

***Panacea Limited***

**IT solutions & services with lifetime support**

# **Information Security, Business and the Internet**



**Prepared by:**  
*Clive Blatchford*

---

# Information Security, Business and the Internet

*This short article considers the perception of a selected number of small to medium sized enterprises in 1998/9 towards the security problems of e-commerce. It emphasises the need for common sense and personal responsibility of individual business users. The centralised approach of those in the IT Industry in the defining of problems and proposing of solutions is questioned following a narrative based study!)*

## Introduction

**Pundits of global networking have announced the start of the next "Longwave" of economic prosperity -a possible 5th Kondratieff Cycle. The popular financial press has named it as the move from the Old to the New Economy! E-commerce is the highly visible face of such change.**

The Business Community is increasingly excited by the resulting opportunities from the rich melding of IT/computers, Telecommunications and associated Media technologies.

Benefits will accrue to those that consider the network as the market and the network as the channel for the market. Books to planes will be purchased by and delivered to the client over the ubiquitous Internet and World Wide Web. The stock market investor seeks a major shift in future corporate profitability driven by the exploitation of IT/Telecommunication services. The Stock market levels reached daily in USA and Europe, highlights the business expectation from the massive investments in the networked infrastructure, if not in all the small opportunistic Dot.com start-ups. The retail failures such as Boo.com will only add to the sum of the technological enablers as their detritus feeds the imagination of entrepreneurs and potential investors alike. The astronomic valuations of dot.com enterprises on the NASDAQ, and other markets, of late 1999 may be over as hard headed realism prevails, but those enterprises with real infrastructure assets should command a premium in the market place].

The networked economy is critically dependent on the speedy access to, and manipulation of, information underpinning goods and services. Individual enterprises are creating pools of administrative and technological knowledge that, if effectively exploited, will sustain a huge market of fine grained business opportunities. Information sources are bonded together via a clever, yet ultimately "kludged", manifestation of many private corporate networks (the intranets) interfaced with the publicly available telecommunication services (including the Internet!).

Global corporate mega-mergers are redefining product and service supply. Technological change is creating new competitors as well as new markets. Enterprises with substantially different backgrounds are seen as selling the similar product to the same client. Time-Warner and America On Line/AOL are merging to compete more effectively for the consumers leisure time. Walt Disney/Bona Vista and Yahoo! are likely candidates in seeking suitable infrastructure partners. In the USA in 1999 a customer satisfaction survey, AOL services beat all the main TV networks for content!.

Small technological enterprises are catalytic in markets, becoming rich beyond their dreams, as short run, monopolistic IT suppliers. Others, with actual or potential, client information databases are expounding the Internet as the medium for the marketing message. The huge valuations of small loss making enterprises reflects this advertising possibilities.

The truism is that the future is always uncertain. The risks are great but the business opportunities are even greater from more commerce, with more customers, in more places, at potentially much lower costs.

In summary, at its basic, the Internet may be considered a "transport mechanism" increasingly easy to access and use (thanks to such excellent technology as the World Wide Web and

---

associated Network browsers): at its most sophisticated it is the bedrock of the New Economy as E-commerce especially creates the market place for buying and selling products and services. The business world will consider each opportunity in the context of this broad spectrum.

### **Networking- The Business Opportunities**

E-Commerce is now a reality. A retailing revolution from books to perishable groceries is underway as goods are bought remotely. Some sectors are being revitalised, especially software, book and CD sales. The major UK supermarkets chains, such as Sainsbury's, Tesco's, estimating that up to 10% of grocery shopping will be via the Internet, in the early 21st Century? This trend will continue as each new company jumps on an apparently unstoppable "bandwagon".

The actual or potential on-line client database of even the smallest dot.com retailer is driving the hypobolae! E-Commerce company valuations are being driven both by the potential on-line sales as well as the advertising revenue that can accrue from selling space on high accessed web sites. An individual client profile can be worth \$1,500 to a Stock Market predator, even if the relationship has never been translated into a profitable sale!

In the USA, major E-commerce enterprises include Amazon (Books etc), eBay (Auctions) and Bluemountain (greeting cards). Their reach is now global. The last company was bought by Excite at Home for \$780m in 1999, although there is no obvious correlation between free E-Mail cards and a profitable revenue stream? In Europe, Internet selling is both a national and increasingly a transnational opportunity. Business Strategies, economic analysts, recently forecast British shoppers spending some £8b plus a year buying goods on-line by 2004. Internet shopping sites will become commonplace! Every major retailer has a Web site. Even the local, speciality store, providing farm products, in the rural heartland is getting into the act.

The design of the Web site may offer little more than a simple image (properties with estate agents). Others will offer richer graphics and text (Antiques auctioneering). The ultimate technological tool kit will allow dynamic multi- media with the virtual inspection of the product before purchase. (The IPIX technology of Interactive Pictures Corporation has been used by Elite Aviation in the USA to buy a \$23m Gulfstream corporate jet over the Internet.

The quality of graphics was such that the buyer could nearly "kick the tyres" before committing!) Technological cutting edge today will become common place tomorrow. Most on-line buyers however will be content with a simple yet robust interface with the supplier, and the assurance that their low value selection arrives on time with the minimum of administrative and financial hassle!

The E-commerce future considers national boundaries as irrelevant. The global economy will evolve through the catalyst of the business enterprise exploiting technology with a sympathetic commercial, legal and, above all, political infrastructure. It is essential, however, that the national and international constraints on the physical movements of goods and services be fully addressed. The on-line virtual world may bring the image of the product to the buyer; it may allow the processing of the financial transactions; it does not however guarantee timely delivery, as expected, by the customer. A 1999 survey showed that 10% of goods did not arrive at all! (Consumer International-a global federation of some 245 consumer organisations-9/1999)

The success of the myriad of on-line sites will be conditional on the physical delivery mechanisms. The true winners in the E-commerce wars will be those retailers with best working relationships with the main international distribution companies.

### **E-Commerce- The Problem of Credibility**

Many financial pundits are warning that financial speculation in Internet Stocks has all the hallmarks of a business bubble. Public announcements or private rumours of the long-term

---

positive business impacts had resulted in astronomic valuations of many young, unknown enterprises. Day Traders use IT to trade "on the margin" in highly volatile IT Stocks with extended lines of credit, has become a social phenomenon in the USA!. Yet E-commerce especially, is no Dutch Tulip or English South Seas mania [Beckman], [Chancellor].

