ', <http://www.g8italia.it/_en/docs/XGKPT170.htm>

'Communiqué: The Denver Summit of the Eight', <http://www.state.gov/www/issues/economic/summit/communique97.html>

'COMPUTER CRIME', <http://www.kcl.ac.uk/orgs/icsa/crime.htm>

D.L. Carter, and A.J. Katz, 'Computer Crime: An Emerging Challenge for Law Enforcement' available on <http://www.crime-prevention.org.uk/>

'Computer Crime Reports',
<http://www.underground-book.com/chapters/ccm/10.html>

'Computer Fraud: Slapa Assignment 3',
<http://www.scitsc.wlv.ac.uk/_cm5067/slapa/fraud.html>

'Computer Misuse Act 1990 (c. 18)',
<http://www.hmso.gov.uk/acts/acts1990/Ukpga_19900018_en_2.htm>

'The Computer Misuse Act 1990: 5 years on',
<http://csrc.lse.ac.uk/people/kelmana/CMA1990_Page3.htm>

'*Computer virus nado yûgai-puroguramu no houtekikisei nikansuru kokusai-doûkoû-chôsa* (The world trend of the legal approach towards injurious computer programme including computer virus)'
<http://www.ipa.go.jp/security/fy11/report/contents/virus/law243.html>

'Computer Virus Prevention Guidelines',
<http://www.ipa.go.jp/security/english/virus/virus-guidelin-e.html>

'Conditional crime list on money laundering',
<http://www.fsa.go.jp/fiu/fiu.html>

'The Constitution of Japan',
<http://list.room.ne.jp/~lawtext/1946C-English.html>

'Consultative Document on The New Basel Capital Accord',
<http://www.bis.org/publ/bcbsca03.pdf>

'Consultative Document, Operational Risk, Supporting Document to the New Basel Capital Accord', <http://www.bis.org/publ/bcbsca07.pdf>

'Consumer Account Aggregation Won't Deliver ROI For Most Financial Firms, According To Forrester Research',
<http://www.forrester.com/ER/Press/Release/0,1769,609,00.html>

'Convention on Cybercrime (ETS no. 185): Explanatory Report',
<http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>

'Copyright, Designs and Patents Act 1988 (c. 48)',
<http://www.hmso.gov.uk/acts/acts1988/Ukpga_19880048_en_7.htm>

'Copyright, Design and Patents Act 1988 (c. 48)',
<http://www.hmso.gov.uk/acts/acts1988/Ukpga_19880048_en_2.htm>

'Copyright Law of Japan', <http://www.cric.or.jp/cric_e/clj/cl1.html>

'Corporate Governance',
<http://www.cpaaudit.co.uk/pages/corpgovernance.html>

'Corporate Governance and the Integrity of Financial Markets: Some Current Challenges', <http://www.oecd.org/pdf/M00029000/M00029848.pdf>

'Crime, Chubb Group of Insurance Companies',
<http://www.chubb.com/businesses/ep/crime/crime.html>

'Cyberlaundering threats should put all bankers on alert, FATF warns',
<http://www.moneylaundering.com/MLAarticles/01Apr5.htm>

'Cyber liability insurance', <http://www.tyseruk.co.uk/cli.html>

'Cybercrime - what SME should know',
<http://www.blindtiger.co.uk/IIA/uploads/-38c9a362-ed71ce5fa5--761f/CybercrimewhateverySMEshouldknowpdf.pdf>

'CyberSecurity by Chubb℠ for Financial Institutions',
<http://www.chubb.com/businesses/dfi/cyber/index.html>

'*Cyber security no kokusaiteki houritsu mondai* (International Legal Issues on Cyber Security by Ikuo Takahashi)',
<http://www.isc.meiji.ac.jp/~sumwel_h/iunc/cmp_crime/cmp_crime-1998-4.htm>

'cybersquatting',
<http://searchwebmanagement.techtarget.com/sDefinition/0,,sid27_gci213900,00.html>

'*Dai 4 suteppu risuku syori* (The 4th step: risk disposal)',
<http://www.hyuga.or.jp/hoken/rskmng/r14.html>

'*Dai-4-kai Chokumen-suru omona kadai to taisaku Part. II* (4. The major problems and countermeasures Part. II)',
<http://www.unisys.co.jp/outsourcing/column/column4.htm>

'*Dai-5-syô Eikoku* (Chapter 5 England)',
<http://www.ipa.go.jp/security/fy11/report/contents/virus/report5.pdf>

'*Dai-7-kou, IT to business moderu* (Chapter7, IT and Business models)',
<http://www.w3c.org/TR/1999/REC-html401-19991224/loose.dtd>

'*Dai-8-kai Densi-syoutoruhiki to kessai* (Vol.8 E-commerce and clearing systems)', <http://www.zdnet.co.jp/help/ebusiness/08/>

'*Daini Tokyo Bar Association, Q28 Du purosesu toha nandesuka?* (Daini Tokyo Bar Association, Q28 What is 'due process'?)', <http://www.dntba.ab.psiweb.com/qna/qna28.htm>

'*Dai-ni-syô Angou seisaku ni kanrensuru sonota no jouhou sekyurityi shisaku* (Chapter II Another security policy in relation to cryptography)' <http://www.npa.go.jp/hightech/secv_repo/2-2.htm>