Technologically assisted, intra-enterprise networking especially will bring operational rewards to the successful company. The "retailing bubble" of the dot.coms however may be pricked if a number of operational exposures are not recognised within the various legal, regulatory, financial or commercial frameworks. The purchasing public can be very fickle if they do not get value for money. Outright fraud over the Internet must be the ultimate nightmare for both the customer and retailer. Security awareness therefore, in its widest sense, is an imperative for the business community. A history of undelivered, paid goods will sour any business link. Unauthorised and/or fraudulent use of financial and personal data will destroy trust relationships so painstakingly built up over time.

Much of business is increasingly little more than the processing and massaging of information. This is most obvious in the Financial Sector. The financial services industry is profitable through trading in "soft products" that are derived from information accumulated by the investment bank, the insurance company or the savings and loan/building society.

Such enterprises are exploiting the Internet technologies; with browsing the Net for new product ideas and potential new markets becoming a legitimate business task! Modelling tools, communication protocols and programming standards, has resulted in information research analysis and product development in the hands of the marketing "front office".

This shift from the operations "back office" has many benefits, including time to market and product innovation. Poor controls (including total product costs) however may result from this market reorientation within the enterprise A co-ordinated, rigorous internal review process is essential to ensure operational viability and integrity. Recent "Internet Banking" fiascos have highlighted the poor preparations of even the largest High Street companies as they jockey for market share.

Business opportunities can be considered from many perspectives. At one extreme, the reputable, trustworthy, financial institutions such as HSBC-Midland/First Direct (a retail bank without any branches with IT and Telecommunications substituting for buildings and people):. the other extreme dubious, virtual, "off-shore" entities offering questionable social/leisure pursuits or highly obscure financial stocks and bonds.

The Internet user is bombarded with unsolicited junk mail through "spamming", the ability in one operation to broadcast to all, of e-mail messages. In the USA, there have been well-publicised cases of network scams on financial products (Personal Choice Opportunities/PCO and a \$100m Life Insurance Scam), or on bogus share offers (Interactive Product Services/IPS and a non-existent product). Rapid network communication facilitates the "pyramid selling" of greed, through rumours, innuendoes etc. Even professionals (brokers) may be tempted in the right social climate! Creating an aura of respectability to the more outlandish claims (historical shades of any financial bubble?)

Such scams have been less prevalent in Europe, as they appear inhibited by the natural barriers of language and currencies. Further economic and political integration through the European Union may however change this. Even a small percentage of gullible recipients in a potential market of millions can generate a lot of revenue to the unscrupulous organisation.

### **Networking- The Impact on Corporate Functions**

The Internet as a viable delivery system accessing "publicly available", yet corporate databases/information, will do more than redefine products and services, it will irrevocably change work and employment patterns.

---

Networking has had a profound impact on the transaction costs of the larger enterprise. Most modern business techniques are being enhanced by the availability of computer networking. The US based multinational corporation is in the vanguard of corporate restructuring. In Europe, Britain leads the "outsourcing" tables. Work is being reallocated over company boundaries, with tasks being shifted "upstream" to suppliers and contractors or "downstream" to distributors and clients/customers.

The historic, vertical integration of the larger enterprise is being replaced by the more flexible and responsive core enterprise with its many "teletesting" partners. The early economic basis for vertically integrated companies was that direct control of all resources would reduce the time/costs of "legal" negotiating between companies. Transaction costs have fallen generating new opportunities. Real time networking will facilitate the mixing and matching of relationship between business entities. Concepts such as "just in time replenishment" do not require total control of the supply process in a truly networked age.

The obfuscation of earlier corporate boundaries can bring problems as well as opportunities! Global, public networks will allow distant competitors to infiltrate local environments with little or no effort. This may provide real products and services thus increasing customer choice, but electronic access can result in the stealing of other's corporate resources (recent well publicised cases of "piggy-backing" international phone services on private networks).

Competition is the lifeblood of capitalism. A successful, dynamic market needs a mixture of investment, short and long term. The local emergence of a range of valuable networked products and services could be inhibited by business fears that investment cannot be justified. The emergence of global opportunists moving in and out of a market, "costlessly" and with "impunity", may destroy the most robust business case.

The extreme case of "costless" competition are those individuals and companies that are inherently fraudulent, adversely impacting the consumer and thus detracting from the development and resilience of the market. Some early products offered over the Internet have either fallen into this category or have characteristics that lend themselves to fraudulent use (on-line auctions and bidding against one's self to inflate prices).

The network must be policed, although there is continuing debate between the need for central control, at various level of government versus self-regulation, and the dynamics of the commercial market place driven on an application by application basis.. Notwithstanding any legal and regulatory infrastructure, and enforcement process, the "buyer beware principle" must prevail. Business common sense and vigilance is probably even more relevant within the interactive global market than in the local context?

The customer for a product or service, everything else being equal, would apparently prefer the trust relationships prevailing in the corner shop to the E-commerce Web site. The on-line service therefore must show measurable advantages of availability, product range and cost!

### **E-Commerce- The Logistical Implications**

To many corporations, E-commerce may be considered the corporate "front office", allowing a transparent view to the customer of all the "back office changes" brought about by the network opportunities; to others it is just about a web address on the advertising material, with no discernible mechanisms in place? Most E-commerce processes now allow retail customers access to on-line catalogues that complement the conventional transactions of mail order and telephone order entry. The final form of the enterprise is yet to be determined. The internal control processes will need to evolve in parallel. Safeguarding, yet not overly constraining the evolution of the business. Customer relationship management (CRM) has underpinned the blossoming of "out sourced" call centres. The potential loss of control of valuable, exploitable customer data however may be a countervailing force. The balance between the various commercial organisational structures is being determined by the market place.

The big "winners" in e-commerce will those that dominate the world of International storage and distribution not necessary those that offer the on-line retailing. Federal Express (FDX), United Parcel Service and DHL and the revitalised "State" Postal Services (e.g. Deutsche Post, GPO-

---

Parcel Force) will have a pivotal role in the evolution of "home shopping". In November 1999, the biggest flotation in USA history saw \$5.5b raised by UPS giving it a market valuation of \$84b. The basic operational viability of home delivery services however, have been questioned. A recent Abbey National/NOP Survey showed that on-line shopping may be the way forward, but that the systems of delivery are still too rigid and that many ordered products never appear! The control needs of the various billing and delivery processes are the same whether or not the initial goods are ordered on line or in face to face customer/supplier relationships. The proliferation of loss making, free delivery services for Internet purchases in the major urban areas can only compound the problem. (UrbanFetch.com, Kozmo.com etc)The success or failure of E-Commerce will depend on the professionalism of customer service especially of the overall attitude to physical logistics of meeting the consumers increasing retail expectations.