'*Data-hason no songai-baisyô-sekinin, backup ha user no sekinin?* (The liability for damaging data, is a user liable for making backup?)', <http://www.asahi-net.or.jp/~zi3h-kwrz/law2backup.html>

'Daiwa Bank shareholders' lawsuit a wake-up call for company execs', <http://www.yomiuri.co.jp/index-e.htm>

'Data Protection Act 1998', <http://www.hmso.gov.uk/acts/acts1998/80029--a.htm>

'Daily News, E-Money Laundering', <http://www.fitug.de/debate/9912/msg00015.html>

'Defamation Act 1996', <http://www.legislation.hmso.gov.uk/acts/acts1996/1996031.htm>

'Definition of Cyberspace', <http://www.education.miami.edu/ep/michigan/sld011.htm>

'*Denshi-manê no genjô* (The present situation of e-money)', <http://members.tripod.com/tsurut/rep/e_money.html>

'*Denshimanê no genjyô to mondaiten* (The present situation of e-money and its problems)', <http://www.glocom.ac.jp/users/taiyo/emoney/emoney.html>

'*Denshi manê rondaringu* (electronic money laundering)', <http://member.nifty.ne.jp/psyche/soi/ips09.html>

'Digital Insurance Now Available for IM', <http://www.instantmessagingplanet.com/enterprise/article/0,,10816_11414 01,00.html>

'Disputes & Litigation Over Domain Names', <http://www.kaltons.co.uk/DNdisputes.htm>

'Domain Names as Trade Mark Usage in the UK', <http://www.kaltons.co.uk/DNasTM.htm>

'Domain Name Regulation',

<http://www.hamiltons-solicitors.co.uk/Domain.htm>

'*Domain no kisochisiki* (The basic knowledge on domain name system', <http://www.solid.ad.jp/solidweb/domain/domain_01.html>

'Domain War Motive a Guess', <http://www.wired.com/news/business/0,1367,35708,00.html>

'Draft Convention on Cybercrime', <http://conventions.coe.int/treaty/EN/cadreprojets.htm>

'DTI - Protecting business information - Understanding the risks', <http://www.dti.gov.uk/PROTECT/risks/risks.htm>

'e-words', <http://www.e-words.ne.jp/frame.asp?body=view.asp&word=%83n%83b%83J%81%5B>

'Earthlink wins $24 million from spammer', <http://zdnet.com.com/2100-1106-945169.html>

'E-commerce Insurance: New Riders of the Digital Age', <http://www.cfo.com/article/1,5309,4662|7|A|55|8,00.html>

'E-money activities and E-banking: Consequences of e-money for the prudential supervision of financial institutions', <http://www.ee/epbe/en/release/hagen.pdf>

'Egg remains confident of breaking even BANKS OUTFLOW OF CUSTOMERS SLOWS IN FOURTH QUARTER BUT ANNUAL LOSSES INCREASE TO Pounds 155M', <http://globalarchive.ft.com/globalarchive/articles.html?id=010220001157>

'*Eiwa tokkyo yougo jiten* (English-Japanese dictionary for the Patents terminology', <http://www.patro.co.jp/EJPatDic/T.html>

'The Electronic Frontier: the challenge of unlawful conduct involving the use of the Internet', <http://www.nctp.org/unlawful1.html>

'Electronic Frontier, Crime and the Computer', <http://www.strath.ac.uk/Departments/Law/dept/diglib/book/criminal/crim11.html>

'Electronic money directive, Directive 2000/46/EC of the European Parliament and of the Council', <http://141.211.44.49/faculty/rmann/Statutes/ElectronicMoneyDirective.pdf>

'Electronic Money Laundering: An Environmental Scan' published by

Department of Justice Canada,
<http://www.sgc.gc.ca/WhoWeAre/PPC/eScan/emoney/emoney.htm>

'Emulex Victims: Who Can We Sue?',
<http://www.wired.com/news/print/0,1294,38581,00.html>

'The End of Computer Virus Coverage as We Know It?',
<http://www.irmi.com/expert/articles/rossi011.asp>

'ETrade Loses Tech Glitch Dispute',
<http://www.wired.com/news/print/0,1294,20595,00.html>

'FATF experts espouse strict laundering controls for cyberbanking',
<http://www.moneylaundering.com/MLAarticles/00Apr2.htm>

'Federal Bureau of Investigation National Computer Crime Squad',
<http://www.fbi.gov/programs/compcrim.htm>

'Fidelity & Crime Insurance', <http://www.tyseruk.co.uk/cri.html>

'Finance@nifty', <http://finance.nifty.com/stocks/tsumitate/column/co1.htm>

'The Financial Action Task Force on money laundering',
<http://usinfo.state.gov/journals/ites/0501/ijee/fatffacts.htm>

'Financial Action Task Force on Money Laundering, The Forty Recommendations', <http://www1.oecd.org/fatf/40Recs_en.htm>

'Financial Fidelity/Mail/Kidnap Ransom for Banks',
<http://www.chubb.com/businesses/dfi/index8.html>

'The Financial Services Roundtable', <http://www.fsround.org/>

'Finite', <http://www.ace-insurance.co.jp/risk/risk08.html>

'First-Party E-Commerce Risks',
<http://www.irmi.com/expert/articles/rossi002.asp>

'Forgery and Counterfeiting Act 1981',
<http://www.butterworths.co.uk/academic/lloyd/Statutes/forgery.htm>