### **E-Commerce- Organisational Change (the USA experience)**

Two important business sectors may be used to illustrate the rapidly organisational implications of E-Commerce- Car retailing and House Purchasing.

Previously one would buy a car on-line by accessing any number of Web sites run by the Main Dealers or selected independents to obtain the necessary details-price, availability. The inquiry would be routed to a traditional dealer with the sale being closed by face to face haggling at the dealers physical site. Systems are now in operation that require no interaction with the dealer to complete a car purchase. In California, Web sites such as CarsDirect.com gives potential car buyers the manufacturers retail price and the negotiated price possible in an extensive network of dealers. Going even one step further, Microsoft's CarPoint Web site has joined forces with Ford Motor Company to create a "build-to-order" so that the on-line shopper can order directly from the factory from the comfort of their own home. Other hardware and software companies such as Dell and Trilogy are behind moves to buy dealerships on the outskirts of the major cities. The successful application of the Internet for instant pricing will put increasing pressure on the traditional ways of selling cars. This is recognised in the USA with the e-commerce heads in Ford and General Motors backing the concept of the "e-dealer". Notwithstanding this virtual market place "bricks and mortar" will remain important in the selling of cars, the potential customer will still enjoy the test drive!

Estate Agents have increasingly put their portfolio of properties on the Internet to facilitate sales. This is a logical extension of their mailing of details to prospective purchasers. Such an on-demand system must eventually reduce the vast bulk of unnecessary correspondence benefiting both professionals and clients alike. But on-line selling of houses could possibly lead to demise of the Estate Agent.

There has been an increase in the selling of houses by the owners directly over the Internet. This has been facilitated by "Home Advertising Sites" offering free/low charge net listing services. Such Net entrepreneurs may charge up to £200-300 yet save on Estate Agent fees of thousands of pounds. (Homes.com etc) This may cut out the Estate Agent. The final organisational form of the industry will depend on achieving a balance between the control of the information about the product being offered and that over the register of potential buyers. The Web sites will need tight security controls over the legitimacy of the data base contents and the credibility of purchasers. The strength of the housing market may however be the final arbiter in the organisational change. A role played by the professional middleman is always questioned in a healthy business market! In the next housing downturn the well connected, local estate agent could prevail.

The advent of the "formal survey/selling package" of house details may however be the catalyst for change. In the USA, the comparable pre-listing appraisal is increasingly being used as a on-line marketing tool. The detailed property descriptions are put on the network accompanied by an analysis of some 6 alternative properties. The Chicago based Appraisal Institute is offering such a scheme following a national test of some 300 appraisers (in the UK- mortgage surveyors) from 11/1999 to 3/2000. The prototype site can be visited at [www.MFHB.com](http://www.MFHB.com)

Obviously the Internet may be more conducive to the buying of a standard product, a motor car, than to a unique family home, but the market boundaries will continue to be tested. The availability of ready information to assist decision-making must make the final purchaser less dependent on

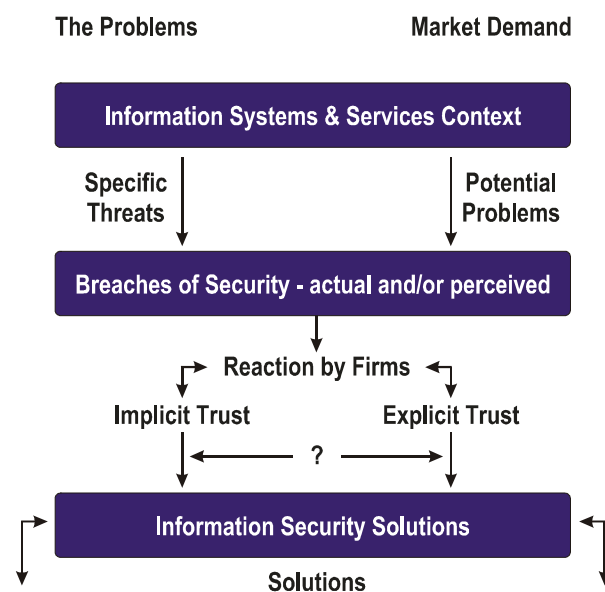
---

the marketing/sales skills of the middleman. The profiles of many businesses will change dramatically!

### Networking- the Security Concern

Information Security, with its elements of confidentiality, integrity and availability, must be considered at the communication, processing and information storage level.

The businessman will demand an adequate and measurable level of risk associated with the use of network services. This is usually translated into attaching various probabilities to his future actions. Business opportunities from the Internet involves risk seeking-this is understood. They are definitely risk adverse, however when it comes to the exploitable services being provided by others. They want the network to be robust. Yet outages of various Internet service providers, for whatever reason, has highlighted its continuing vulnerability. Business applications must trust the underlying IT and Telecommunications networked facilities offered by the "transport" services. This trust could be misplaced!



In e-commerce, the basic availability and integrity of the website and its contents is essential. This may range from "informative" financial advice or statistics on a reputable "Message Board" to the subsequently "performative" pricing of the retailers on-line "e-catalogue". Although not caused by unauthorised amendment - the recent experience of Argos apparently offering coloured TVs over the Internet at £1.99 has raised important legal and commercial questions. The smaller E-Commerce outlet would have far less muscle to resolve any subsequent mayhem from the unauthorised tampering of their product and service information.

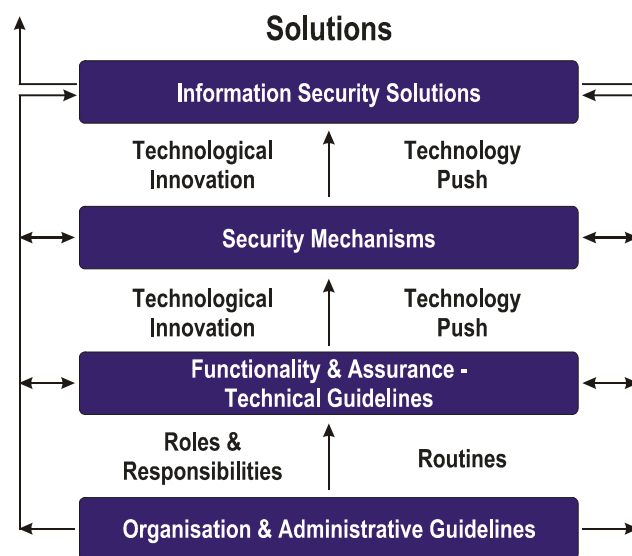
In the infinitely adaptable world of commerce, however, even operational glitches can generate profitable business opportunities. Recently, the free Encyclopaedia Britannica web site generated so much access traffic that the system went down. Many users implies a huge potential advertising market. Would be Stock Market investors revalued the company accordingly!

Some potential networked IT applications have always been of acute concern to the cautious business man (e.g. the remote electronic processing of orders and the handling of payments). The use of debit and credit cards for such transactions require secure registration schemes of customer numbers and card details. The ease by which spurious, yet apparently, valid credit card numbers may be generated has raised questions concerning the cosy relationships between the card issuing companies and the global banks. More on-line reconciliation with client accounts may be necessary to avoid miss-billing.

In addition new technology will be implemented. This will include hardware and software that uses encryption for the privacy and integrity of data including card details. Such security packages must now be a fundamental service of the major Internet access providers especially those offering on-line shopping sites. Global solutions however require both a political/legal infrastructure as well as technical fixes in which to enhance business controls.

### Networking- the Sources of Threat

Criminology is the study of crime. It defines crime, describes the perpetrators and victims, propounds causes and solutions; either pro-actively in crime prevention or reactively in finding and punishing the guilty. Unfortunately, what constitutes crime is contested, with much ontological debate and confusion! [Foucault] The sharpest conflict is between those that believe crime is a recognised "deviancy", from some universally accepted moral and/or legal code (the "classical" perspective), and those with crime is an "ideological concept", political and social constructs enforcing a specific politico-economic system. This latter radical, or "critical", perspective has underpinned much social thinking in the USA and Europe since the WWII.



The classical versus critical debate continues to vex the Criminal Justice Systems. Classical criminologists consider crime within a simple "hedonistic calculus" of individuals exercising free-will, committing an offence, when the perceived rewards outweigh the chance of capture and punishment. Crime prevention would be achieved by reducing the opportunity, increasing chance of capture and/or raising the sentencing tariff. Critical criminologists however, maintain that we are now facing a much more complex philosophical argument. Many "crimes" may result from the perpetrator believing that there is a perceived, inherent lack of legitimacy of the existing social order. Alternative forms of legal governance are advocated including forms of "social democracy" that have little place for the Capitalist, business community!

Any brief analysis of the source of the threats, and whether or not they constitute a crime, can put the level of operational uncertainty into context. This may be considered from the service provider, the malefactor or hacker perspective.

In a competitive commercial world, the Service Provider may not be committing a crime by the non-availability of a critical service, but failure to assure operational safeguards to the business community has legal and regulatory implications. Obviously, no robust underlying "transport" communication mechanisms- then no E-Commerce. Operational malfunction must be minimised. Independent technical auditing of the total Internet capability may be necessary to ensure the robustness of the "transport" processes to the user enterprise. The lack of clear ownership and thus responsibility of key components may hamper independent review. The Internet may belong to everyone yet no one, but in reality, the service/access providers may find that operational problems may become a major financial liability? There may be a role for national administrations in this world of operational "laissez-faire"?

Responsibility for the robustness of specific Internet applications is more easily assigned. Published studies in "Computer Crime" have reinforced the contention that the majority of attacks on corporate IT come from insiders; employees and recent past employees of the enterprise, "authorised" to access and manipulate information resources.[Elsevier] Collusion between two or more employees may compound the problem. Good administration supported by technology was seen as essential. There has been an abundance of codes of good practice from both the Authorities worried by the apparent vulnerabilities of the commercial and industrial sectors (OECD Guidelines, DTI-The BSI 9977 Code of Practice for Information Security Management etc). The major Accountancy and IT Consultancy firms have emphasised the good administration that could be built on the implementation of common, increasingly, international standards.(II-SF..Generally Accepted Systems Security Principles) Protection against internal malefactors will continue to be primarily driven by good management. Computer controls will assist but not replace human vigilance.

The actions of corporate insiders may be a matter for internal disciplinary processes. However the organisational obfuscation that comes from network may dictate a more consistent industry wide approach to malefactors. The wider social policing may dictate less operational fragmentation?. Finally, external hacking into computer systems for whatever reason must be of concern to a society increasing dependent on the expected benefits of networking. Hacking is defined as unauthorised, primarily, "outsider", access to electronic data and services It is difficult to measure the extent of the hacking problem faced by the smaller businessman. Such enterprises do not have the obvious target kudos of a Government Office or International Bank!

Many hackers take as moral justification their actions as "Latter-Day-Luddite" destroying the "tools of oppression" of the "ruling class"-their computing and communication systems. The rational, "hedonistic" criminal will normally consider the extent of access difficulty or resulting punishment: whereas the advocate of the different social order may just be spurred into greater effort by the tighter control! Rational economic argument on the deterrence value of punishment for hacking may be irrelevant when applied to the behaviour of these people with social "norms" opposed to the providers or users of Internet services. The general public may have been influenced by the generally favourable stance taken by Hollywood towards the young hacker however deliberate orchestrated failure of key networked services will soon change attitudes amongst Internet users!

### **Computer Security- The Solutions Revisited**

Most mainstream "administrative criminology" is not interested in the individual reasons for computer crime, only in altering the situations in which offences can occur. Historically, the study of corporate business victims has been about "situational crime prevention"; implementing security policies and procedures to deter the "criminal".

Designing out crime in computer systems can be achieved by target hardening. This ranges from an architecture with secure building blocks to better operational administration. An overall computer security "Meta" architecture should encapsulate the functionality and assurance criteria that maintain service and data confidentiality (privacy), integrity (avoiding unauthorised change or destruction) and availability (avoiding withholding). Robust operational examples are few! There is some anecdotal evidence, yet to be measured, that improvements in the controls of the major public administrations and multinationals has resulted in some crime "displacement", measured by the factors of;

- spatial-hacking against smaller and less prepared enterprises.
- tactical-alternative attack modes to obtain access privileges, "masquerading" etc.
- targeting-more "destruction" of data or service availability, or criminal fraud.