'Formation of New Comprehensive Insurance & Financial Services Group',
<http://www.sumitomomarine.co.jp/english/pres20000218.html>

The FSA website, <http://www.fsa.go.jp/indexe.html>

The FSA website, '*Songai hoken dairiten seido no minaoshi nituite* (Re-constructing agency system for the non-life insurance industry)',

<http://www.fsa.go.jp/p_fsa/news/newsj/f-20000524-1.html>

'fsa, what's new, e commerce',
<http://www.fsa.gov.uk/consumer/whats_new/updates/e_commerce/mn_aggregation.html>

'FTyourmoney launches online "financial dashboard"',
<http://uk.biz.yahoo.com/011219/66/cm3og.html>

'Funding of BSI and Standards Development',
<http://www.dti.gov.uk/strd/fundingo.htm>

'*Fuhô Kôi* (Tort)', <http://cc.matsuyama-u.ac.jp/~tamura/minpo-709.html>

'*Funsyoku kessan* (a window dressing settlement)',
<http://www.hi-ho.ne.jp/yokoyama-a/funshoku.htm>

'*Fusei-akusesu boushi-hô ni kansuru chôsa* (Research on Unauthorized Computer Access Law)',
<http://www.ipa.go.jp/SECURITY/pub/contents/crack/research/law/Criminal-3.html>

'*Fusei-akusesu taisaku-hou no yukue* (The future of Unauthorized Computer Access Law)',
<http://members.tripod.co.jp/hatzemi/resume/zemirepo/1999-2kcss/05.htm>

'*Fusei-akusesu-taisakuhousei ni kansuru Keisatsuchou-an oyobi Yûseisyou-an heno paburikku komento bosyû henotaiou nitsuite* (The correspondence to the public comment advertisement on Unauthorized Computer Access Bills by the NPA version and the Ministry of Posts and Telecommunications version'),
<http://www.jisa.or.jp/activity/opnion/990107-j.html>

'*Fusei-akusesu taisakuhoû ni taisuru kihonnteki-kenkai* (A fundamental opinion to Unauthorized Computer Access Law)',
<http://www.asahi-net.or.jp/~vr5j-mkn/fuseiakusesu.htm>

'*Fuseipuroguramu no haifukeiro* (A distribution route of mal-computer programme)', <http://cherry.webdos.net/~bluesky/virii/haizen.html>

'G7 Lyon Summit Information',
<http://www.mofa.go.jp/mofaj/gaiko/economy/summit/lyon/index.html>

'G8 AND INTERNATIONAL CRIME',
<http://birmingham.g8summit.gov.uk/crime/>

'G8 COMMUNIQUÉ OKINAWA 2000',
<http://www.g7.utoronto.ca/g7/summit/2000okinawa/finalcom.htm>

'*Gabanansu* (Governance)',
<http://home.att.ne.jp/sea/tkn/Issues/Issue-Governance.htm>

'*Gendai no Zaibatsu Rokudai Kihyou Syuudan* (Big six financial group at present) ', <http://www.geocities.co.jp/WallStreet/6757/09/09.htm>

'Getting to grips with e-risk',
<http://www.fsa.gov.uk/pubs/press/2001/066.html>

'Global Programme Against Money Laundering',
<http://www.odccp.org/money_laundering.html>

'Got Cyber Insurance?',
<http://computerworld.com/cwi/Printer_Friendly_Version/0,1212,NAV47-665_STO48721-,00.html>

'GRAMM-LEACH-BLILEY ACT',
<http://www.finmod.state.tx.us/content/theact/glbatext.htm>

'Greenhalgh Insurance Cyber Liability',
<http://www.greenhalghinsurance.com/cyber.html>

'Guidelines for the Security of Information Systems',
<http://www1.oecd.org/dsti/sti/it/secur/prod/e_secur.htm#11>

'Guidelines for the security of information systems and networks towards a culture of security', <http://www.oecd.org/pdf/M00034000/M00034292.pdf>

'*Hakkâ wo terorisuto toshite atsukau eikoku no shinpô* (A brand-new British Law that refers a hacker as a terrorist)',
<http://www.idg.co.jp/report/security/backnumber/us_topics/200102/sec20010220_01_us.html>

'*Hacker wo teroristo toshite atsukau eikoku no sinpou* (The new British Law against cyber terrorists dated 20th February 2001)',
<http://www.idg.co.jp/report/security/backnumber/us_topics/200102/sec20010220_01_us.html>

'*Hacking tokuju* (Special hacking procurements) ',
<http://www.mainichi.co.jp/digital/netfile/archive/200002/08-1.html>

'*Hani potto wo riyou-shita nettowâku no kikikanri* (Crisis management of computer network by using the honeypot project)',
<http://www.atmarkit.co.jp/fsecurity/special/13honey/honey01.html>

'*Heisei 13nendo OECD Jôhô sekyuriti gaidorain ni kansuru chousa* (2001 A survey on OECD information security guideline)',

<http://www.ipa.go.jp/security/fy13/report/oecd-guideline/oecd-guideline.pdf
>

'*Hôritsu, gaidorain nado* (Regulations and guidelines)',
<http://www.meti.go.jp/policy/netsecurity/law_guidelines.htm>

'*Hougaku Dai-ichi-bu* (Jurisprudence Part 1)',
<http://www5a.biglobe.ne.jp/~kaisunao/ho-kogi/05hogen.htm>