The corollary is that good individual enterprise level controls may result in hacking into the basic communications infrastructure of the Internet. The expected sustained attack on the message switching mechanisms over the Millennium period did not occur. The ongoing vulnerability of the ubiquitous Microsoft Windows E-mail systems, as illustrated by the "Love Bug" virus and its many variants, however, must be taken seriously. A technical monoculture has significant financial advantages, in "pseudo-biological" terms it is much more vulnerable to the "virus" attack. Lack of

genetic variety can lead to extinction in any population! Complacency and poor security could have a catastrophic impact on many Internet application.

The business world however has benefited from the increased technical concern with networked security. IT components remain fragmented and/or vendor specific, but international standardisation is supporting more secure solutions. Secure networks need a robust, foolproof systems architecture with multiple layers of protection using trusted components and encrypted communications traffic.

Encryption of data and processes, primarily in integrity of individual financial transactions will become a fundamental part of protecting the network. Commercial Internet software suppliers are now offering a range of crypto controls to improve commercial acceptance.

The businessman, especially in the small or medium sized enterprise, will not really be expected to address or even understand the technical problems. He (or she) need only be sure that any implicit (or increasingly explicit) contract with the network service provider reflects an acceptable level of service and has considered the operational hazards. Trying to define what is meant by such an acceptable service underpins all transactions in a complex business environment; whether between the service provider and the enterprise or the individual on-line retailer and the eventual customer. A continuous dialogue between all players is essential, not just a monologue from the technical community.

### **E-Commerce- Creating the Legal Framework**

The need for increased information systems security was reflected in the Queen's Speech for the current legislative session of Parliament. [Legislation] The proposed agenda included an E-Communication Bill and the updating the existing Interception of Communication Act with a new Regulation of Investigating Powers Bill (by the Home Office) to cover E-Mail interception. Recognition of Electronic Signatures and Digital Certificates reflected the importance of encryption techniques in proving customer identity and authenticity and the network integrity of financial transactions. Payment Service Providers to Credit Card Companies and Banks are especially keen to see legally binding digital signatures. Consequentially secondary legislation is likely to apply recognition of electronic signatures to focussing on areas such as consumer credit etc. Voluntary regulatory infrastructure, yet DTI approved, "kite mark" on enterprises offering services but with possibility of government "statutory licensing system if the Business driven schemes fail. There is continuing confusion on the resulting balance between Strong and Weak encryption, especially in the role of data confidentiality? National security will always have a constraint on International Commerce. Such issues are resolved only by trial and error?

International problems will still be faced in the fullest global exploitation of E-Commerce including - service provider liability, IPR-intellectual property rights, and taxation. A question must remain do the smaller companies entering E-Commerce really understand or worry about the security issues, the solutions and the likely cost (for example in applying robust customer digital signatures?)

At the time of writing the debate is acrimonious on the various proposed bills and clauses. The Regulation and Investigative Powers Bill (RIP) especially has raised hackles both amongst civil libertarians (personal freedoms/privacy) and business community (cost of implementing crypto - control processes). What is at stake, is the role of the nation state and its social contract with its citizens within an increasingly global economic system. E-Commerce "equivalency of controls" is the first real test case of the possible global alignment of the new technologies. Solutions should remain flexible.

### **Information Security Controls- Defining the Need**

Do we really understand the information security problem in a rapidly changing business infrastructure? Are the controls adequate in protecting the assets of both the supplier and customer? Control implies at least partial ossification of existing processes! This may be an anathema for the successful entrepreneur?

## Information Security & Questionnaires

The Roman Empire was vast and literate extending uninterrupted over 600 years. Yet of the 10m words of Latin that remain, over 90% is post the advent of Christianity. The winners in the religious, and hence social, struggles for the hearts and minds of the Western Peoples destroyed everything else that was deemed at best irrelevant, at worst sacrilegious! [Vincent] In a similar vein, most of all studies and writings on the problems and solutions of information security have been written by those with a vested interest in "spreading the gospel". There can be no unbiased interpretation of events by the computer vendors, service providers, auditors or even information security experts. The earlier "unbiased" financial auditors have moved rapidly into security consultancy -more problems drive more funded solutions!

In the corporation, there is an increasing dichotomy, more openness can result in less real evidence. Those in power, whether the Finance Director, the IT Manager or Head of Security can ensure an increasing disparity between evidence and reality, if they feel that their actions are open to scrutiny. Not just US Presidents have been known to shred tapes! The corollary is that those not in power can reduce the chance of "corporate downward mobility" by hyping up problem of the "the Millennium Bug syndrome" or corruption and fraud. Whistleblowing can be seen as the ultimate collectivist sacrifice in the Corporate World! The result is thus invariably a demand for more central control over the "unbelievers" - the "corporate" Edicts, Inquisition, and even excommunication!

Historically, the formal questionnaire with its structure and contents has been the main building block in the creation of the Information Security Industry. It has been used extensively in collecting and analysing data on information security matters. Such pseudo-science has bounded the discussion, preconditioning the answers. Often the resulting metrics were given a factual status they didn't deserve! Much subsequent technological development has been made on such self-fulfilling analysis.

Quantification of the problem must have a more solid theoretical preparation. A type of questioning must be adopted that explores the firms and/or peoples points of view, their motivations and their own categories. Even the smallest firm now has a valid position on the need to control their computing resources.

The Questionnaire has many weaknesses, for example, is not just about omitting narration for simpler completion and interpretation-it can omit truth by obfuscating the part played by chance, uncertainties, random events and contingencies. The structure sets limits to what has or could happen, and above all, it can never explain one course of events over another. The bias of the questionnaire is creating the evidence. It is a bias however towards stability, the status quo and what is tried and tested. Yet E-Commerce may be more than just an extension of existing of business practices. Information systems security problems and solutions (if they exist!) must be built up by narrative throughout the enterprise not just by those in power.

Past questionnaires have been submitted by and completed by those with a vested interest. The results have been used as "evidence", endlessly quoted in many contexts-most computer crimes are committed by insiders, hackers are socially deprived nerds etc. The level of awareness and subsequent concern is driven by the questioning process. Are businessmen worried by security concerns of E-Commerce or do the business opportunities outweigh the risk? Is security over the financial transaction the most important consideration by the on-line purchaser and services? (E.g. none delivery of goods more important than unauthorised use my credit card details). Computer Security Concerns and the Internet- diffusion into the smaller firm.

A Qualitative Research Study into the computer security concerns of the smaller enterprises in using the Internet was undertaken. A range of non-questionnaire interviewing techniques were applied.

A secondary aim was to assess how far existing legal and regulatory proposals and the availability and use of secure IT and networking products had resulted in organisational and procedural changes.

---

## Research Area and Methodology

The study, with its two phase interviewing process, allowed some preliminary assessment of whether or not the formal controls, as recommended by the Department of Trade (DTI), were being implemented. Qualitative, fieldwork methods of interviewing and analysis were deemed more appropriate than detailed quantification based on IT budgets, capital inventories (both hardware and software), telecommunication traffic flow analysis and actual incident, audit logging. Study subjects were smaller companies with limited administrative resources for planning, maintaining and extracting such data. In fact, if threats could be foreseen, with reporting controls implemented pro-actively, then IT Security exposures would always be minimal. The state of mind of the interviewee and perception of threats, not cardinal measurement of actual incidents, is essential when measuring utility from changing administration and new technologies. Qualitative analysis gives research visibility to the smaller companies, "real world fears". Business opportunities and constraints however are usually more about perception than reality! Information security may be important but it may not have the pivotal role in decision making as thought by earlier pundits.

### Phase 1- Qualification of Information Systems Controls

The study subjects were selected enterprises applying publicly available, "Open Networking", standard protocols. There was face to face, qualified, discourse using a semi-structured interview technique based on Grounded Theory -the discovering of theory from qualified empirical research. [Glaser] The DTI sponsored "Code of Good Practice" was used to bound the interview and assist questioning. The firms selected for interview had similar information systems profiles. They were small and medium sized enterprises (up to 250+ employees), using primarily networked IBM "Unix RS 6000" or PC systems, who have, or who are contemplating, telecommunications links to external public Internet systems services. The companies included those that are implementing flexible e-commerce software solutions (especially when supporting web site development, intranet and Internet on-line order processing, integrated with the "back office" finance system". [Panacea] Preliminary profiling of the selected firms was with the external service supplier -either sales or service personnel. The subsequent direct contact with customer management followed the scoping review. An initial, biased, non-random, sample of 10 firms was selected, this was subsequently increased to 16 The firms having already expressed some interest in security through the IT service supplier. Firms included small manufacturing and construction/building companies in addition to service sector providers of Information Technology, Food & Electrical Wholesalers, Motor Traders, Estate Agents, Travel Firms, Solicitors and Interior Designers. Phase 2 Testing for relationships-specific questions.

Any comparative evaluation of the information security controls needed an interview with specific questions. The "open questioning process" was loosely based on the DTI "Code of Good Practice" as illustrated below but was highly tailored to meet the technical context of the individual firms. (Following phase 1 preliminary analysis)

In 13 out of the 16 firms, Phase 1&2 were juxtaposed; in the other three cases the interviews reflected meetings with staff of different levels of administrative and/or technical knowledge. Firms, computer networked to others, have installed "situational" computing controls. These may just include administration, from simple after the event audit log reviews to regular allocation of access, identification and authorisation privileges; most however have supplemented primarily human administrative actions with dedicated hardware and software. Simpler solutions were based on be-spoke or proprietary software: the more extreme protection came from rigorously implemented hardware, including network boundary- "Firewalls" to protect against hacking and malicious viruses. Some technical solutions were "validated" by external Audit services, with legal albeit limited "guarantees" of service.

An understanding of the likely threats was an important adjunct to the interview. The author passes no judgement however on the level of individual corporate threat, the basic operational vulnerability before or after the additional controls, or the success of any particular implementation as discussed with the selected firms.

The Project “Qualitative discussion” [Glaser]. The open questioning, semi-structured interview was loosely based on EU and DTI sponsored educational material. This was expanded to include “discretionary” subjects as the discussions evolved. Emphasis was placed on listening and learning not in the completion of standard checklists!

### Contextual Discussion

- A] Security risks-threats and vulnerabilities..potential set based on business impacts.
- B] Set of statutory and contractual requirements.. underpinning intercompany communication.
- C] General principles, objectives and requirements for IT in which information security fits.

Control and compliance procedures

- 1] Information Security Policy
  - 2] Security Roles and Responsibilities
  - 3] Security Awareness, Education and Training
  - 4] Reporting- including statutory auditing
  - 5] Specific Processes against Hacking, Viruses etc
- Additional areas with some information security impacts included.
- 6] Business Continuity Planning
  - 7] Control of Proprietary Copying
  - 8] Safeguarding Company Records
  - 9] Compliance with Data Protection Legislation
  - 10] “Millennium Bug” Actions [in 1999]

Interview with specific questions on procedural solutions as embodied in firms “routines”. Further specific questions were asked on additional “assurance” controls at the end of the interview- depending on the interviewers subsequent perception of the level of operational security of those firms with implemented network firewall protection.

Selected owners, management and staff were interviewed. Anonymity and privacy within the interview were paramount. Especially in matters of internal staffing. Records were not maintained post research period. Findings are not mapped in the text to individual named enterprises-the subject matter was deemed too sensitive. Limited implementation of the “formal” information systems security controls may or may not imply poor security-that would require an in-depth vulnerability analysis and/or risk assessment! That was not part of the study.

### Grounded Theory - The Economic Analysis

The collection and analysis of qualified data can take many forms. The approach adopted in the study was that of Grounded Theory developed by Glaser and Strauss. [Glaser] Theory is generated by analysis. The hypotheses then if necessary being tested using quantified methods. The fundamental tenet of the theory is derived from participants answers not imposed by any rigid questionnaire.

In summary, the qualitative methodology of Grounded Theory is a method of discovering theories from data (not-testing or proving a theory). It has the following features;

- 1] Descriptive not numerical data.
- 2] Inductive approach (developing concepts from patterns in data collected)
- 3] Flexible research approach (open questions, semi-structured yet bounded framework)
- 4] Phenomenological approach (understanding the perspectives of others in the context of their own not interviewers reality)
- 5] Naturalistic Approach (minimise interviewers affect on others opinions)
- 6] Suspension of own values and beliefs (“just a game”)
- 7] Validity of qualified sample (not the replicating quantified numerical data)

The basic mechanics of the fieldwork study was to examine the data in fine detail, allocating categories or labels/codes to each small part of it. Each individual statement was a fragment of information that could be labelled in different ways. This process of categorisation was compiled from qualitative fieldwork interviews. The final outcome was a full illustration of the particular theoretical categories, any refinements, elaborations or modifications.