'House of Commons, Friday 9 February 1990',
<http://www.parliament.the-stationery-office.co.uk/pa/cm198990/cmhansrd/1990-02-09/Debate-1.html>

'*IBM no USB memori ni uirusukonnyû no kanôsei* (A possibility of containing computer virus in IBM USB memory)',
<http://www.zdnet.co.jp/news/bursts/0201/29/10.html>

'Identity and the Internet: A symbolic interactionist perspective on computer-mediated social networks',
<http://www.buffalo.edu/~reymers/identity.html#intro>

'Interactive News', <http://www.mainichi.co.jp/>

'International Insurance',
<http://www.roughnotes.com/ao-onlinedemo/pfm/300/329_0402.htm>

'International review of criminal policy - the United Nations Manual on the prevention and control of computer-related crime',
<http://www.ifs.univie.ac.at/~pr2gq1/rev4344.html>

'Introducing Insurance',
<http://www.abi.org.uk/Display/default.asp?Menu_ID=508&Menu_All=1,506,508>

'Investigating International Developments in eCommerce Insurance Policies', <http://www.inslawgroup.com/pdf/marcusevans020801ppt.pdf>

'investorwords.com',
<http://www.investorwords.com/cgi-bin/getword.cgi?5817>

'Is Computer Data Tangible Property or Subject to Physical Loss or Damage Part 1', <http://www.irmi.com/expert/articles/rossi008.asp>

'Is Computer Data Tangible Property or Subject to Physical Loss or Damage Part 2', <http://www.irmi.com/expert/articles/rossi009.asp>

'*ISID, Hitachi Seisakujo, Sofutobanku-Tekunorojî ga agurigêsyon-jigyoukaisya wo setsuritu (ISID, Hitachi and Softbank*

Technology set up aggregation joint enterprise)',
<http://www.watch.impress.co.jp/internet/www/article/2001/0911/acount.htm>

'ISO, Catalogue searched for standards',
<http://www.iso.org/iso/en/CombinedQueryResult.CombinedQueryResult?queryString=15408>

'The ISO17799 Security Newsletter - Issue 2',
<http://www.iso17799-web.com/issue2.htm>

'The ISO17799 Security Newsletter', <http://www.iso17799-web.com/>

'*ISO/TC68 Kokunai-iinkai* (ISO/TC68 Domestic Committee)',
<http://www.imes.boj.or.jp/iso/gaiyou.html#soshiki>

'IT Law LLM Reading List: Computer Crime',
<http://www.qmw.ac.uk/~ccls/itlaw/reading/crime.htm>

'Japan's First Aggregation Service (Next-generation B-to-C Service) to be introduced', <http://www.nri.co.jp/english/news/2001/010313.html>

'JCA Newsletter Number 10',
<http://www.jcaa.or.jp/e/arbitration-e/syuppan-e/newslet/news10.html>

'*Jitsurei ni miru chiteki-zaisanken mondai 33* (The issues in actual cases of Intellectual Property Rights 33)',
<http://www.ngb.co.jp/iitsureichizai/jitsureichizai_34.htm>

'*Jôhô kanren hô Dai 4 kou Computer programme no houtekihogo* (Law related to information, Part 4 Legal protection on Computer Programme)',
<http://www.mars.dti.ne.jp/~kos/law/lives/infolaw/info-04.html>

'*Jôhô kanren hô Dai 6 kou Eigyô-himitsu no houtekihogo* (Law related to information, Part 6 Legal protection on trade secret)',
<http://www.mars.dti.ne.jp/~kos/law/lives/infolaw/info-06.html>

'*Jôhô sekyuriti seisaku jikkô proguramu, Tûsansyô* (Information security policy programme by the Ministry of International Trade and Industry)',
<http://www.meti.go.jp/policy/netsecurity/downloadfiles/esecu01j.pdf>

'*Jôhô sisutemu anzen taisaku kijun* (the standards for secured information system, MITI annunciation No. 518 in 1995)',
<http://www.meti.go.jp/policy/netsecurity/downloadfiles/esecu03j.pdf>

'*Kabunushi-Daihyô-Sosyô* (The shareholder derivative action)',
<http://www.eiko.gr.jp/topics019.htm>

'Kakudai-suru intânetto bankingu (Expanding Internet Banking business)', <http://www.nttdata.com/usinsight/8Watch1.htm>

'*Keihoû* (Criminal law)', <http://www.lec-jp.com/law/houritsu/k_33.html>

'*Keihoû, Syouwa 62nen-kaisei no fusei-akusesu kanrenbubun wo bassui* (Criminal law, the relevant articles to unauthorized access amended in 1987)', <http://www.ipa.go.jp/security/ciadr/law1987.html>

'*Keihou Souron Kougi Nouto* (Criminal Law lecture Note)', <http://web11.freecom.ne.jp/~aimon/kei/kei_n1.html>

'*Keihou-souron 1. Resume No.7* (An introduction to Criminal Law *1. Resume No.7*)', <http://www.h2.dion.ne.jp/~tabu/01lec-cg1-e-7.htm>

T. Kobayashi, '*Kenpô* (the Constitution)' (1989) Nihon Hyouron, Tokyo, at 111 and 259-260, and also 'The Constitution of Japan', <http://list.room.ne.jp/~lawtext/1946C-English.html>

'Key Concepts', <http://www.coso.org/KeyConcepts/index.html>

'*Kigyô risuku jôhô* vol.9 (Corporate risk information vol.9)', <www.irric.co.jp/library/management/risk_info09.pdf>