The categorisation of problems & solutions was generated from the following labels/coding. Problems of, \*Threats (Actual/Perceived), \* Risk, \* Trust (Implicit -> none), \* Control (minimum -> "overkill")

Resulting in/from solutions of, \* Physical Security, \* Administration, \*Logical Controls, \*Encryption, \*Organisation, \* Policies, \* Standards, \* Roles & Routines, \* Business Relationships, \* IT/Telecomm facilities, \* IT Functionality & IT Assurance, \* Audit/Validation (external/internal) General approach-\* Learning by doing, \* Benefits/Profits impacts, \* Future Direction Qualification is the necessary beginning of the analysis into the Information Systems Security Problem. The IT specialist must be disciplined enough just to listen and learn from the smaller enterprise! Too long have they imposed their own ideas and preconceptions.

### Findings- The Study Results

The businessman expresses some concern about information security in the context of using the Internet and there is some evidence that "formal" information security controls are being implemented. The type and extent of such controls however varied widely between the firms visited. DTI, BSI and other material was referenced and/or demonstrated as having been implemented. "We have got the BSI 5570 Quality Standard and it does include our computer security policy" (Plastics Component Manufacturer). There was a good general level of understanding of the subject with the need for semantic clarification kept to the minimum. This was borne out by the lack of discussion of the "Millennium Bug" (another DTI Awareness Campaign). The firms understood the operational difference between external security exposures and internal operational deficiencies, although it was recognised that the customer was just interested in the outcome not the reasons. "Access to our web site was so slow when we first set it up that security wasn't a concern. We were more worried about losing potential customers than protecting against hackers". The level of necessary security against selected threats was explored in the interview. It highlighted the conundrum that functionally richer controls may give no higher operational assurance in the solution (e.g. a longer password, easy to ascertain, gives no extra protection.). "We had to stop people sticking their passwords up on the wall for all to see when they came into the shop". (Travel Agent)

The two main threads in the innovation process for information systems security were understanding the problem and developing the solution. Neither are linear however; there are complex feedback and iterative processes. Information systems have been implemented to improve the planning and operational performance of firms, yet the application of computers generated their own security exposures. New problems; new solutions. Even the smallest firms had to reach a technical competence that had not been foreseen in the initial planning for the information system. "We had lots of parts pilferage problems before the computer. We have solved that problem by having computer produced, random "bin checks" but we now have new ones (problems) that need even more complicated controls. (Dynamic safety stock limits?) We are having to run just to stand still!"(Motor Main Dealer/Garage)

The discussion on security could not be divorced from the overall information systems context. Applications that handled private internal services (e.g. payroll) were a confidentiality issue; those that were supplying public services (e.g. advertising goods) usually demanded operational integrity and availability. Confidentiality problems result from the issue that electronic data is non-rival. Multiple copies can be produced without diminishing the original; yet information is, usually, highly excludable, private to an individual or firm.

In reducing importance; availability, integrity and confidentiality of computer applications/data, are the usual, a priori, security assumptions underpinning information processing in the larger commercial firm. Study findings showed however that privacy of data was seen as most important. This discovery was unexpected, as published quantitative research with major commercial institutions, had usually given confidentiality control a lower priority. The size and management style of the small firm may be the reason for the differing emphasis. An owner, with operational

control, knows his/her customers personally and respects their privacy. The boundaries therefore between corporate and client information may be indistinct. "B\*\* S\*\*\* is having his new house completely refurbished. We have been told to keep it quiet!" (Interior Designers). Controls over confidentiality may also help maintain competitive advantage, especially against larger competitors, in an increasingly integrated global market. "Information security is not about size of operations but about type of business. We are a small company in a specialist international market, good margins but highly competitive. We protect our designs from the big outfits." (Reproduction Furniture)

Availability of service and integrity of records are still important but parallel manual administration, with associated procedural skills, was possible if systems failed. Many smaller companies have only been recently computerised (last 10 years?) and fall back systems were still available- unlike larger corporations (?). "We get very worried when the system (network) goes down. This doesn't happen much but it gets very heavily loaded sometimes- we are not overly concerned about people destroying things, we still keep manual records." (Travel Agent)

The threats to computer systems were diverse reflecting the firms interviewed. Actual incidents ranged from physical tampering with equipment, "If we leave anything valuable on site, in the works shed, it will get stolen. We are now using smaller portable computers that plug in (to BT lines) when we do on site measurements" (Construction): to unauthorised amendment of "public access data" (with subsequent commercial embarrassment) "We are worried by pornography in the office. We created a Web Site of houses on the Internet only to find that it included nude pictures. We didn't know about it until a customer complained. It sounds funny but it wasn't!" We have a lot of temporary staff, it might have been one of them". (Estate Agent)

All the firms had an IT Security "policy", but with various levels of increasingly complex administration, covering physical and logical "control barriers". Three firms had tried encryption to maintain data privacy, but regular data coding on the Internet was experimental.

Good physical security was a fundamental starting point in all firms interviewed. Many problems were simply addressed by the common sense locking of offices, switching off machines etc. The complementary administration was documented. Other threats were understood as technically more challenging, yet, on cursory investigation by the interviewer, seemed to be more perceived than actual. The "DTI Security Awareness" campaigns seem to have been quite effective. "I used to listen to the DTI audio tape "The issues explained" whilst stuck in the traffic!" (Plastics Component Manufacturer). The media hype, however, on computing hacking and viruses etc, has obfuscated the main messages of risk assessment, trust and balanced business opportunity. "Small companies consider good security a checklist item. They are especially concerned about privacy following newspaper articles on hacking. Encryption products are now selling well, but it may be overkill considering the likely threats?" (IT Systems Integrator-1)

Knowledge within the client on specific hardware and solutions of logical access controls to enforce security appears limited. The management did not understand the significance of the DTI security product evaluation E-numbers. "Being in the business, we thought it was just about the quality of the computer electronics- mean time between failures. That sort of thing. We didn't realise that 99% is about how you use it (hardware). We're too busy to mess about with complicated procedures!" (Electrical Wholesaler) Secure variants of computer operating systems in "Internet Firewalls" were implemented in four of the selected firms, however the protective features were not consistently administered. Logical access authorisation controls required user identification, information security categorisation and recognised privileges associated with information management (who can access, what, when, how etc). "Every partner thinks that he/she is an expert and can write security policies but no one wants to take day to day responsibility in enforcing controls." (Solicitors/Partnership). In fact, even those companies selling such advanced security products questioned whether the customer was achieving the desired benefit. "Companies are buying hardware and software security solutions hoping that it will improve their administrative control- obviously it won't by itself. They must do a lot themselves- many just don't have the discipline!" (IT Systems Integrator-2)