'*Kinyû akaunto agurigêsyon* (The financial account aggregation)', <http://www.sw.nec.co.jp/finance/N_Souken/Article/200107-3.html>

'*Kinyû to hoken no yûgô ni-tsuite* (Uniting finance and insurance)', <http://www.imes.boj.or.jp/jdps99/99-J-13.pdf>

'*Kinyû-gyôkai ni jisedai-BtoC sâbisu tanjô. Agurigêsyon-sâbisu niyoru kokyaku-kakoikomi ha seikousuruka*? (The account aggregation, the new service for the next generation BtoC, has now arrived in the financial market. The question is will it prove a success in ensuring customers?)', <http://www.atmarkit.co.jp/fitbiz/keyword/aggregation/keyword7.html>

'*Kinyû-kikan gyoumu no autosôsingu ni saisite no risukukanri* (Risk management on outsourcing services in financial services industry)', <http://www.boj.or.jp/seisaku/01/sei0112.htm>

'*Kinyû-kikan-nado niyoru kokyaku-nado no honnin-kakunin-nado ni kansuru houritu* (The Law for Financial Institutions Identifying the Customers)', <http://www.fsa.go.jp/houan/154/hou154.html#01>

'*Kinyû-shin-sâbisu: akaunto agurigêsyon no dôkô* (A new financial service: The trend of the account aggregation services)', <http://www.nttdata.com/usinsight/8Report1-1.htm>

'*Kojin-muke ni 3-taipu no agurigêsyon-sâbisu teikyou-kaishi* (Three different types of aggregation services are available for individual customers)', <http://www.nri.co.jp/news/2001/011025.html>

'*Kouza jyôhô syûyaku sâbisu* (aggregation services)', <http://www.fin-bt.co.jp/comment9.htm>

'*Kyûden Mizuho ni seikû he* (Kyûsyû Electric Power Company decided to claim compensation to Mizuho)', <http://www.nikkei.co.jp/sp2/nt26/20020417eimi189717.html>

'*Kyûgin-saito, kakikaerareru* (A hacker attack on Kyûgin website)', <http://www.mainichi.co.jp/digital/netfile/archive/200003/24-1.html>

'Lack of Regulation Increases Insecurities', <http://www.erisk.com/news/analysis/news_analysis2001-05-22_01.asp?>

'Lawsuit Aims at Short-Sellers', <http://www.wired.com/news/print/0,1294,38522,00.html>

'Liability for Computer Glitches and Online Security Lapses', <http://www.sidley.com/cyberlaw/features/liability.asp>

'Links to Laws of Japan, Codes, Statutes, Regulations of Japan', <http://www.isc.meiji.ac.jp/~sumwel_h/links/linkJ04.htm>

'The London Court of International Arbitration', <http://www.lcia-arbitration.com/lcia/lcia/>

'Looking ahead', <http://www.fstech.co.uk/thebigfeature.htm>

'Love Bug probe widened at BBC News Online: Sci/Tech', <http://www3.overture.com/d/sr?xargs=00u3hs9yoaT00KwTCD%2FQv9GIIIdbXg81xBHu8fdsXaVhIrg%2F6twv5cFI8IvJd4R8fxILGDa6e0sDa4uRTrYvmm%2F56FQjYvMG6N5iASFKAuw4bPjYXHjBeaMeSJjzky3U2GF2u2Ay3sA4CCuzwn3sNeRLIUdZDykiRaT2JDv5rVfMk9ShCtaK2LvQHmziUaM3%2FYk%2FITmg%2Facd%2BShEr9vVbIVas0%2BHi9BUxx3g%3D%3D>

'The Marine & Fire Insurance Association of Japan', <http://www.sonpo.or.jp/outline/gaiyo.html>

'Microsoft Industry Solutions Review: Public Services for Local Government vol.2', <http://www.microsoft.com/japan/PARTNERS/industry/misr/pub2xso2.htm>

'Ministerial Conference of the G-8 Countries on Combating Transnational Organized Crime, (Moscow, October 19-20, 1999), COMMUNIQUE', <http://www.moj.go.jp/PRESS/991020-1-1.html>

'*Minpô* (Civil Law)', <http://www.houko.com/00/01/M29/089.HTM>

'*Minpô no manabikata* (How to learn Civil Law)', <http://www.nomolog.nagoya-u.ac.jp/~kagayama/howtostudy/howtociv.html>

'*Mitsui-Sumitomo toraburu; Seishiki-happyô okureru, jôhô-kôkai ni kadai* (A system error at Sumitomo-Mitsui; the official announcement delayed, the problem of disclosure)', <http://www12.mainichi.co.jp/news/search-news/861311/8eO88e48fZ97F-0-12.html>

'*Mondex-jikken no nihon ni-okeru jôkyô* (The situation of Mondex test in Japan)', <http://law.rikkyo.ac.jp/98zemi/mondex4.HTM>

'Money laundering: EU Directive to be extended', <http://europa.eu.int/comm/internal_market/en/finances/general/launden.htm>

'Money laundering: The International And Regional Response' published by Asia/Pacific Group on Money Laundering Secretariat, <http://www1.oecd.org/fatf/pdf/APGBack-1998_en.pdf>

'Montesinos had accounts at BONY that facilitated his money laundering' <http://www.moneylaundering.com/index.htm>

'NATIONAL NEWS: One-stop money e-shop to open NEWS DIGEST', <http://globalarchive.ft.com/globalarchive/articles.html?id=010821000823&query=account+aggregation>

'Nations Worry About a Rise In On-Line Money-Laundering', <http://www.monkey.org/geeks/archive/9703/msg00008.html>

'NEC solutions, Weekly Topics Vol. 105', <http://www.sw.nec.co.jp/column/backnum/11/115.html>

'*Netbanking akuyou, Beiôtegin de sagi, Anzentaisaku saigo ha hito* (The abuse of Internet banking, a fraud in a major US bank, the last resort of safety measures is 'human beings')', <http://www.yomiuri.co.jp/bitbybit/bbb07/261701.htm>

'*Netbanking de hakensyain ga yaku 370 manen sasyu, Keisichô* (A temporary staff obtained 3.7 million yen by abusing Internet banking, The Metropolitan Police stated)', <http://www.mainichi.co.jp/digital/netfile/archive/200205/10-2.html>

'NetLingo Dictionary of Internet Words', <http://www.netlingo.com/lookup.cfm?term=portal>

'*Network-jô no fuseikoui ni kansuru siyousyasekinin nokentou* (An analysis on employer's liability on online unlawful behaviour)', <http://www.kisc.meiji.ac.jp/~skondo/ethics/genko000920hp.pdf>

'The New Basel Capital Accord: an explanatory note', <http://www.bis.org/publ/bcbsca01.pdf>

'New crime measures have cops all ears', <http://www12.mainichi.co.jp/news/mdn/search-news/837080/DoCoMo-0-3.html>

'New FSA help for consumers on making the most of the internet', <http://www.fsa.gov.uk/pubs/press/2001/065.html>

'The New Hacker's Dictionary', <http://www.tuxedo.org/~esr/jargon/jargon.html#hacker>

'New JR SUICA CARDs for smooth traveling in Tokyo', <http://www.tcvb.or.jp/en/hot/sizzling/0112/sizzling_12c.html>

'New online 'account aggregation' service will not be regulated, warns the FSA', <http://www.fsa.gov.uk/pubs/press/2001/057.html>

'New privacy law easy on media', <http://www12.mainichi.co.jp/news/mdn/search-news/846176/diet20data-0-2.html>

'New Stand-Alone E-Commerce Insurance Policies for First-Party Risks', <http://www.irmi.com/expert/articles/rossi006.asp>

'New Stand-Alone E-Commerce Liability Insurance for Third-Party Liability Claims (Part 1)', <http://www.irmi.com/expert/articles/rossi004.asp>

'*Nihon chiteki-zaisan chûsai sentâ* (Japan Intellectual Property Arbitration Centre), <http://www.ip-adr.gr.jp/>

'Nikkei net', <http://www.nikkei.co.jp/sp2/nt48/20020615eimi204515.html>

'*Ohsyû online hanzai jouyaku ni soshikiteki-na-kougikoudou* (An organisational protest against the draft European Convention on Cybercrime)', <http://www.zdnet.co.jp/e-businenn_topb4f5b96f>

'Operational Risk Management', <http://www.bis.org/publ/bcbsca07.pdf>

'Opinion 4/2001 on the Council of Europe's Draft Convention on Cyber-crime', <http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp41en.ht

m>

'*P-8 Kokusai-soshiki-hanzai jôkyû senmonka kaigou no 40 kankoku* (P-8 Forty recommendations against international organised crime prepared by the Senior Specialists Meeting)', <http://www.mofa.go.jp/mofaj/gaiko/summit/birmin98/bun_40.html>

'*Pasokon shittaka jiten* (PC dictionary)', <http://www.nttpub.co.jp/paso/index.html>

'Patents Act 1977', <http://www.jenkins-ip.com/patlaw/pa77.htm#s1>

'The Policy of Protection', <http://www.nwfusion.com/research/2000/1023feat2.html?nf>

'Prepare for the worst', <http://www.darwinmag.com/read/120100/worst_content.html>

'Prepare for the worst', <http://www.darwinmag.com/read/120100/worst_content.html>

'The present and the future of Lloyd's (*Lloyd's no genjô to syôrai)*', <http://www.yasuda-ri.co.jp/quarterly/data/qt31-2.pdf>

'*PRESARIO 229x sirîzu gokounyû no okyakusama he* (To whom purchased PRESARIO 229x computer series', <http://www.compaq.co.jp/support/presario/info/service/pre_v.html>

'Proceeds of Crime Bill (HL Bill85)', <http://www.publications.parliament.uk/pa/ld200102/ldbills/085/2002085.pdf > and its explanatory notes <http://www.publications.parliament.uk/pa/ld200102/ldbills/057/en/02057x>

'Profile of the BIS — Bank for central banks', <http://www.bis.org/about/profcbank.htm>

'Proposal for a European Parliament and Council Directive amending Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering', <http://europa.eu.int/comm/internal_market/en/finances/general/com352en.pdf>

'Prosecutors, Police and Judges', <http://www.edu.tuis.ac.jp/~b97049/climinal2.html>

'Publication 833 Joint Recommendation & Article 1', <http://www.wipo.int/about-ip/en/development_iplaw/pub833-01.htm>

'*Puraibasi mâku to wa* (What is the privacy mark?)', <http://www.kcs.co.jp/p-mark/privacy_1.htm>