The integration of good security administration with supporting functionally innovative, high assurance Information Security products has yet to happen in many of the small firms. The most successful product installations appear to be in those firms that are building in better operational administration generally (not just in computer applications). "Security must be built in not bolted on

---

to our administration.” (Interior Decorators/Reproduction Furniture etc) “ Security is about thinking of the system-not some (IT) security product” (Construction). Specialist IT security products would then be implemented to maintain service and data assurance. Poor operational administration was unlikely to be rectified by innovative computer products, although this was the apparent approach sought by some of the firms questioned. “We are putting the new system in. It should force us to improve our administration which is a bit ramshackle at the moment!” (Coach/Bus Company).

The apparent technical nature of the subject is resulting in a high reliance on external IT and Telecommunication Suppliers both for the initial solution and on-going maintenance. “We are getting a computer company to design and implement our software. In general terms we have told them what sort of controls we want (on ticket sales) but we have to trust them implicitly to program things properly” (Coach/Bus Company) Such “consulting firms” have a high level of tacit knowledge built upon dealing with many clients This is the basis for their fees“ We depend upon our external Auditors to sign of our controls each year-that is what we pay them for”. (Motor Parts Dealer) It is probable that the feedback into “formal” industry level policies, standards and procedures is via such technical advisers. “We are planning to include computer security into our annual ISO 9000 (BSI) Quality Standards review with their help”.(Motor Parts Dealer) The larger multinationals may have the power to dictate user needs but the smaller firms may be at the mercy of suppliers who have an interest in selling unnecessary solutions.

The level of modification of “standard” products to meet unique individual needs, varies considerably. A high assurance solution appears to need as much absolute investment by the small company as by a company ten times the size. Even the Systems Integrators seem to be shunning the formal “accreditation” services, preferring the less stringent, more flexible approach of self “product/service” evaluation. “No-we are not a recognised “licensed facility” but we know enough about the problem for our customers to trust our judgement. Our reputation is far more important than a written “guarantee” of better security!”(IT Systems Integrator-1) The smaller end user may not be visible enough to directly influence the creation of formal IT security standards. The high assurance hardware and software solutions being pushed by the IT suppliers, with, or without, formally “certified” IT security products, may be an unnecessary overkill.

Fear however is a commercial motivator. High visibility prosecutions from the Computer Misuse Act of 1990 have heightened the awareness of what could happen. The small firms interviewed however, do not appear to be likely targets for malicious attack (in the judgement of the interviewer). There has been however no measurable risk assessment. There was no “independent” evidence of malicious hacking. In fact, with the possible exception of the Estate Agent, there were few recorded “unauthorised” accesses, via the Internet, to any respective Web sites. In one instance the implementation of the network “firewall” has had an unforeseen control benefits hidden from junior staff ,“The programmers think that the installation (IBM RS 6000) is to stop unauthorised access to internal records, in fact the monitoring facilities have allowed management to minimise “time wasting” from surfing the net! (IT Systems Integrator-2) Some security solutions may be just too much “insurance”, especially when considering a firms difficulty when trying to classify and code data. “Anything that’s really important will never be put on a computer!” (Solicitors/ Partnership) More trust and less explicit controls may even be in order? “We don’t trust anyone including ourselves” (Construction).

A much broader issue pervaded the discussions. This was whether or not organisational change from Internet exploitation would create new threats not necessary to information but to clients themselves... “The owner selling directly over the Internet may appear to save some money but have they thought of the risks they take of inviting unknown people into their homes. At least we chase up to ensure that the prospective details are correct on both sides”. (Estate Agents). It appears that E-Commerce may become the normal way of purchasing small, low value, non-perishable item. The perceived risks involved in other types of purchase may inhibit its universal appeal. Professional service from unbiased advice to correct delivery will remain paramount.

## Conclusion

E-Commerce is the stated aim of many of the smaller firms. It can help them compete on level terms with the larger multiples. The extent to which networked technology assists the necessary organisational and administrative changes varies accordingly.

---

The use of Grounded Theory, to generate explanations from “situations” as described by the people interviewed, appeared well suited to a study into understanding of information systems security attitudes and actions. The early pioneers of formal IT security controls may not necessarily achieve higher “profitability”. The controls may even be unnecessary. It is possible that operational experience in using the Internet will result in a higher level of commercial confidence with less need for stringent controls. “I can see nothing but costs from trying to implement these better controls. It might be worth it but who knows? We will give it a try as our major customer (a vehicle assembler) seems to be pushing network security. But unlike us they could lose millions of pounds if production fails?” (Plastic Component Manufacturer) The firms, from learning-by-doing, may be in a better position in two/three years time to make rational decisions on the correct balance of IT security controls.

They will be less vulnerable to the “threat” hysteria and paranoia generated by the R&D “technology push” of the IT services sector. In E-Commerce however, the security perspective of the general public may be the ultimate determinant of what security controls need to be offered by the retailer. A few well-publicised scams however may unduly influence a rational decision making process within the business community!

A follow up study was suggested post-Millennium. This was positively received by most of the firms interviewed.

#### **References- selected**

- Vincent, John -An Intelligent Persons Guide to History, Duckworth 1995  
Beckman, Robert C. -Crashes: Why they happen-What to do, Grafton 1990  
Chancellor, E- Devil Take The Hindmost-A History of Financial Speculation, Macmillan 1999  
Glaser, B.G. and Strauss, A.L. (1967) The Discovery of Grounded Theory; Strategies for Qualitative Research, Chicago: Aldine Publishing Company  
Legislation- The Queens Speech -Forthcoming Legislation 1999/2000  
Elsevier Science (Publications) Ltd -Computer Audit Update (1987-1997) & Computer Fraud & Security (1992-99) Oxford (selected items)  
Panacea [and other systems integrators] , IBM RS6000 users with Unix/AIX 2.2, Amerigo E-Commerce and Secure ISO/OSI  
Foucault, Michel- Discipline and Punish (1977) Allen Lane, London.