'R v. Gold and Schifreen [1988] 2 WLR 984', <http://www.underground-book.com/chapters/ccm/Gold.html>

'Regulating Cyberspace', <http://www.bileta.ac.uk/00papers/teichner.html>

'Regulations and Documents related to Anti-Money Laundering', <http://www.fsa.go.jp/fiu/fiue/fhe001.html>

'Regulations at the Financial Services Agency', <http://www.fsa.go.jp/fiu/fiue/fhe001.html>

'Risk Management Discussion Forum', <http://260.teacup.com/ysugimoto/bbs>

'Risk Management Strategies', <http://www.c-risk.com/Construction_Risk/RM_Strategies_01.htm>

'Risk Transfer Programs: An approach to greater risk control', <http://www.chubb.com/businesses/art/>

'*Risuku-manejimento toshiteno houmu-senryaku vol.1* (The legal strategy on risk management vol.1)', <http://jdc.sun.co.jp:10000/developers/column/column0110_1.html>

'*Risuku to konpuraiansu* (Risk and compliance)', <www.zenginkyo.or.jp/pub/pamph/pdf/dp1-7.pdf>

'*Rokudai Kigyô Syûdan no kisochisiki* (The basic knowledge of six *Zaibatsu*)', <http://www02.u-page.so-net.ne.jp/pb3/keikyu-t/6dai.html>

'Russian money launderers plead guilty', <http://news.bbc.co.uk/hi/english/world/americas/newsid_645000/645717.stm>

'*Sakura KSC unyou no shinkin-saito, fusei-kakikae higai* (The incidents of unauthorized alteration on the websites operated by Sakura KSC)', <http://www.mainichi.co.jp/digital/netfile/archive/200003/27-4.html>

'The Scottish Law Commission', <http://www.scotlawcom.gov.uk/index-1.htm>

'Scraping Phobia Yields To Business-Case Merits', <http://globalarchive.ft.com/globalarchive/article.html?id=020305001872>

'searchWebManagement.com Definitions',

<http://searchwebmanagement.techtarget.com/sDefinition/0,,sid27_gci213900,00.html>

'Second Commission Report to the EUROPEAN PARLIAMENT and the COUNCIL on the implementation of the Money Laundering Directive', <http://europa.eu.int/comm/internal_market/en/finances/general/launden.pdf>

'Section 3 of the Computer Misuse Act 1990: an Antidote for Computer Viruses!', <http://webjcli.ncl.ac.uk/1996/issue3/akdeniz3.html>

'*Sécurité Informatique : la loi* ', <http://cri.univ-tlse1.fr/documentations/securite/loi_penetration.html>

'*Setagaya Cable Kasai* (Setagaya Cable Fire: A 100 years of the urban disaster)', <http://xing.mri.co.jp/research/research/bousai/setagayacable.html>

'Security Online', <http://www.nildram.co.uk/primers/security.shtml>

'Serb hackers' on the rampage', <http://news.bbc.co.uk/1/hi/world/europe/712211.stm>

'*Site shinnyuû: Secutiry-koushinkoku Nippon* (Developing country on computer securityJapan) ', <http://www12.mainichi.co.jp/news/search-news/811991/83T83C83g90N93fc-0-6.html >

'Social Engineering', <http://www.atmarkit.co.jp/aig/02security/socialengineering.html>

'Social Engineering', <http://www.seas.rochester.edu:8080/CNG/docs/Security/node9.html>

'Social Engineering by Daintry Duffy', <http://www.darwinmag.com/read/120100/defenses_sidebar1.html>

'*Songai Baisyô - Kinsen Baisyô* (Redress of Damages, Monetary compensation)', <http://www02.u-page.so-net.ne.jp/rb3/tortslaw/3-3aDamages.HTM>

'*Sonota no risk kanri* (Other risk control)', <https://www.jbic.go.jp/japanese/investor/siryou/risk/others.php>

'Spyonit', <http://www.spyonit.com/>

'The St. Paul Companies Educates Washington, D.C.-Area Agents and Brokers about E-Commerce and Technology Risks',

<http://www.risk-engineering.com/rep/s/knowledge_navigator/search/kno_quickview_popup.jhtml?docId=256440&Links=CYB,RISK&image=yahoo#>

'Standards of TC68/SC2',
<http://www.iso.ch/iso/en/stdsdevelopment/tc/tclist/TechnicalCommitteeStandardsListPage.TechnicalCommitteeStandardsList?printable=true&COMMID=2193>

'Statutory Instrument 1997 No. 3032',
<http://www.hmso.gov.uk/si/si1997/73032--b.htm>

'Stock Hoax Suspect Had Motive',
<http://www.wired.com/news/print/0,1294,38552,00.html>

'"Suck sites" and Trademark Infringement',
<http://www.kaltons.co.uk/TMandhyperlinking.htm>

'Suica' <http://www.ireast.co.jp/suica/03.html>

'Sumitomo Marine and Fire Insurance',
<http://www.sumitomomarine.co.jp/english/index.html>

'Survey Reveals Business Not Prepared for E-Risks',
<http://insurancejournal.com/html/ijweb/breakingnews/archives/national/na0700/na0731004.htm>

'*Syakai kôgaku* (Social Engineering)',
<http://www.ut-info.com/security/se.html>

'TC 68-SC 2',
<http://www.iso.org/iso/en/stdsdevelopment/tc/tclist/TechnicalCommitteeDetailPage.TechnicalCommitteeDetail?COMMID=2193>

'Technology and Cyber risk', <http://www.tennant.com/p-cyber.html>

'Terrorism Act 2000',
<http://www.hmso.gov.uk/cgi-bin/htm_hl3?URL=http://www.hmso.gov.uk/acts/acts2000/00011--x.htm&STEMMER=en&WORDS=comput+misus+&COLOUR=Red&STYLE=s>

'The Terrorism Act 2000',
<http://www.legislation.hmso.gov.uk/acts/acts2000/20000011.htm>

'There is an old saying that "what you don't know cannot hurt you." When it comes to money laundering, nothing could be further from the truth',
<http://www.aciworldwide.com/trends/loss_prevention.asp>

'Third-Party Liability E-Commerce Risks and Traditional Insurance

Programmes', <http://www.irmi.com/expert/articles/rossi003.asp>

'Tokyo Mitsubishi Direct', <http://direct.btm.co.jp/kiyaku/index.htm>

'*Toumen no sôkaiya-nado heno taiousaku ni-tsuite* (The urgent countermeasures against *sôkaiya* issues and the like)', <http://www.keidanren.or.jp/japanese/policy/pol142.html>

'*Tôshbia no after service, homepage no iryoku 700 mankai* (The power of the homepage, seven million hits for the Toshiba After-service problem)', <http://www.acc.ne.jp/~h-kyoko13/kakokizi/tosibamondai.htm>

'Tracking money trails with technology', <http://news.com.com/2008-1082-276078.html>

'UK gets new one-stop site', <http://globalarchive.ft.com/globalarchive/articles.html?id=010728001043&query=account+aggregation>

'UN General Assembly Special Session on the World Drug Problem', <http://www.odccp.org/adhoc/gass/ga/20special/featur/launder.htm>

'uk, outsourcing, reduce business operating costs ', <http://www.outsourcer.co.uk/core-competency.htm>, <http://www.outsourcer.co.uk/efficiency.htm>, <http://www.outsourcer.co.uk/cost-effectiveness.htm>, <http://www.outsourcer.co.uk/freedom.htm>

'Unauthorized Computer Access Law (Law No. 128 of 1999)', <http://www.npa.go.jp/hightech/fusei_ac2/UCAlaw.html>

'Unauthorized Computer Access Countermeasure Guidelines', <http://www.ipa.go.jp/security/english/access-guideline-e.html>

'Unauthorized Computer Access Law (Law No. 128 of 1999) (provisional translation)', <http://www.npa.go.jp/hightech/fusei_ac2/UCAlaw.html>

'Unisys, AIG eBusiness Risk Solutions Partner To Minimize Business Risk From Cyber Attacks', <http://www.unisys.com/news/releases/2001/apr/04037082.asp>

'United Nations Office for Drug Control and Crime Prevention (ODCCP), Global Programme Against Money Laundering', <http://www.imolin.org/ml99eng.htm>

'Update to A Guide to the UK Legal System by Sarah Carter', <http://www.llrx.com/features/uk2.htm>

'*Wagakuni niokeru jûyou-infura bouei notameno houseibi no mondaiten memo* (The issues on introducing law for protecting important infrastructure in Japan)', <http://www1.sphere.ne.jp/netlaw/sec/cipj.htm>

'Waiting for 'Love' Suspect', <http://abcnews.go.com/sections/tech/DailyNews/virus_000508.html>

[1]The Wall Street Journal dated March 10, 2000. See 'Investors Are Betting That Bank of New York Will Emerge Unscathed From Investigation', <http://www.russianlaw.org/wsi100300.htm>

'Web-based email services offer employees little privacy', <http://news.com.com/2102-1017-246543.html>

'Wells Fargo revs up account aggregation wagon', <http://sanfrancisco.bizjournals.com/sanfrancisco/stories/2001/01/22/newscolumn2.html>

'What's Domain?', <http://www.uma.nu/domain.htm>

'What is BS 7799?', <http://emea.bsi-global.com/InformationSecurity/Overview/WhatisBS7799.xalter>

'The WIPO Arbitration and Mediation Centre', <http://arbiter.wipo.int/center/background.html>

'Working Paper on the Regulatory Treatment of Operational Risk', <http://www.bis.org/publ/bcbs_wp8.pdf>

'Xerox fires 40 for online pornography on clock', <http://news.com.com/2100-1001-231058.html?legacy=cnet&feed.cnetbriefs>

'Yahoo! Domain', <http://domains1.yahoo.co.jp/help/13.html>

'Yodlee strengthens UK presence', <http://www.yodlee.com/company/pressreleases/uk.html>

'*Yôgosyû* (a glossary)', <http://www.dandi.co.jp/yougo.html>

'THE YOMIURI SHIMBUN/DAILY YOMIURI: CHIYODA MUTUAL FAILS; AIG SAID POISED TO HELP', <http://search.ft.com/Search/MultiSearch/globalarchive.jsp?docId=001011003330&query=chiyoda&resultsShown=20&resultsToRequest=100>

'You say Professional Services, I Say B2B Activities', <http://www.irmi.com/expert/articles/rossi010.asp>

'Zenginkyô',
<http://www.zenginkyo.or.jp/abstract/katsudou/abstract0406.html> .

OTHER RESOURCES

CD-ROM of 1997 Encyclopaedia Britannica.